

SOC4Academia Toolbox



WE PLAY FOR CYBER
IN ACADEMIC SECTOR

This publication was supported by the SOCCER project, funded under Grant Agreement No. 101128073, with the support of the European Cybersecurity Competence Center (ECCC).

The project is co-financed by the Polish Ministry of Science and Higher Education under program *Co-financed International Projects*.

The project is co-financed by the programme entitled Recovery and Resilience Plan of the Slovak Republic implemented through the Ministry of Investments, Regional Development and Informatization of the Slovak Republic (MIRRI SR).

ISBN 978-83-980194-3-9



9 788398 019439

COORDINATOR



AGH UNIVERSITY
OF KRAKOW

AGH

CONSORTIUM MEMBERS



JAGIELLONIAN UNIVERSITY
IN KRAKÓW



UNIVERSITY OF AGRICULTURE
IN KRAKOW

MUNI



cesnet
.....



Tomas Bata University



UNIVERSITY
OF TARTU



Mykolas Romeris
University

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

List of authors

SOC4Academia Toolbox	Teamwork of the SOCCER Consortium Partners, edited by Łukasz Faber
AGH University of Krakow	Łukasz Faber, Paweł Kopeć, Michał Kutra, Jakub Izak
University of Agriculture in Krakow	Michał Cupiał, Mateusz Ponikiewicz
CESNET	Martin Žádník, Václav Bartoš, Matěj Barnat
Jagiellonian University in Kraków	Lucjan Stalmach, Michał Hanasiewicz, Piotr Janczura, Arkadiusz Wierzbowski, Mateusz Sykała, Aleksander Orłowski, Bogusław Mielec
Mykolas Romeris University	Marius Laurinaitis, Saulius Kvedaravičius
Masaryk University	Matúš Raček, Stanislav Špaček, Andrej Tomči, Matěj Smyčka, Ondřej Molík, Daniel Tovarňák, Martin Laštovička, Daniela Belajová
Pavol Jozef Šafárik University in Košice	Kristína Kováčová, Monika Rapavá, Pavol Sokol, Laura Bachňáková Rózenfeldová
University of Tartu	Pelle Jakovits, Tommy Tomson, Gular Samadova
Tomas Bata University in Zlín	David Malaník, Nicol Daňková, Roman Šenkeřík,

SOCGER Project 2025

Table of contents

CHAPTER 1 SOC MODELS IN ACADEMIA

1.1. Obtaining and providing SOC services for Academia	11
1.2. Review of SOC Models	16
1.3. Location of the SOC in the organizational structure	19
1.4. Interdependencies with other departments	20

CHAPTER 2 MATURITY MODELS FOR SOC-S

2.1. Connection to SIM3 (Security Incident Management Maturity Model)	24
2.2. SIM3 Maturity Assessment Tools	71

CHAPTER 3 SOC ORGANIZATIONAL AND ENVIRONMENTAL REQUIREMENTS FOR ACADEMIA

3.1. Context in EU Academia	77
3.2. Legal and regulatory environment (EU level and per member country)	86
3.3. Personnel/ Roles and requirements	105
3.4. Cyber Threat Intelligence and data sharing – compliance, legal and organizational issues	111
3.5. Supporting requirements	124

CHAPTER 4 SOC TECHNICAL ARCHITECTURES

4.1. Architectural considerations for building a SOC	166
4.2. Logging architecture	169
4.3. Networking configuration and placement of sensors	178
4.4. Scanning, asset management, vulnerability management	182
4.5. Tools required to build a SOC	185

CHAPTER 5 INTRODUCTION TO DIGITAL FORENSIC AND INCIDENT RESPONSE (DFIR)

5.1. Security incident handling and response	190
5.2. Digital Forensics	195

CHAPTER 6 REVIEW OF SOFTWARE AND HARDWARE SOLUTIONS

6.1. Review methodology	205
6.2. Open-source vs commercially available off-the-shelf (COTS) SOC tools	207
6.3. SIEM, SOAR, EDR, XDR	213
6.4. Asset Inventory Management	221
6.5. Network Monitoring Tools	227
6.6. Incident management - Solutions review	233
6.7. CTI sources, CTI sharing platforms	237
6.8. Vulnerability assessment and scanning tools	246

Introduction

Izabela Albrycht - Director of the Cybersecurity Center at the AGH University of Krakow, the Initiator and Leader of the SOCCER project.

The world is going through tangible turbulence caused by a combination of conventional and unconventional threats. The period of relative peace has ended with the return of war to Europe and with cybersecurity threats reaching the highest level in history [1]. The academic sector is, in fact, at the center of this turmoil due to its critical role in developing emerging and disruptive technologies, which have recently become powerful tools in the geopolitical struggle between major global actors. These technologies have become both the drivers of economic growth and the foundations of the modern defense sector.

If this role is not yet fully recognized by the Science and Research sector (R&S) leadership, it soon will be - due to the need for enhanced collaboration with public institutions on projects aimed at the R&D&I of innovative solutions for national security and technological sovereignty. This will go in parallel with the need of the R&S sector to comply with restrictive, yet highly relevant, cybersecurity measures imposed by new EU regulations focused on protecting the most critical assets of the modern world, i.e., data and innovation. More such measures may follow with the aim to address the "Research Security" challenge.

The period of relative peace has ended with the return of war to Europe and with cybersecurity threats reaching the highest level in history.

R&S Threat Landscape

In the 21st century, the dynamics of the threat landscape of the R&S sector are driven by the traditional industrial espionage and physical threats but also by new types of threats related to the nature of hybrid warfare characterized by various actions and campaigns of destabilisation and incidents of sabotage. Among these, cybersecurity threats are increasingly ranked high. Sensitive data of various kinds – personal data of current and future R&S leaders, professionals, and innovators, information about scientific and technological breakthroughs and financial information of institutions - as well as daily operations are at stake. The statistics are alarming. The R&S sector has been targeted with an average of 3,828 weekly attacks. When compared with the Government/Military and Healthcare sectors, with 2,553 and 2,434 attacks [2], respectively, it has been leading in the statistics and has been by far the most impacted “accounting for more than 50% of breached organizations”. [3] In 2024, cyberattacks affected the operations of institutions such as the University of Cambridge, Università di Siena, Université Paris-Saclay, Reykjavik University, Berliner Hochschule für Technik, University of Winnipeg, Heinrich-Heine-Universität, Universitätsklinikum Brandenburg, Sveriges lantbruksuniversitet, Kansas State University and South East Technological University Waterford Campus.

These incidents have significantly increased the awareness among R&S leaders and politicians that the need to build cyber fences in this sector is imminent. In fact, it is further reinforced by recent EU regulations such as Network and Information Security Directive 2 (NIS 2) or Critical Entities Resilience Directive (CER), which will require compliance from R&S organizations, including universities.

Moreover, Research Security has reached new heights in the political discussion regarding the hybrid threats faced by the R&S sector, which is illustrated by the Council **Recommendation on enhancing research security** [4], approved in May 2024, as well as by the ongoing political discussion on the structure and priorities of the EU Framework Programme for Research and Innovation (FP10), which will run from 2028 to 2034. The discussion highlights the need to align security considerations in the R&D&I process across the EU.

The Role of the S&R Sector in R&D&I for Security and Defence Capabilities

The Warsaw Declaration on the strategic role of the future EU R&I framework programme [5], signed by the ministers responsible for research gathered on 10-11 March 2025 in Warsaw under the Polish Presidency of the Council of the European Union, stresses that the future framework programme should support excellent and impactful R&I in order to boost competitiveness and contribute to the ‘EU’s security, sustainability, resilience, technological sovereignty and strategic autonomy, and allow the European Union to respond to current and future challenges more effectively’. The motto of the Polish Presidency, “*Security, Europe!*”, is illustrative of the biggest challenge ahead of us all: ‘the arms race between the European Union and the Russian Federation’ [6], which will particularly require collaboration between governments and the R&S sector. The recent report by Boston Consulting Group [7] -shows that the demand for enhanced collaboration between the S&R sector and ministries of national defense keeps increasing each year. This demand is driven by the need to integrate scientists and innovators into efforts to strengthen defense capabilities and build a state’s resilience. Additionally, innovation accelerators, often embedded within universities or research institutions, are expected to play a key role in developing these capacities.

For all these overlapping reasons, the necessity of strengthening security and resilience of the S&R sector against cyberattacks, including cyber espionage targeting emerging and disruptive technologies, most of which have dual use nature, continues to grow.

The Cybersecurity Way Forward in the S&R sector

Due to the rise of cyberthreats and the need to engage the S&R sector in technological efforts contributing to national security, we can expect that along with the recent implementation of the NIS 2 Directive and General Data Protection Regulation (GDPR), the EU will impose additional mechanisms to enhance the security of research outcomes against external interference and misuse. This will probably include greater scrutiny in terms of international collaboration, best practices in risk management, and other measures aimed at protecting R&D&I processes and their outcomes, particularly in strategic technological areas encompassing dual-use technologies such as artificial intelligence, quantum technology or biotechnology.

Implementing advanced and effective security measures is a long and multidimensional process. However, one of the key objectives for S&R organizations should be the establishment of Security Operations Centers (SOCs), which have recently become instrumental in building cyber resilience by monitoring and responding to cybersecurity incidents. SOCs can be established exclusively in-house or in the hub formula offering a SOC's services for many different institutions. The concept and the possible models are presented in the publication that you are about to read. The Toolbox examines various models, practices, and requirements for SOC implementation tailored to the unique needs of universities and research organizations. It provides a comprehensive guide on the strategic, technical, and operational considerations necessary for building effective SOCs.

What can be learned from the SOC4Academia Toolbox

The aim of the **SOC4Academia Toolbox** and its technical and legal considerations is to help decision makers and cyber specialists navigate the complex process of SOC development and implementation. The Toolbox contains information on SOC development, deployment and functioning as well as different models of the deployment and integration of the possible SOC services, along with the challenges of incorporating a SOC within the organization. Digital forensics capabilities can further empower SOCs operators to investigate and address security incidents effectively, providing insights into attack methods and mitigation strategies. The information offered in the publication helps assess budget needs, establish a roadmap of SOC implementation, create its organizational structure, and support community trainings aimed at educating skilled personnel capable of handling diverse cybersecurity threats and tasks.

The analysis presented on European Union regulations such as NIS2 will help navigate the complexity of legal requirements and maintain legal and ethical standards in cybersecurity management, establish relevant cybersecurity policies as well as facilitate collaboration with CSIRTs and European and international structures in order to expand Cyber Threats Intelligence sharing and enhance a collaborative cybersecurity resilience framework. However, this collaboration requires careful management of privacy concerns and regulatory constraints. From a practical perspective, this analysis will help universities adapt to applicable, complex standards and regulations.

We hope that the SOC4Academia Toolbox will serve as an important source of practical information for many institutions in the coming months and years and will contribute to numerous successful cybersecurity transformations in the S&R sector, ultimately

increasing the cybersecurity of the R&D&I process supporting both national security and economic competitiveness.

We also do believe that the document will contribute to the development of cybersecurity as a scientific discipline, which, due to its interdisciplinary nature, integrates legal and regulatory dimensions. Moreover, the content will be useful for cybersecurity experts and specialists in academia and the tech industry, who will be able to utilize the gathered information for further fundamental and applied research, as well as for R&D&I efforts and the implementation of new cybersecurity technical solutions.

On behalf of the SOCCER Consortium, I encourage all Readers to make good use of the Toolbox as it provides a roadmap for universities and research organizations to enter the path of building resilient cybersecurity operations tailored to their unique challenges and opportunities. By prioritizing SOC implementation, institutions can safeguard their digital assets, foster trust, and contribute to a secure S&R ecosystem.

References

- [1] The latest records indicate that in Q3 of 2024, the number of cyber-attacks worldwide has reached an all-time high, with a 75% increase compared to the same period in 2023. A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide, <https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/>
- [2] Ibidem.
- [3] 2024 Data Breach Investigations Report, <https://bakotech.pl/upload/fileuploads/files/2024-dbir-data-breach-investigations-report.pdf>
- [4] Council of the European Union, Council Recommendation on enhancing research security, 2024/0012 (NLE), <https://data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf>.
- [5] https://polish-presidency.consilium.europa.eu/media/r5fa13v5/warsaw-declaration_final.pdf
- [6] Donald Tusk, 'Europe must take on the challenge and win the arms race. I am convinced that Russia will lose, just as the USSR did. This is the only way to avoid a larger-scale conflict', <https://www.rp.pl/polityka/art41887141-donald-tusk-mowi-o-wyscigu-zbrojen-rosja-przegra-tak-jak-przegral-zsrr>
- [7] Schlueter M., Giesener M., Mayer L., Key L., Hassan M., Overcoming the Six Unspoken Barriers That Impede Defense Innovation, <https://web-assets.bcg.com/c0/ad/ed8e25f5483aa1f42a614c0224bf/overcoming-the-six-unspoken-barriers-that-impede-defense-innovation-msc.pdf>

1. SOC models in Academia

Security Operations Centers (SOCs) form the backbone of an organization's cybersecurity infrastructure, serving as centralized hubs for monitoring, detecting, and responding to potential threats.

This chapter takes an in-depth look at the landscape of SOCs, focusing on the diverse approaches organizations can adopt to meet their security needs.

From traditional in-house setups to outsourced and hybrid models, SOCs offer a range of frameworks that can be tailored to different operational requirements. By exploring these models, the chapter aims to shed light on their structural variations, core functions, and unique advantages. These insights provide a comprehensive understanding of the essential components and strategies that underpin successful SOC implementations.

This chapter presents several possible SOC models to consider. However, we strongly recommend reviewing the other chapters for a broader understanding of the topic. By exploring the additional recommendations and analyzing your organization's specific needs, you will be better equipped to make an informed decision about the SOC model most suitable for your organization's needs.

1.1. Obtaining and providing SOC services for Academia

Each organization has to do security monitoring, but not all organisations are equally capable of doing it or want to do it by themselves. Thus, they have to make a crucial decision on whether to build an in-house security operations centre and obtain all required resources or to outsource this area to a security service provider.

Of course, midway solutions are possible – the organization can build a small SOC with basic functions and outsource those more advanced ones (e.g., digital forensics) to an external entity.

In this section, a less popular model, i.e., “shared services”, will be considered. In this model, multiple organizations join their forces to build a common SOC from their separate resources. This is not very popular with commercial organizations, but something to consider in public (or governmental) organizations with a similar scope of operation (e.g., universities, hospitals).

Building an in-house SOC

Larger universities may consider building their own SOC. This may be rational for universities, which:

- have a larger, separate, in-house IT team;
- have a large number of devices (IT, OT, networking, endpoints) or use multiple independent IT services;

- have already existing research cybersecurity departments or a faculty, which may benefit from cooperation with internal technical security staff;
- have non-standard, specific needs that may not be easily covered by MSSPs. This may be especially important with research-related hardware and software, high-risk facilities, or national security or military research that may have a higher confidentiality classification;
- have non-standard privacy and data security needs. For example, medical or military universities;
- have large financial resources, as the SOC may be treated as a potential investment.

Outsourcing SOC services

In many situations, it is simpler and cheaper to just obtain the needed services from the market. Before doing that, there are decisions to be made and questions to be answered:

Easily outsourced capabilities are:

- Forensics and malware analysis.
- Penetration testing and red teaming.
- Alert triage outside business hours.
- Business continuity assistance.

1. What services are outsourced? Or maybe the whole SOC capability should be outsourced?

2. Which MSSP (Managed Security Service Provider) to use? Is it important for them to have experience in providing services to academia? Do they have any references? Is the technology stack matching yours or are they able to work with another one that fits your needs?

3. What level of service should be provided?

The SLA (service-level agreement) needs to be discussed with the provider, and define levels for, among other things, response times, 24/7 availability, proactivity of services, and reporting frequency.

4. What is the model of data control and ownership? How will sensitive data be protected? Who owns the data collected? Where is the data located (also in terms of geographic location). Which (if any) third parties will have access to this data?
5. How will the offered services and tools used by the provider be integrated with the university tools? The same goes for the integration of the processes.
6. What will be the cost structure? Is it a monthly flat fee or will the cost be based on the number of incidents handled? Are there any hidden costs?
7. Is the provider compliant with the local regulations? For example, is it handling personal data in accordance with the GDPR guidelines?
8. What are the responsibilities of the university and the provider in terms of incident escalation processes?
9. What reports and metrics should be produced and how often?
10. How flexible should the provider be? Academia is a specific field and may require some tailoring of the services.
11. Is the BC and DR guaranteed by the provider?
12. What will be the exit strategy? Dependence on a single provider is always a risk and the university has to have a plan for a possible termination of the services.

13. Will training for the university teams be provided? Will there be any knowledge sharing?

“Shared services” SOC

By “shared services”, we understand a cooperation between universities (and possibly other similar organizations) to create a shared SOC for a group of them. This may be done in the form of a SOC department within one of them, a federated SOC, or as a separate business unit.

Benefits:

- Better cost efficiency, as multiple resources can be shared.
- Access to advanced security tools, as organizations can buy better tools on a joint basis.
- Skilled security personnel, due to building a common team of experts.
- Scalability, as the shared services SOC can scale services according to the needs of each organization.
- Threat intelligence sharing.
- Standardised compliance and reporting.

The features of such a model are as follows:

1. Centralized infrastructure for monitoring, detection and response.
2. Multi-tenant environment.
3. Shared costs.
4. Unification of some of the security services, for example: threat monitoring, incident response, threat intelligence sharing, compliance.
5. Tailored configurations for each organization.
6. Shared expertise and collaboration.

Challenges:

- Data privacy and segregation between organizations has to be ensured, so that no cross-contamination can occur.
- Customization and flexibility may be limited.
- Incident response coordination has to be properly defined and not always can be universal.
- Governance and control of specific organizations may be limited.
- Performance consistency may be hard to obtain if there is too much performance demand from some organizations

What to choose?

Ultimately the decision will be dependent on multiple factors, for example:

1. Costs of operation. In a larger and more diverse organization, outsourcing may be more costly than building in-house capability.
2. Staff retention. This may be especially important for public/government-funded universities, which may have problems with hiring and maintaining required teams.
3. Need for 24/7 operation.

The table summarizes advantages and disadvantages of various models of SOC.

Table 1 – Models of SOC

Model	Advantages	Disadvantages
Building in-house	• Complete control over security policies, tools, and operations. • Tailored to specific organizational needs and risk profiles. • Full data privacy, compliance, and control over sensitive information. • Flexibility in adapting to changing security requirements and incidents. • Ideal for high-complexity organizations with unique or sensitive requirements.	• High upfront costs (infrastructure, tools, personnel). • Requires hiring and retaining skilled cybersecurity professionals. • Continuous operational expenses (training, upgrades, 24/7 staffing). • Slower to implement and scale compared to outsourced models. • Managing and maintaining an SOC can be resource-intensive and complex.
Outsourcing	• Access to skilled experts and cutting-edge security technology immediately. • Reduced upfront costs compared to building an in-house SOC. • Scalable and flexible according to business needs. • 24/7 monitoring and faster incident response without internal staffing needs. • Easier to manage regulatory compliance via the provider's certifications.	• Less control over security processes and policies. • Potential data privacy concerns and risks with third-party providers. • Dependency on external provider for critical incident response. • Long-term costs may increase depending on service agreements. • Customization and service tailoring may be limited.
Shared services	• Cost-sharing with other organizations, reducing overall operational costs. • Access to advanced security tools and resources that may be too expensive alone. • Shared threat intelligence and insights across multiple organizations. • Scalable services that can adapt to changing needs.	• Limited control over SOC operations and processes. • Potential risks in data privacy and separation between participants. • Customization may be more limited compared to in-house SOC. • Incident response can be slower due to shared resources.

	• Ideal for organizations with smaller budgets or those lacking in-house expertise.	• Performance may vary if not properly managed across tenants.
--	---	--

Building SOC-as-a-service capabilities

When the in-house SOC implementation has been chosen, then the university may also decide to establish a Security Operations Center (SOC) as a service. In such a situation, it must first focus on building its internal SOC infrastructure. This foundational step could take the form of either an in-house SOC, specifically dedicated to the university's needs, or a shared services SOC, which would serve multiple institutions or departments within the university. Establishing this internal capability is crucial as it will provide the necessary experience, tools, and processes that will form the backbone of the SOC-as-a-service offering.

What kind of services can be offered?

Typical SOC services (for a detailed description – see the ENISA guide [1]).

Points to consider:

- What kind of services can be offered?
- What technology stack will be used?
- What staff is needed?
- Can the existing staff be used or is there a need to hire new employees?
- Can the staff be remote or is it required to be on-site?
- How is the resiliency and continuous operation going to be assured?
- What will be its financial model?

1. Incident Management
 - Alerts and warnings
 - Incident handling
 - Incident analysis
 - Incident response on-site
 - Incident response support
 - Incident response coordination
2. Vulnerability Management
 - Vulnerability analysis
 - Vulnerability handling
 - Vulnerability response
 - Vulnerability response coordination
3. Artifact Management
 - Artifact analysis
 - Artifact response
 - Artifact response coordination
4. Monitoring and Detection
 - Intrusion detection services
 - Technology watch
5. Risk and Security Assessments
 - Risk analysis
 - Security audits or assessments
6. Security Tools and Configuration
 - Configuration and maintenance of security tools
7. Awareness and Information Sharing
 - Security-related information dissemination
 - Awareness building

- Education/Training
8. Security Consulting and Continuity Planning
 - Security consulting
 - Business continuity and disaster recovery

This is a broad range of possible services. Typically, at the very beginning of operation, a newly founded SOC will be focusing on selecting core services, usually related to monitoring and incident response support. With more experience and end-users, new services will be added.

It is important to note that some of these services require each other to provide a meaningful portfolio and some of them are different scopes of the same service (for example, if the client is paying for incident response coordination, they will not get incident response on-site as this is more involving type of the same service).

What staff is needed?

In terms of the required roles, they will be fully dependent on the services offered. Usually, the team will require:

- SOC analysts of various tiers or types:
 - Traditionally, SOC analysts were split into three tiers – first, second and third tier (according to their experience). Nowadays, it is common to have untiered SOC in which people handle issues more often in line with their expertise;
- Security/SOC engineers who are responsible for implementing security solutions used by the SOC;
- Pentesters or red teamers both for internal testing and possible external services;
- Digital forensics examiners providing expertise in forensics for the rest of the team;
- Security trainers for providing cybersecurity awareness training services;
- And, of course, managers (they may be part of the technical staff, but it is important to keep in mind that they will spend a lot of time on managing their teams).

In terms of the numbers, this depends on the operating model (for example, 8/5 vs 24/7). For the full 24/7 coverage, the organization will require at least two off-hours shifts per day. Depending on the employment law in the country, it may even double the required number of employees to fully cover all shifts.

The detailed information about personnel roles will be discussed in Chapter 3.

1.2. Review of SOC Models

Security Operations Center (SOC) models refer to the different ways organizations structure their cybersecurity operations to monitor, detect, respond to, and prevent security incidents. The model a company chooses depends on factors like the size of the organization, budget, security requirements, and available resources.

In-house SOC

An in-house SOC is a dedicated team within an organization. This team is responsible for monitoring, detecting, and responding to security incidents. This model offers the highest level of control and customization, allowing the organization to tailor security operations to its specific needs. The team can develop deep expertise in the

Advantages

- fully managed and operated within the organization
- high level of control and customization
- significant investment in infrastructure and skilled personnel

organization's unique infrastructure, applications, and threat landscape. However, building and maintaining an in-house SOC requires significant investment in technology, infrastructure, and highly skilled personnel. Organizations must invest in security tools, such as SIEM, threat intelligence platforms, and many other advanced monitoring tools. Additionally, ongoing training and development for the SOC staff are critical to keeping pace with the evolving threat landscape.

An in-house SOC can provide faster response times to incidents due to the team's familiarity with the organization's environment and the absence of communication delays that might occur with external partners. This model also ensures that sensitive data remains within the organization, addressing potential privacy and compliance concerns. However, the costs associated with staffing, technology, and continuous improvements can be substantial. Organizations must also contend with the challenge of retaining skilled cybersecurity professionals, who are in high demand across the industry.

Outsourced/Managed SOC

An outsourced SOC involves partnering with a third-party service provider to manage security operations. This model can significantly reduce the operational burden on the organization, allowing internal teams to focus on core business activities. Outsourced SOC providers typically offer a comprehensive range of services, including 24/7 monitoring, incident response, and threat intelligence. These providers leverage

Advantages:

- managed by a third-party provider
- reduced operational burden and costs
- potential challenges with control and data privacy

economies of scale to deliver services at a lower cost than an in-house SOC. However, the market cost of full external SOC services often poses a budgetary challenge for academic organizations which are funded by public money.

One of the primary advantages of an outsourced SOC is access to a broad pool of expertise and advanced technologies. Service providers often have specialized teams with experience in dealing with a wide variety of threats and incidents. They also invest heavily in state-of-the-art security tools and threat intelligence capabilities. However, organizations may face challenges related to control and data privacy. Ensuring that the service provider adheres to the organization's security policies and regulatory requirements is critical. Effective communication and coordination between the organization and the service provider are essential to ensure a timely and effective response to incidents. However, this can also be challenging due to the organization's complex structure.

Hybrid SOC

A hybrid SOC combines elements of both in-house and outsourced models, aiming to leverage the strengths of each of them. In a hybrid SOC, some security functions are managed internally, while others are outsourced to a third-party provider. This approach allows organizations to maintain control over critical security operations while benefiting from the expertise and resources of external partners.

For example, an organization might handle strategic functions such as incident response planning and threat hunting in-house, while outsourcing 24/7 monitoring and initial incident triage to a managed security service provider (MSSP). This model offers flexibility in resource allocation and can be more cost-effective than a fully in-

Advantages

- combination of in-house and outsourced elements
- balances control with cost-effectiveness
- flexibility in scaling and resource allocation

house SOC. It also allows organizations to scale their security operations more easily by leveraging external resources during peak periods or in response to specific threats.

Another example of a hybrid SOC is the concept of “shared services”, understood as cooperation between universities (and possibly other similar organizations) to create a shared SOC for a group of them. This may be done in the form of a SOC

department within one of them, a federated SOC, or as a separate business unit. This model promotes collaboration and resource sharing, which can be particularly beneficial for academic institutions with limited budgets. By pooling resources and expertise, universities can enhance their security posture without the need for each institution to maintain its own fully staffed and equipped SOC.

However, a hybrid SOC requires careful management and integration of internal and external teams. Clear roles and responsibilities must be defined, and effective communication channels must be established to ensure seamless collaboration. Organizations must also ensure that both internal and external teams have access to the necessary tools and information to perform their duties effectively.

Virtual SOC

In this model, the SOC is not centralized in one physical location. The team operates remotely using cloud-based tools and technologies. Unlike traditional SOC, where the

Advantages

- Cost effectiveness with minimal need for physical infrastructure
- Remote flexibility, allowing experts from different locations to collaborate
- Scalability, making it possible to meet changing business requirements

team is housed in a central, physical facility, a virtual SOC relies on cloud technologies and remote collaboration tools to deliver 24/7 security operations, often across different locations and time zones. SOC team members can work from anywhere with an internet connection, offering flexibility to security professionals. With teams spread across time zones, a virtual SOC can provide 24/7/365 security monitoring without requiring personnel to work night shifts in a central location.

Virtual SOC's often rely heavily on automation to manage routine tasks like log analysis, incident triaging, and alerting. This reduces manual workloads and speeds up response times.

On the other hand, storing sensitive security data in the cloud or having remote teams access confidential information might introduce data privacy and regulatory concerns. Cloud-based solutions need to be properly secured to avoid potential breaches or misconfigurations that can lead to data leaks.

Other SOC models

The following SOC models are not directly useful for most of the universities, as they are a better fit for larger, multi-national companies. They are included here only to give a broader picture of the implementation possibilities.

Federated SOC

This model involves multiple SOC's located in different geographical regions, all working together under a unified governance framework.

Advantages:

- Global coverage, able to monitor threats and incidents across time zones
- Distributed resources for resilience and scalability
- Better insight into region-specific threats and regulations

Command SOC

This model acts as a central hub for multiple regional or department-specific SOC's. The Command SOC oversees operations, sets policies, and coordinates the overall security strategy.

Advantages

- Centralized control with local execution of security tasks
- Global threat intelligence sharing and streamlined coordination
- Scalability for large enterprises

1.3. Location of the SOC in the organizational structure

In the organizational structure of a higher education institution, the SOC plays a critical role in maintaining cybersecurity.

Ideally, the SOC should be positioned directly under the governing body, such as the university's executive leadership or board of directors. This placement underscores the importance of cybersecurity and ensures that the SOC has the necessary authority and visibility to address security threats effectively.

The SOC should operate within a dedicated security unit that is distinct from, yet closely collaborates with, the IT department. This separation ensures that the SOC can maintain an independent focus on security operations without the potential conflicts of interest that might arise from being part of the IT department. However, close collaboration with IT is essential because the SOC relies on IT infrastructure and systems to monitor and respond to threats. This structure ensures that the SOC has the necessary authority, focus and resources to protect the institution's digital assets while fostering a cooperative environment with IT to address potential threats comprehensively, enabling a thorough and prompt incident response.

In many places, especially smaller or less mature, the SOC team will be placed inside an IT department or, less often, a risk or compliance team. While the SOC can be part of the IT department, it serves a specialized role focusing on cybersecurity. It collaborates with IT teams, but has a distinct mission centered around protecting the organization from cyber threats.

1.4. Interdependencies with other departments

In each organization, not excluding higher education institutions, the SOC must work closely with various departments to ensure a robust cybersecurity posture.

The effectiveness of the SOC is significantly enhanced through its interdependencies with the IT department, GDPR officers, and the legal department. These relationships are crucial for a comprehensive and proactive approach to cybersecurity.

The IT department is a critical partner for the SOC. Given that the SOC relies on the IT infrastructure for monitoring, detecting, and responding to security threats, seamless collaboration between these two units is indispensable. The IT department provides the technical backbone that the SOC needs to operate effectively. This includes network configurations, system logs, and access controls that are essential for threat detection and response. The IT team's deep understanding of the institution's technical environment aids the SOC in quickly identifying and mitigating potential security incidents. Regular communication and coordination between the SOC and the IT department ensure that security policies are properly implemented and that both teams are aligned in their objectives.

GDPR officers, or data protection officers, play a vital role in maintaining compliance with data protection regulations. Their collaboration with the SOC is essential for ensuring that the institution adheres to legal requirements related to data privacy and security. The SOC needs to work closely with GDPR officers to ensure that any data breaches are handled in accordance with the relevant regulatory requirements, including timely reporting and appropriate mitigation measures. This partnership helps in developing and enforcing policies that protect personal data and ensures that the institution remains compliant with the GDPR regulations and other relevant data protection laws. The expertise of GDPR officers in data privacy issues provides valuable guidance to the SOC in managing sensitive information securely.

The legal department is another indispensable partner for the SOC. Cybersecurity incidents often have legal implications, and the SOC must be prepared to navigate these complexities. The legal team provides crucial support in interpreting laws and regulations related to cybersecurity, intellectual property, and data protection. They

assist in drafting incident response plans that include legal considerations and ensure that the institution's actions during and after a security incident are legally sound. Collaboration with the legal department is also vital in the event of litigation or investigations, where the SOC's activities and findings may be scrutinized. This partnership ensures that the institution's response to cyber incidents is not only effective but also compliant with legal standards.

The interdependencies between the SOC, IT department, GDPR officers and legal department create a comprehensive security framework. This collaborative approach allows for a more thorough understanding of the threat landscape and enables a coordinated response to incidents. Each department brings unique expertise and perspectives that enhance the SOC's ability to protect the institution's digital assets. Regular cross-departmental meetings, shared training sessions, and joint policy development are strategies that can strengthen these interdependencies.

Furthermore, incident response process requires cooperation with various additional internal parties: the PR department, management (which, in the case of Academia, is usually the Rectorate), heads of departments and faculties, physical security officers and human resources officers. These are usually not constant, day-to-day interactions, but they still need to be considered when the SOC is developed.

References

- [1] "How to set up CSIRT and SOC," ENISA, <https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc> [Accessed ...]
- [2] "Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02)," Don Murdoch. Independently published.

2. Maturity models for SOC-s

Maturity models are structured frameworks that help organizations assess, improve, and manage their capabilities and processes over time.

They typically outline a progression through various stages of “maturity”, where higher levels represent more advanced and effective practices. Maturity models are widely used in areas such as software development, project management, and IT, among others, to guide continuous improvement and organizational development.

Key Features of Maturity Models

1. **Stages or Levels:** Maturity models are usually composed of several levels (often 4-6), each describing an organization's capabilities or practices at a specific stage of maturity. Moving from lower levels to higher ones signifies improvement in performance, efficiency, and consistency.
 - a. **Initial (Ad hoc):** Processes are unstructured and chaotic, with success depending on individual efforts;
 - b. **Repeatable:** Basic processes are established and can be repeated with some consistency;
 - c. **Defined:** Processes are documented, standardized, and integrated across the organization;
 - d. **Managed:** Processes are measured, monitored, and controlled;
 - e. **Optimized:** Processes are continuously improved through innovation and proactive optimization.
2. **Assessment:** Organizations can evaluate their current state against the model's levels to identify where they stand and what gaps exist between their current practices and higher maturity levels.
3. **Guidance for Improvement:** Maturity models provide a roadmap for growth. They often include best practices, processes, or capabilities that need to be developed to move from one level to the next.
4. **Scalability:** Maturity models can apply to an entire organization or be specific to departments, functions, or particular processes, such as IT, data management, or innovation.

Examples of Maturity Models

- **Capability Maturity Model (CMM):** Developed for software development, it assesses the maturity of software engineering processes.
- **CMMI (Capability Maturity Model Integration):** Extends the CMM to other business processes beyond software development, such as product development and service delivery.
- **Project Management Maturity Model (PMMM):** Assesses the maturity of an organization's project management practices.

Benefits of Maturity Models

- **Structured Improvement:** Provides a clear, step-by-step path for enhancing processes and capabilities;
- **Benchmarking:** Organizations can benchmark themselves against industry standards or competitors;
- **Risk Reduction:** Higher maturity levels often correlate with lower risks, as processes become more predictable and controlled;
- **Strategic Decision-Making:** Enables leadership to make informed decisions about where to allocate resources for the greatest impact.

For the purposes of SOCCER, we have selected the SIM3 maturity model as a suggested tool for assessing the maturity of the SOC.

2.1. Connection to SIM3 (Security Incident Management Maturity Model)

SIM3 is one of the most popular maturity models across the globe. The first version of SIM3 was published by the Open CSIRT Foundation (OCF) in 2008. As explained in [1], SIM3 is designed as a generic maturity standard that applies to all types of CSIRTs, including national CSIRTs. The level of maturity in a CSIRT reflects the team's effectiveness in governing, documenting, executing, and assessing its functions.

SIM3v2i parameter measurement scale

- 0 = not available / undefined / unaware
- 1 = implicit (known/considered but not written down, 'between the ears')
- 2 = explicit, internal (written down but not formalised in any way)
- 3 = explicit, formalised on authority of the CSIRT head or above (rubberstamped or published)
- 4 = explicit, audited on authority of governance levels above the CSIRT head (subject to control process/audit/enforcement)

ENISA had previously established a three-tier maturity approach, consisting of the Basic, Intermediate, and Advanced steps. Each of the three steps is associated with a minimum value assigned to each of the forty-five parameters. Consequently, certain parameters may be more pertinent to some national teams than others, and it is the responsibility of the respective teams to determine the weighting of these parameters.

SIM is built on 4 main pillars:

- Prevention
- Detection
- Resolution
- Quality control & feedback

SIM3 version 2 interim replaces the original SIM3 version 1, which was in use from 2008-2022 [2].

SIM3 v2i includes forty-five parameters, i.e., one additional compared to SIM3 v1. These parameters represent attributes pertinent to the organization, operation, or functioning of a CSIRT and they are divided into the following 4 categories [3]:

O: Organisation

With Organisation, we refer to the ensemble of humans, resources, tools and infrastructures that work together in a planned manner. The objectives or aims of an organisation are directed by a set of specific strategic goals. As SIM3 focuses on the maturity of the management of security incidents, we need to distinguish between the strategic goals of the whole organisation and, on the other hand, the (service) specific strategic goals related to that part of the organisation that manages security incidents - commonly referred to as 'CSIRT'. The following 'O' Parameters refer to the mandate, setup, and services of that CSIRT, and the framework connecting all organisational aspects.

O-1: Mandate

The official description of the parameter from the SIM3v2 [3]:

Your CSIRT needs to derive the justification for its existence, its assignment from some higher level of governance. This is called the CSIRT mandate. Ideally, the mandate comes from the highest governance levels in your specific environment. Sometimes it initially comes from a lower level, like the company's head of IT, or the leadership of a ministry. But preferably it comes from the highest levels, like the board of directors, or state government - and in the latter case it can also be anchored in legislation. Does your CSIRT have such a mandate?

Maturity levels:

1. *We never really discussed this and we don't formally know our mandate or assignment. We just do our work.*
1. *We have a pretty good idea that we are doing is what we were assigned to do, but it was never written down.*
2. *We don't have a formal written mandate, therefore we wrote something for our own purposes. Our team management has not formally approved this.*
3. *We have a written mandate approved by our team management.*
4. *We have a written mandate from higher management that our team management regards as authoritative. In the periodic review of our team it is checked if and how we fulfil our mandate.*

The CSIRT's assignment is derived from upper management [4]. Many CSIRTs lack a clear understanding of their goals or fail to effectively communicate them to stakeholders, leading to unnecessary effort and confusion, especially during crises. Without a concise mission statement, CSIRTs struggle with setting priorities, managing expectations, and determining appropriate responses. A well-defined mission statement, supported by senior management, is essential for guiding the CSIRT's goals, services, policies, and procedures. It ensures that the CSIRT aligns with the broader organization's mission and secures necessary resources. Additionally, a purpose statement can clarify why the team was established, helping define its goals and services. Making these statements public enhances understanding and collaboration with external parties.

O-2: Constituency

The official description of the parameter from the SIM3v2 [3]:

Your CSIRT's constituency is defined as the 'client base', the target group for who you do the CSIRT work. This constituency can be your own organisation or company - then it is said that your constituency is internal to your organisation. Your team can also have a constituency external to your own organisation, like for instance your country's universities when you serve the academic community, or a paying customer base, or all municipalities in your country. Does your CSIRT has a well-defined constituency?

Maturity levels:

1. *We never really discussed this.*
1. *We know our constituency, but it was never written down.*
2. *We don't have a formal written constituency definition, therefore we wrote something for our own purposes. Our management has not formally approved this.*
3. *We have a written constituency definition approved by our team management.*
4. *We have a written constituency definition approved by our team management. In the periodic review of our team it is checked if and in how far we serve this constituency, and whether the definition needs to be adapted.*

The description of the O-2 parameter from the [4] simply says that the constituency is where the CSIRT functions are aimed at – the “clients” of the CSIRT. The Constituency Parameter refers to the definition, scope, and understanding of the group or entities that the team is responsible for protecting and serving. It plays a critical role in determining how effectively the CSIRT can respond to and manage security incidents. It is essential because it directly impacts the mission, services, and response strategies of the team.

The constituency of a CSIRT encompasses the organizations, departments, users, or systems that fall within its area of responsibility. Constituents can be internal (e.g., within a company or institution) or external (e.g., across sectors, nationally, or globally). The constituency must be clearly defined and documented, ensuring all stakeholders, including the CSIRT members and constituents, understand the CSIRT's boundaries and responsibilities. A mature understanding of the constituency allows the CSIRT to operate more efficiently and improve its services over time.

For example, in the context of a university environment, the constituency of a university CSIRT typically includes its students and staff, the university network defined by its range of IP addresses, and the associated domains under its administration.

The Constitution section is formally included and described as part of the Request for Comments (RFC) 2350 document for CSIRT teams, which should be publicly accessible for review. The definition of the constituency should create a perimeter around the group to whom the team will provide service. If a CSIRT decides not to disclose its constituency, it should explain the reasoning behind this decision [5].

How to define a constituency, what the relationship between the constituency and the CSIRT team might look like, and how to gain the constituency's trust is thoroughly described with examples in the document Handbook for Computer Security Incident Response Teams (CSIRTs) [6].

O-3: Authority

The official description of the parameter from the SIM3v2 [3]:

*The authority of a CSIRT is what your team is *allowed* to do towards your constituency, so that you can fulfil your mandate. The authority is basically the powers that have been invested in your CSIRT. Some teams, like especially coordinating teams with an external constituency, have little powers, little authority and can perhaps only give advice to the constituency. Whereas others CSIRTs have the authority to enforce measures. What and how you can escalate, is also part of this. The whole purpose of this Parameter is to help ensure that the CSIRT has a clear and distinct description of their authority, which can serve as support in the back especially in crisis cases. It is important to realise that the authority of any CSIRT needs to come from higher governance, or else there will be no high-level support for the team in cases where the “power” needs to be used. For the example of a national CSIRT, if the national cyber security law provides clarity on their authority, so much the better U+2013 however, if the law is not very specific, then the CSIRT should make sure that the authority is defined more precisely, starting from the law. What authority does your team have?*

Maturity levels:

1. *We never really discussed this.*
1. *We know our authority, but it was never written down.*
2. *We don't have a formal written authority definition, therefore we wrote something for our own purposes. Our management has not formally approved this.*
3. *We have a written authority definition approved by our team management.*
4. *We have a written authority definition approved by our team management. In the periodic review of our team it is checked if and how we align with this authority, and if it is sufficient to meet our mandate.*

The Authority Parameter in SIM3 refers to the extent of the decision-making power and autonomy granted to the CSIRT in managing security incidents. This parameter evaluates whether the CSIRT has the authority to take necessary actions during an incident, such as escalating issues to higher management, implementing incident response measures, allocating resources, and engaging with external entities like law enforcement or third-party vendors. It is crucial for the CSIRT to operate effectively and respond promptly to incidents without unnecessary delays due to hierarchical constraints. A well-defined authority structure empowers the team to act decisively, ensuring a more efficient and effective incident response.

O-4: Responsibility

The official description of the parameter from the SIM3v2 [3]:

*The responsibility of a CSIRT is what your team is *expected* to do and perform towards your constituency, so that you can fulfil your mandate. Basically, the responsibility is a high-level version of what is detailed below in the team's services (O-5). In almost all cases a team has more responsibility than authority. An example: a team may well be responsible for checking out if new threats could hurt their constituency, e.g. by doing non-interruptive port scans. But that's not to say that the team has the authority to go beyond “non-interruptive” scans - or indeed that if the team finds such vulnerabilities, that it can 'order' the constituents in question what to do: this will often be in the form of advice, not enforcement. A situation to avoid is where a team's authority is very small - but their responsibility very big. If the gap between O-3 and O-4 becomes too big, then a team is more or less expected to do many things, without having the power to actually make them work. That is a recipe for malfunctioning. There is a natural gap between O-*

3 and O-4 but it should not become too big. What responsibility does your team have?

Maturity levels:

1. *We never really discussed this.*
1. *We know our responsibility, but it was never written down.*
2. *We don't have a formal written responsibility definition; therefore we wrote something for our own purposes. Our management has not formally approved this.*
3. *We have a written responsibility definition approved by our team management.*
4. *We have a written responsibility definition approved by our team management. In the periodic review of our team it is checked if and how we meet this responsibility.*

Responsibility refers to the actions a CSIRT is expected to take in relation to their constituency to fulfil their role. The Responsibility Parameter refers to the clarity, definition, and allocation of responsibilities of and within a CSIRT. This parameter is crucial for ensuring that the team functions effectively and that security incidents are managed in a structured and accountable manner. A CSIRT benefits when its purpose and competencies are clearly defined and backed by the organization's management. The responsibilities of a CSIRT can be outlined in a document that details the scope of each unit within a larger organization or in a separate document dedicated to the CSIRT.

The main responsibility of any CSIRT team is incident response. However, there are many other responsibilities that are also important. *Computer Security Incident Response Team (CSIRT) Handbook* [6] is a guide on setting up computer security incident response teams, which lists the tasks that a CSIRT should handle, with a description of each task. These tasks are divided into three groups: reactive, preventive and quality improvement.

- Reactive tasks involve addressing active incidents, such as coordinating response efforts or assisting in system recovery;
- Preventive tasks aim to reduce potential attack vectors, such as through vulnerability testing or raising security awareness;
- Quality improvement tasks focus on activities like education and analysis to enhance overall security posture.

These responsibilities are also discussed in *Introduction to Computer Security Incident Response Teams (CSIRTs): Structure and Functions of Cybersecurity First Responders* [7].

O-5: Service Description

The official description of the parameter from the SIM3v2 [3]:

Whereas 'responsibility' is usually formulated as a high level form of expectations of your CSIRT, the description of your team's services are the way you further shape that into a concise list of services that you offer to your constituency, which will most likely include incident management/response, but also possibly vulnerability handling, malware analysis, awareness raising and potentially others. The original most popular listing of possible services to select from was the one from CERT/CC's CSIRT Handbook (also adopted by ENISA and Trusted Introducer). Since 2017, the FIRST CSIRT Services Framework has become a de-facto standard, because it offers a well-structured and granular approach, especially in its latest 2.1 version. Whichever source you use, it is important to make a clear selection of those services you must or should offer based on your mandate, authority and responsibility - and taking into account the resources you have available.

It is essential to note here that the concept of O-5 is only to ask, “have you defined your services towards the constituency, and what's the result”. Detailing what those services should or should not include is up to the team, SIM3 makes no specific demands (although of course in other parameters it is assumed that every CSIRT at least deals with Incident Management as a service). The best way of using SIM3 and the FIRST CSIRT Services Framework as complementary standards is by looking at it like this: SIM3 serves as the overall maturity standard for the CSIRT, and can be visualised by a horizontal line with over 40 Parameters as tick marks on that line. On O-5 a vertical line intersects the SIM3 horizontal line: that vertical line is the visualisation of the FIRST CSIRT Services Framework, which every team is strongly recommended to use to map their services portfolio in detail.

*All of this then leads to a list of services, and it is important to consider that at least your constituency needs to have access to this list, including your team's contact information and service windows. It is strongly advised to use RFC2350 as a standardised way to publish a high-level list of their services, contact info and service windows even to the Internet at large, as for any CSIRT it is important that it is known how to reach them, as they take responsibility for (part of) the security of their constituency, which is part of the wider Internet - **when adopting RFC2350 make sure to have an English version publicly available** (next to one in your native language). Does your team have a clear service description?*

Minimum Requirement: Contains the CSIRT contact information, service windows, concise description of the services offered and the CSIRT's policy on information handling and disclosure. Publicly available in English.

Maturity levels:

1. *We never really discussed this. We just do our work.*
1. *We know what services we offer, but it was never written down.*
2. *We don't have a formal written service description, therefore we wrote something for our own purposes. Our management has not formally approved this.*
3. *We have a written service description approved by our team management, and it has been made available to our constituency.*
4. *We have a written service description approved by our team management, and it has been made available to our constituency. In the periodic review of our team, it is checked if and how we provide these services.*

As already mentioned in the description of the parameter, the document *The Computer Security Incident Response Team (CSIRT) Services Framework* [8] provides a suitable document for getting oriented in the matter of the possible services provided. It is a structured document outlining a collection of cybersecurity services and related functions that CSIRTs and similar incident management teams may offer. Its mission is to support the establishment and improvement of CSIRT operations, particularly for teams selecting, expanding, or refining their service portfolios. While the framework lists potential services, no CSIRT is expected to provide all of them; each team must choose services aligned with its mission and mandate. The framework categorizes services and their subcomponents, offering standardized terms and definitions for consistency across the community.

The services are divided into 5 basic Service Areas:

1. Information Security Event Management
2. Information Security Incident Management
3. Vulnerability Management

4. Situational Awareness
5. Knowledge Transfer

Each area is assigned to specific services along with their functions, which is an activity or a set of activities aimed at fulfilling the purpose of a particular service.

O-6: Public Media Policy

The official description of the parameter from the SIM3v2 [3]:

Your team needs to be able to interact with the press, and other public media. That is sometimes done together with a communications department, or press office - sometimes directly. This also depends on the kind of public media: dealing with the press is different from working with social media for instance. A public media policy will identify the various public media that are used, and how to deal with each of those. But this policy can also describe how to interact under specific circumstances, like for instance a big incident or crisis, an awareness raising campaign, or when e.g. the press wants to contact you instead of you reaching out to them. Does your team have such a public media policy?

Remark: *This parameter is not applicable when assessing/auditing teams based on SIM3 v1 (2008-2021) for FIRST or TI, in which O-6 does not exist yet. Please choose 'O' as level and the parameter will have no effect.*

Maturity levels:

1. *We never really discussed this. We would just handle this ad hoc.*
1. *We have an idea how to interact with public media, but nothing in writing.*
2. *We don't have a formal written public media policy, therefore we wrote something for our own purposes. Our management has not formally approved this.*
3. *We have a written public media policy approved by our team management.*
4. *We have a written public media policy approved by our team management. In the periodic review of our team it is checked if and how we have interacted with the public media.*

Communication during the handling of an incident is essential for a proper and reactive resolution of the incident. Proper external communication is as important as communication between team members during the incident handling. Media interest is not anticipated in smaller scale incidents but is likely in larger scale occurrences. For this reason, it is necessary to have a pre-established procedure for media communication as well as a designated person who will be the media relations officer (communications department or press office) before the incident occurs, so that no mistakes can be made in any situation.

Depending on the time parameter, we can talk about 2 possible cases of interaction with the media discussed in this section, specifically the moment when the information is made public and how it is disclosed. For instance, if an organization is affected by a data leak, and these employee details (whether login details or personal information about the person such as date of birth, salary level, job title, etc.) have been published on online forums and the media has been notified, the response time to media communication decreases rapidly. The rule for all staff involved in the case of media interest is not to communicate with the media in person; any questions should be forwarded to the press department. Under no circumstances is it appropriate to take any information to the media as a private person. When it comes to the official statement of the organisation, the goal is to provide as limited information about the incident as possible, providing

only the most necessary information as well as the current progress and potential impacts. In the second, more straightforward case, the organisation itself is the primary 'whistleblower' on the details of the incident when the media can be informed in a timely and appropriate manner.

O-7: Service Level Description

The official description of the parameter from the SIM3v2 [3]:

When defining services that your CSIRT offers, it is useful to also set service levels for those services. What can your constituents expect of you in that regard? What can other CSIRTs expect of you? The simplest service level is some measure of the amount of time in which to send a first (human) reaction to an incoming incident report - SIM3 sets a minimum level here, it is mandatory to send a human reaction to peer teams within two working days (peer teams are those CSIRTs you have a well-defined relationship with, like being members of the same CSIRT cooperation or forum). Service levels can also be more detailed 'SLA' type demands, and can then also depend on the type, severity and priority of incidents (as e.g. defined in Parameter O-8, incident classification). Based on incident type and severity, different reaction times can be defined, but also e.g. the percentage of incidents that needs to be dealt with within a certain set amount of time. Does your CSIRT have a service level description?

Minimum Requirement: *Specifies the speed of reaction to incoming incident reports and reports from constituents and from peer CSIRTs. For the latter a human reaction within two working days is the minimum expected.*

Maturity levels:

1. *We never really discussed this.*
1. *We have a basic understanding of the level of service expected of us, but it was never written down.*
2. *We don't have a formal written service level description, therefore we wrote something for our own purposes. Our management has not formally approved this.*
3. *We have a written service level description approved by our team management.*
4. *We have a written service level description approved by our team management. In the periodic review of our team it is checked if and how we meet our service level(s).*

As part of this section, it is necessary to have defined reaction periods for specific types of incidents. In fact, when responding to an incident, we are referring to the reaction time in which the first response is sent. For organizations of different sizes, this can vary rapidly depending on, for example, the number of employees or the services being provided in which time range. For this reason, each organisation should determine, to the best of its ability, the reaction time that should be met when an incident notification is received. For minor incidents, such as the compromise of an unprivileged account of an employee without higher privileges, this period would range within a few hours. Incidents such as a reported vulnerability in a service/on a device, or an active network scan will be in larger time ranges. At this point, it is important to be aware of 2 facts that may have an impact when deciding to estimate the number of hours to be allocated: one is the severity of the incident from minor to critical, while the other is the priority of the incident. The following article from Atlassian discusses this topic [9]. When receiving less severe incidents, it is possible to prioritize them in one sequence as long as another incident of higher priority occurs during the handling of the first one. As an example of this scenario, consider the compromise of an account held by an employee responsible for finances in an organization against the suspicion of malware. In general, a malware

infection is often categorized as a more serious security incident, but, in this case, prioritization is needed. The reason is that when the employee in consideration is compromised, we are more likely to speak of financial losses as well as losses to the reputation of the organization or others. Password resets and logging out of all active sessions should be the primary actions to be taken.

O-8: Incident Classification

The official description of the parameter from the SIM3v2 [3]:

An incident classification scheme usually contains at least a list of technical incident categories to associate an incident or threat with, like whether it has the characteristics of 'spam' or 'root compromise' or 'DDoS' etc. A popular classification scheme of that type is ENISA's 'Reference Incident Classification Taxonomy'.

It is however recommended to also include in such a classification some measure of the potential severity (impact) of an incident or threat - and potentially also its assessed priority (as a high impact threat for instance can be low priority when its probability of happening any time soon is very low). Such more advanced ways of classifying incidents, coupled to the service levels defined in O-7, can help to deal in a structured way with higher incident loads. There are many ways of doing this, but it's advised to first see if the internal organisation already has some kind of severity/priority scheme for IT operations, and then possible adopt that. If you need to build one your own, the strong advice is to keep it simple, because all permutations you create may become visible in your O-7 and in various processes. Does your team have some kind of incident classification?

Maturity level:

1. *We don't classify incidents, we just deal with them.*
1. *We appreciate that there are different types of incidents, but we don't make this explicit. If an incident needs special attention, we just deal with that accordingly.*
2. *We don't have a formal written incident classification, therefore we wrote one for our own purposes. Our management has not formally approved this.*
3. *We have a written incident classification approved by our team management.*
4. *We have a written incident classification approved by our team management. In the periodic review of our team attention is given to the different types of incidents and how we handled those.*

The use and implementation of an incident classification system for documenting reported incidents:

There are several taxonomies of incidents from which one can be selected and adapted to specific needs. Among the most frequently used was the Incident Classification / Incident Taxonomy according to eCSIRT.net – adapted [10]. According to the eCSIRT.net – adapted, Incident Classification or Incident Taxonomy refers to a standardized way of categorizing and describing cybersecurity incidents. This system allows different teams, organizations, and entities to communicate more effectively by using consistent terminology to describe the nature and scope of incidents. The taxonomy includes predefined categories or classes of incidents, such as unauthorized access, a malicious code, or denial of service attacks, along with relevant subcategories. This helps in identifying, managing, and reporting incidents in a clear and organized manner, ensuring that stakeholders across different sectors can understand the type and severity of the security threat. This taxonomy was the basis for the currently used *Reference Security Incident Taxonomy* [11].

This taxonomy is designed to be adaptable and extendable, meaning that organizations can modify or expand the classification system to fit their specific needs while

maintaining a common structure for broader collaboration across the cybersecurity community.

However, as mentioned in the parameter description, it is also important to determine the severity associated with each category. *Cybersecurity Incident Taxonomy* from the NIS Cooperation Group [12] addresses the impact of an incident (on services, in particular sector(s) of the economy and society) in more detail.

Depending on the scope and severity of the impact, security incidents can also be classified as follows:

- a. low severity, which has minimal impact on the operation of the organisation;
- b. medium severity, which has a moderate impact on the operation of the organisation, (compromising a small part of the organisation or the provision of support services);
- c. high severity, which has a negative impact on the running of the organisation (threat to a significant part of the organisation or to the provision of essential services);
- d. critical severity, which has a significant negative impact on the operation of the University (threat to the whole organisation and/or the provision of essential services).

O-9: Participation in CSIRT Systems

The official description of the parameter from the SIM3v2 [3]:

With 'CSIRT systems' we mean well-established cooperations of CSIRTs, like in your country, sector, geographical region or worldwide. Your CSIRT can participate in those either directly, e.g. as member, or you may do so indirectly when you can make use of the services of an 'upstream' CSIRT that participates in such CSIRT cooperations. To be effective as a CSIRT, it is necessary to engage in this kind of participation, as the CSIRT community at large depends on this cooperation between teams. It is important to realise that this participation is crucial on various levels: inside a country for instance, it is necessary to create a CSIRT network, which includes the national CSIRT, plus CSIRTs defending the various parts of critical infrastructures, and also including the healthcare sector and research/education; in geographical regions it is also pragmatical and fruitful to come together (e.g. initiatives like or inside TF-CSIRT, APCERT, OAS, LACNIC, AfricaCERT, TBA, OIS-CERT, ASEAN, and so on); and last but not least participation in global fora like FIRST, or in CSIRT initiatives taken by the GFCE, ITU, African Union and others. Where the focus of your team's participation will be, depends fully on the type and scope of your team. Does your team participate in such cooperations directly, or indirectly via an upstream CSIRT?

Maturity levels:

1. *We never really discussed this.*
1. *We know in what CSIRT co-operation(s) we participate, but it was never written down.*
2. *We don't have a formal written statement on the CSIRT co-operations we participate in, therefore we wrote something for our own purposes. Our management has not formally approved this.*
3. *We have a formal written statement on the CSIRT co-operation(s) we participate in, approved by our team management and budget supported.*
4. *We have a formal written statement on the CSIRT co-operation(s) we participate in, approved by our team management and budget supported. In the periodic*

review of our team it is checked if and how actively we participate in these co-operations, and what the benefits are.

Collaboration between organisations or teams as a whole is crucial in handling incidents as well as sharing various information and more. The importance of communication and proper communication has already been discussed in O-6. When talking about cooperation on a national or worldwide level, there are a large number of organizations that can be joined in to share common ideas and opinions. Various organizations may have different conditions of entry and may have different requirements for regular contributions, depending on the scope of the issue. This may include regular online/ face-to-face meetings dedicated to the topic with the possibility of contributing one's own solutions or ideas that may be beneficial to the community. Examples of larger organisations might include the European organisation for the European CSIRT community - TF-CSIRT [13], as well as FIRST [14], which has over 700 members spread over Africa, the Americas, Asia, Europe and Oceania. However, in the case of CSIRTs, building relationships at the national level by collaborating with other CSIRTs or teams focused on the area of security is equally valuable.

O-10: Organisational Framework

The official description of the parameter from the SIM3v2 [3]:

What we call a 'team charter' or 'organisational framework' for your CSIRT, is a consolidated controlling document for your team, describing who/what your team is, who you work for, what is expected of you and how this was mandated. This charter should include at least the SIM3 Parameters O-1 to O-9 and potentially a few more. Ideally, this charter has been approved by the same governance level that mandated your CSIRT. The great use of having such a consolidated write-up of O-10 is that this is indeed the high-level "charter" of any team the controlling document describing all the foundational issues for which the approval of higher governance is needed and can serve as a reference from then on for the functioning of the team, for audits, etcetera.

O-10 is not necessarily only ONE document, though it is generally beneficial to have the foundational O-Parameters described in one document. Your team's charter is normally an internal document - therefore RFC2350, which is basically meant as public service description of your team, is not suitable as team charter - also RFC2350 is much more limited in scope than the charter is. If O-10 consists of more than one document, RFC2350 can be part of O-10 (but not all of it). For the example of national CSIRTs, most of O-10 can be in the national cyber security law - yet even then it can be very useful to re-iterate the O-10 related aspects in a charter on the team wiki, with the proper references.

There is one more variation that is worth mentioning: some CSIRTs decide to expand the charter document to comprise most or all SIM3 Parameters, thus creating what is often called a CSIRT handbook. The advantage of that approach is that all Parameters are described in one consolidated document - the flip side is that to get approval for such a handbook from the highest governance levels, means you also need to get high-level approval for all the more team-internal items like tools and processes, which may make version management more of a challenge. Does your CSIRT have such a charter?

Minimum Requirement: Describes the team's mission and Parameters O-1 to O-9 by either providing references to specific documents or combining the required details in a single document.

Maturity level:

1. *We never really discussed this.*
1. *We do have a coherent view on our organisational set-up, but it was never written down.*
2. *We don't have a formal written charter, therefore we wrote something for our own purposes. Our management has not formally approved this.*
3. *We have a written charter approved by our team management.*
4. *We have a written charter approved by our team management. In the periodic review of our team, it is tested if the charter is up-to-date and effective.*

To meet this parameter, it is necessary combine O-1 to O-9 into a unified framework document that acts as the authoritative guide for the CSIRT. At a minimum, it outlines the CSIRT's mission and defines the parameters of O-1 to O-9. The statement will offer a basic understanding of the team's objectives and, more importantly, will provide a clear focus for the overall goals and priorities of the CSIRT. A mission statement is essential for the CSIRT to establish a service and quality framework, defining the scope and nature of services offered as well as its policies, procedures, and service standards. If the team operates within a larger organization or is funded by an external entity, the CSIRT mission statement must align with the missions of those organizations.

As highlighted in [6], it is important to have the backing and support of senior management in the parent organization (e.g., the corporate security officer, head of information technology, board of directors, or equivalent). Without such backing the CSIRT will struggle to obtain recognition and resources.

O-11: Security Policy

The official description of the parameter from the SIM3v2 [3]:

Your CSIRT is usually embedded in a host organisation. That host organisation will have information security and business continuity (BCM) policies, that will also apply to your team. Though often information security and business continuity are treated separately, it is more logical in the context of IT/cyber to have business continuity as an integral part of a good security policy, and that is the approach we take here. So when we say 'security policy' this includes such important aspects as 'availability', and how to get back to normal after disruptions - but the landscape is even broader than that, thought also needs to be given to site security and resilience, and workspace security and resilience. Two important notes must be made here:

There are some other BCM related aspects that surface in other SIM3 Parameters. Specifically in H-2 which is about staff resilience, and T-5 to T-7 which are about the resilience of basic CSIRT tools.

As a CSIRT, you often have IT/security/BCM requirements that differ from the normal ones - like you may want to be able to run tests without a firewall blocking those tests, or to receive e-mail without spam/malware filtering, you may want to place a honeypot somewhere, or you may need to be able to use encryption software like GPG or perhaps you need to have a dedicated Internet connections for back-up reasons, testing, etcetera. Such special CSIRT requirements often make it necessary that additional to your host's organisation security policy, your CSIRT also has its own security policy (again including the aspect of BCM). Of course, when you are a stand-alone CSIRT without host organisations (meaning: you are your own host organisation), the same arguments apply.

Does your CSIRT follow a set security policy, or security policies (including BCM aspects), whether your own and/or of your host organisation?

Maturity levels:

1. *We never really discussed this.*
1. *We know the kind of security limitations that apply, but those were never written down.*
2. *We don't have a formal written security policy that applies to us, therefore we wrote something for our own purposes. Our management has not formally approved this.*
3. *We have a written security policy that applies to us, approved by our team management.*
4. *We have a written security policy that applies to us, approved by our team management. In the periodic review of our team it is checked if we meet this policy and if it works for us.*

It is advisable to have adopted internal IT/security requirements that each employee is required to follow. This may involve a set of mandatory and recommended actions required during work. The following recommendations may contribute to the development of such a security framework:

- work on secure computers that are encrypted using full disk encryption (e.g. BitLocker, FileVault), with the security benefit that if the computer is lost/stolen/sold/serviced; all the data will be protected from unauthorised access/copying
- use SSO (Single Sign-On) to access key systems, whereby all access to these systems is protected by two-factor authentication enforced by security policy
- secure internal communication by encryption
- hardening the browser, with the effect of blocking all scripts and frames on third-party domains
- use password manager for storing and generating passwords
- have signed a non-disclosure agreement when working with personal data

An additional recommended practice is to keep accounts of the team members under security monitoring as well as the accounts of other employees. It is also recommended to implement on-boarding and off-boarding policies and procedures. As part of the termination policy, access to repositories, communication channels and accounts should be blocked when an employee leaves. The team members are expected to have a consistent form of their official signature, which should be included at the end of every email message sent. Another related aspect is signing email messages with an electronic signature. An electronic signature (EP) puts a signed electronic document on the same level as a physically signed document. For this reason, the use of electronic signatures (similar to email encryption) is recommended.

H: Human

With **Humans** we refer to the people working together to provide the services described in the Organisation area and satisfy the mandate. All people contributing to the goals of the (CSIRT) organisation that manages security incidents require a technical and/or management-oriented education with considerable on-the-job training plus additional training for more detailed expertise like malware analysis or forensics. The 'H' Parameters in this area are about the factors of importance in regard of the most important factor in any CSIRT: the human 'capital' of the people working there.

H-1: Code of Conduct/Practice/Ethics

The official description of the parameter from the SIM3v2 [3]:

Does your CSIRT provide guidance, guidelines or sets of rules for its team members on how to behave professionally, in an ethical manner? Often called a 'Code of Conduct (CoC)' a 'Code of Practice (CoP)' or 'Ethics guideline', it can provide golden rules on confidentiality, trustworthiness, and other key human qualities expected from CSIRT team members. Note that in most cases the CSIRT's host organisation will have some kind of ethics code, but such codes are of a generic nature and have nothing to do with the specific work that the CSIRT does - therefore such generic codes are not valid to satisfy H-1. The CSIRT regularly deals with highly sensitive data, and communicates not just inside the host organisation, but also outside. Also, responsible behaviour of CSIRT team members is not limited to the work context, but also relevant in private circles where security is concerned. The Trusted Introducer CSIRT Code of Practice (TI CCoP) can be used as CoP baseline, as it was written specifically for CSIRTs; another excellent starting point is 'EthicsFIRST' made by FIRST, which has its own website. That said, specific CSIRT cooperations, or even specific teams, can have good reasons to make their own code. Do note that proper alignment with the security policy (O-11) is always necessary. Does your team support such a code of conduct/practice/ethics?

Maturity levels:

1. *We never really discussed this.*
1. *We know what kind of work ethics are expected of us, but they were never written down.*
2. *We don't have a formal written code of conduct, therefore we wrote something for our own purposes. Our management has not formally approved this.*
3. *We have a written code of conduct approved by our team management.*
4. *We have a written code of conduct approved by our team management. In the periodic review of our team it is checked if and how this code has been used and if it serves its purpose.*

A code of conduct is a set of general rules to be followed within an organisation. These rules should reflect the company's values and its purpose, which can be summarised in the initial section of the document. The code of conduct should also set out the principles to be followed by individual members when working with sensitive data or on a day-to-day basis. This document is required to be signed by each employee when taking up a new employment or when changes in key responsibilities occur and should be reviewed periodically.

It is also recommended to state the cooperations within other organisations/entities and what are the mandatory and suggested elements that need to be fulfilled based on the cooperation. Laws, regulations or policies relevant to your code of conduct policy should also be included in the case of code violations or reporting possible misconduct. As regards the scope of the document, it should not be too short to avoid possible confusion and at the same time it should not be too long. One section included in the code of conduct should be also devoted to the identification of basic terms and definitions that are commonly used in the organization.

As regards the resources, we refer to the Code of Conduct from the companies Insight [15], CyberArk [16], and CLP [17] as the options to guide you in creating your own code of conduct.

H-2: Staff Resilience

The official description of the parameter from the SIM3v2 [3]:

Does your CSIRT have enough staffing to deal with planned or unexpected team members' unavailability? Such cases include illness, holidays, quitting of job ... Depending on the services offered (O-5) and the service levels (O-7), the number of team members will vary, but ensuring availability in times of crisis must be anticipated. Based on the list of the bare minimum services to deliver in all contexts, it is commonly agreed that three (part-time) team members is an absolute minimum for any team. Note that staff resilience is also an aspect of Business Continuity Management (BCM), which also appears in the O-11, and T-5 to T-7 Parameters. What about the staff resilience of your team?

Minimum Requirement: Three (part-time or full-time) CSIRT members.

Maturity level:

1. *This is outside our scope.*
1. *We do have sufficient people on the job to be resilient, but this was never put down in writing.*
2. *We don't have a formal statement on the number of available CSIRT staff, therefore we wrote something for our own purposes. Our management has not formally approved this.*
3. *We have a formal statement on the number of available CSIRT staff approved by our team management.*
4. *We have a formal statement on the number of available CSIRT staff approved by our team management. In the periodic review of our team it is checked how the staffing situation was, and if there was sufficient resilience.*

To ensure continuous CSIRT staffing during absences such as illness, holidays, or staff turnover, several strategies can be implemented while maintaining the minimum requirement of three part-time or full-time members. Cross-training and skill sharing are essential to ensure that most of the team members are proficient in key incident response tasks. By cross-training staff, it is easier to cover critical roles during absences, preventing disruptions. Additionally, establishing a detailed documentation for all roles helps new or temporary staff to adapt quickly, at the same time ensuring operational continuity.

On-call rotations and proactive scheduling further guarantee availability during critical periods, such as holidays. By implementing a well-structured on-call system, responsibilities can be distributed evenly among team members, balancing workloads and avoiding burnout. Advanced planning for holidays and foreseeable absences ensures that CSIRT operations remain fully staffed, reducing the risk of unexpected coverage gaps.

These strategies combine to ensure that CSIRT operations remain functional and resilient, even with a small team size.

H-3: Skillset Description

The official description of the parameter from the SIM3v2 [3]:

Does your CSIRT have a description of the skills needed on all CSIRT team position(s)? All positions must be defined and include a description of expected team members' skills: this includes technical, knowledge, experience, and soft skills - e.g. communication, team spirit, working under stress, etcetera. Staff development planning (see H-4) can help to fill the gaps in team members' skills. Has your team described the skillsets needed?

1. *We never really discussed this. Our staff are experienced.*
2. *We know what kind of skills we need to have, but they were never written down.*
3. *We don't have a formal written skillset description; therefore, we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a written skillset description approved by our team management.*
5. *We have a written skillset description approved by our team management. In the periodic review of our team, it is checked if this skillset is sufficient to tackle current threats and incidents.*

The minimal (basic level) SIM3 v2i for the H-3 parameter is **2**. It means that you have a document where you have a set and explained list of job roles and their skills that are necessary for the functioning and achievement of the set objectives.

As an example, to handle this parameter, we consider the organisational structure of a bigger CSIRT according to [18].



Figure 1 Example of organisation units for a bigger CSIRT [18]

The excel document *role_description_H-3*, which can be used as a template, is attached as output material to meet the required level for Parameter H-3.

H-4: Staff Development

The official description of the parameter from the SIM3v2 [3]:

Does your CSIRT have a policy for the professional development of their staff? This parameter is about staff development as a whole, probably including but not limited to a training plan for new team members, personal development planning and a catalogue of trainings for existing team members, team building/education schemes, etcetera. Staff development should enable new as well as existing team members to improve their skills, and meet the targets defined in the skillset (H-3) that applies to their

job position. Staff development can take the shape of on-the-job-coaching, internal or external trainings, but also includes peer mentoring schemes (colleagues helping each other to get better at their jobs), management evaluation interviews, and team meetings and internal workshops. Note that H-5 and H-6 zoom in on two important aspects of staff development, important enough to warrant separate parameters, but H-4 is the overarching policy. Does your team have such a staff development policy?

Maturity levels:

1. *We don't offer this kind of training.*
2. *We have ideas about internal training and/or we train team members informally, but we never wrote down anything about training demands, topics or materials.*
3. *We don't have a formal internal training programme, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have an internal training programme approved by our team management.*
5. *We have an internal training programme approved by our team management. In the periodic review of our team it is checked if this internal training programme has been put into action sufficiently to meet the training needs of the team.*

Training for employees provides an important aspect of enriching and acquiring new knowledge. The organization itself, as well as an employee in a particular job position, may develop a training plan for the job position. Internal trainings that every employee has to complete upon starting a new job position can be generalized. It is appropriate to link these trainings to their role and skillset. In this instance, we are referring to a more general workshop focused on the broader area of cybersecurity. Another option is also providing training by more experienced employees on an issue that they are currently focused on and that can benefit other team members. This may also include purchasing training materials, participation in conferences or debriefing (a workshop after external training has been completed). Attending various conferences in particular can serve as a useful resource to continuously learn more and more. Another form of training for all staff can be a post-incident activity debriefing. It serves to both learn from previous failures as well as to improve current processes.

H-5: Technical Training

The official description of the parameter from the SIM3v2 [3]:

Does your CSIRT provide team members with a programme of (external and/or internal) trainings they can take in order to improve their technical or 'hard' skills (as opposed to the 'soft' skills that are the subject of H-6), in order to meet the technically oriented targets asked for in the skillset (H-3) that applies to their job position. This includes new topics or technologies, future security directions, and technological deep dives. CSIRT-related trainings are TRANSITS, trainings delivered by ENISA or FIRST or any of the regional cooperations, or commercial training programs - e.g. CERT/CC, SANS, ... Note that H-5 should be part of H-4, but is so important that it warrants to be a parameter in and of itself. Does your team have such a technical training programme?

Maturity levels:

1. *We have no options, time or money for this kind of training.*

2. *We send people to such trainings when it is necessary, but we have no written policy on this.*
3. *We don't have a formal technical training programme, therefore we wrote something for our own purposes which helps in sending our staff to such trainings. Our management has not formally approved this programme.*
4. *We have a technical training programme approved by our team management, which allows us to send our staff to such trainings.*
5. *We have a technical training programme approved by our team management, which allows us to send our staff to such trainings. In the periodic review of our team it is checked if this technical training programme has been used sufficiently to meet the training needs of the team.*

The importance of training has already been described above, in H-4. In this instance, it is essential to highlight the significance of external training, which is mostly provided by external programmes such as CERT/CC, SANS, etc. These are often more in-depth and elaborate courses, ending with the completion of a certificate. Such trainings are often dedicated to current topic issues in the field of cybersecurity. The requirements may vary in the case of each type course, depending on whether we are referring to an on-going course evaluation where it is necessary to undergo either a general or a practical hands-on tutorial demonstration. The courses can include various videos that can illustrate the content in a graphical form or short questions after each section. The evaluation of a given course may involve answering a set of questions correctly, and a certificate will be issued upon completion. The certificate may be valid for a limited period, which can involve retaking a course or collecting enough credits from other activities. However, it should be emphasized that these are valuable trainings that contribute to a person's educational background in the field. In the case of larger course providers of such trainings, additional study materials are often provided that may offer a different perspective or more in-depth information.

H-6: Soft Skills Training

The official description of the parameter from the SIM3v2 [3]:

Does your CSIRT provide team members with a programme of (external and internal) trainings they can take in order to improve their 'soft' skills (as opposed to the 'hard' skills that are the subject of H-6), in order to meet the soft skills oriented targets asked for in the skillset (H-3) that applies to their job position. All team members should be trained in such soft skills as team building, time management, working under stress, but especially also in (human) communication and presentation: The latter in order to better interact with clients, colleagues, managers, peers, local or foreign authorities, and sometimes also the press. This applies to all sorts of media - e.g. phone, chat, email, social media ... - and all types of communications - e.g. direct talks, meetings, presentations, advisory or report writing, blog posts, tweets and text messages. It applies to formal and informal communications, and not only to work activities, but sometimes also outside work (in compliance with the ethics code H-1). Also there needs to be attention for the fact that although 'normal' communication may cover 90% or more of all situations, crisis communication is different but equally important. Finally, those who may talk to the press, need additional training for that. Note that H-6 should be part of H-4, but is so important that it warrants to be a parameter in and of itself. Does your team have such a soft skills training programme?

Maturity levels:

1. *We have no options, time or money for this kind of training.*

2. *We send people to such trainings when it is necessary, but we have no written policy on this.*
3. *We don't have a formal communication training programme, therefore we wrote something for our own purposes which helps in sending our staff to such trainings. Our management has not formally approved this programme.*
4. *We have a communication training programme approved by our team management, which allows us to send our staff to such trainings.*
5. *We have a communication training programme approved by our team management, which allows us to send our staff to such trainings. In the periodic review of our team it is checked if this communication training programme has been used sufficiently to meet the training needs of the team.*

As communication is needed when any kind of verbal interaction among people takes places, handling and managing communication skills are an inherent part of it. Every person uses certain communication techniques to communicate. Also, in communication, we differentiate between formal and less formal ways. We discuss and will further develop the topic of dealing with the more formal side of communication in this section. For proper communication, there are communication trainings where one can learn to handle certain situations in an appropriate manner, depending on whether we are referring to the written form, such as writing emails and guidelines, or situations such as how to communicate in a telephone conversation. These courses are also useful in managing critical situations, where one learns certain patterns, what words are appropriate to use, how to proceed, all of which will be helpful in real-life situations. The principle in these situations is to keep a cool head and be able to help the person on the other side of the line. For some people, just simply talking to others on the phone can be a stressful situation, as there is no time to prepare after the phone rings. Many organisations provide such training courses in language skills, where even those more advanced can practise their skills and use their experience to improve their linguistic competence.

H-7: External Networking

The official description of the parameter from the SIM3v2 [3]:

Does your CSIRT have a policy to send team members to CSIRT-related or cybersecurity-related meetings? This contributes to the national, sectorial, regional and/or worldwide CSIRT collaboration (the topic of O-9) - and those collaborations are essential for the success and effectiveness of the CSIRT community as a whole. Also, meeting in person creates the foundation for trust relationships with peers, and 'trust' is the cement of the CSIRT collaborations. Does your team have such a policy for external networking?

Maturity levels:

1. *We have no options, time or money for this kind of activity.*
1. *We go to such meetings when we can, but nothing has been written down about it.*
2. *We don't have a formal written statement on our external networking, therefore we wrote something for our own purposes. Our management has not formally approved this.*
3. *We have a formal written statement on our external networking, approved by our team management.*
4. *We have a formal written statement on our external networking, approved by our team management. In the periodic review of our team it is checked if and how actively we pursue our external networking, and what the benefits are.*

According to [4], it simply means going out and meeting other CSIRTs, contributing to the CSIRT system when it is feasible.

Various organizations, such as the Forum of Incident Response and Security Teams (FIRST) [14] and TF-CSIRT (a European task force for incident response team collaboration) [13] promote cooperation among teams and offer valuable resources to support both new and established teams. Fortunately, newly forming CSIRTs no longer need to rely solely on their own experiences or risk making costly mistakes—they can now benefit from the collective knowledge of others to build more effective teams. A CSIRT should aim to promote its services broadly to ensure that its constituency is aware of its existence and to gain recognition within the broader CSIRT community and potential partners.

T: Tools

With Tools, we refer to the collection of programs, applications, services, instruments, and even simple pieces of equipment used by the personnel that we discussed in the Human area to reach the objectives and offer the services defined in the Organisation area. We specifically mean those tools that enable or improve the management of security incidents timewise, quality wise, and/or ensure higher granularity, i.e., enable 'seeing' incidents that may have gone unnoticed before.

T-1: IT Assets and Configurations

The official description of the parameter from the SIM3v2 [3]:

The availability of an up-to-date and sufficiently detailed list of what kind of computer/networking/OT resources the constituency uses, is very important for efficient security incident management. Such a list should include information about hardware, software and OT that the constituency members use. This should include relevant configurations: such more detailed information (including software versions in use) is necessary to deal with threats more effectively. Some organisations use IT assets management (ITAM) for this purpose, and maintain a configuration management database (CMDB). The CSIRT usually does not manage such assets/configuration lists, but does need to have access to them. Maintaining up-to-date and detailed information about the whole IT hardware/software and configuration landscape is challenging, and sometimes even impossible as in the case of coordinating CSIRTs with constituencies who 'run anything you can think of'. The fallback solution is to focus on only the most critical assets - and in such a case it could be the CSIRT itself who collects and maintains that information, in direct communication with their constituency. For national CSIRTs this task is even harder - and there especially a focus on CI(I) assets is necessary. Does your CSIRT have access to IT assets and configurations?

Maturity levels:

1. *We don't really know.*
2. *We have a good idea of the most important IT assets, but there is no list for this.*
3. *We don't have a formal IT assets list, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have access to a formal IT assets & configurations list, and this has been approved by our team management.*
5. *We have access to a formal IT assets & configurations list, and this has been approved by our team management. In the periodic review of our team it is*

checked if this list is useful and sufficiently accurate for the goals of our team.

As part of this topic, proper implementation and maintenance of an asset management within an organization is essential. When referring to an asset, this may involve any software, hardware, etc. that is considered valuable to its owner as well as the organization. Associated with the term asset is the concept of risk analysis, which is performed to evaluate the risks to assets. The association of these assets is used to manage and search within the list. Minimising the time from detection to resolution is important if an incident occurs, so appropriate asset management is key to searching for assets as well as their administrators who are responsible for them (especially in the case of larger organisations). Vulnerability testing can be one approach to obtaining a list of assets in an automated manner. Since the goal is to obtain as detailed list of assets as possible, automated vulnerability testing may be implemented by using a specific vulnerability scan to identify more information.

T-2: Information Sources List

The official description of the parameter from the SIM3v2 [3]:

A very important part of the CSIRT operations is the daily monitoring of all relevant information sources. These sources should include e.g. relevant social media accounts, that publish or distribute valuable information, or IT security related blogs or website services. Both time constrained information as well as longer term observations are important, not only for continuously adjusting the CSIRT operations but also for - and most importantly - the timely and effective reaction to current events. Of course this list needs to be maintained. Does your team have such an information sources list?

Maturity levels:

1. *We don't have any such list. We don't systematically check sources but instead react to incident reports.*
1. *We know our most important sources and check them out, but there is no list for this.*
2. *We don't have a formal list of information sources, therefore we wrote something for our own purposes. Our management has not formally approved this.*
3. *We have a formal list of information sources approved by our team management.*
4. *We have a formal list of information sources approved by our team management. In the periodic review of our team it is checked if this list is useful and sufficient for the goals of our team.*

This parameter evaluates the comprehensiveness and diversity of the information streams available to the CSIRT for effective incident management.

Key elements of the Information Sources List include:

- **Internal Sources:** Logs from network devices, intrusion detection/prevention systems (IDS/IPS), firewall logs, endpoint security tools, and application logs within the organization;
- **External Sources:** Threat intelligence feeds, security advisories, collaboration with external CSIRTs, vulnerability databases, and information from industry partners or government agencies;

- **Automation Tools:** Use of SIEM (Security Information and Event Management) systems, automated log correlation tools, and data aggregation platforms to streamline information gathering.

A more mature CSIRT has a well-rounded and continually updated list of information sources, enabling better situational awareness and faster, more effective responses to incidents.

Examples of possible sources:

- **Shodan** [24]: Shodan is a search engine for internet-connected devices, often referred to as the "search engine for hackers." It scans and indexes publicly accessible devices such as webcams, routers, servers, and more, allowing users to identify vulnerable systems or explore the Internet of Things (IoT). It is widely used by cybersecurity professionals for network reconnaissance and vulnerability assessments.
- **Taranis** (<https://github.com/SK-CERT/Taranis-NG>): Taranis is an open-source threat intelligence management tool used to collect, analyze, and disseminate cybersecurity information. It helps CERTs/CSIRTs manage incident reports, share threat data, and collaborate on security alerts, offering an organized approach to incident response and threat tracking.
- **SocRadar** (<https://platform.socradar.com/>): SocRadar is a cloud-based cyber threat intelligence platform that provides threat detection, attack surface monitoring, and digital risk protection. It helps organizations identify potential threats, vulnerabilities, and exposure points in real time, offering a comprehensive overview of cyber risks through threat intelligence and early warning systems.
- **Have I Been Pwned** [25]: Have I Been Pwned is a free online service that allows users to check if their personal data has been exposed in a data breach. By entering an email address or username, users can see whether their information has been compromised and which breaches it was involved in.
- **MISP** (Malware Information Sharing Platform & Threat Sharing) is an open-source platform designed to facilitate the sharing of threat intelligence, including indicators of compromise (IOCs) and malware analysis data. It helps organizations collaborate on cybersecurity efforts by pooling information on threats, making it a vital tool for CERTs/CSIRTs, SOCs, and other security teams.
- **I Know What You Download** (<https://iknowwhatyoudownload.com/en/contacts/>): This tool tracks and monitors torrent downloads associated with specific IP addresses. It allows users to see what files have been downloaded via BitTorrent from a particular IP, offering insight into file-sharing activities. The tool is often used in cyber investigations to link illicit downloads to specific networks or individuals.
- **Recorded Future** (<https://www.recordedfuture.com/>): Recorded Future is a threat intelligence platform that uses machine learning and natural language processing to collect and analyze data from open web sources, dark web forums, and technical feeds. It helps security teams predict, prevent, and respond to cyber threats by providing actionable intelligence in real-time, making it a valuable tool for proactive threat management.

- **Censys** (<https://censys.io/>): Censys is a search engine that maps and indexes devices, services, and infrastructure exposed on the internet. By continuously scanning the internet, it provides insights into security vulnerabilities, misconfigurations, and risks within an organization's attack surface. Censys is widely used by security professionals for vulnerability assessments, asset discovery, and monitoring of internet-facing infrastructure.

T-3: Consolidated Messaging System(s)

The official description of the parameter from the SIM3v2 [3]:

A CSIRT should organise its work in such a way that ensures the effective handling of incidents. This includes continuous information sharing between team members - in many cases also when they are not on duty. Also, incident reports will come in, and communication with other teams needs to be managed as well. E-mail and other types of messaging, like signal, threema, wire and other messaging tools, are the dominant communication mechanisms in most of these cases. Therefore the team must have resilient, high-quality, messaging system(s) that are consolidated (in the team's office, with good back-up facilities - or secure cloud based solutions) and all team members need access to it. It's of course possible to use the messaging system(s) of the host organisation, or a cloud service - however the security of such solutions needs to be taken into account - strong encryption of confidential data may be needed, or even obligatory. Does your CSIRT use consolidated messaging systems?

Maturity levels:

1. *The messages go to the laptops/computers of the team members. There is no need to keep it in one place.*
2. *We keep messages in dedicated systems, but this system is not under our control and we don't know much about it.*
3. *We keep messages in dedicated systems. Our management has not formally approved this.*
4. *We keep messages in dedicated systems and this was approved by our team management.*
5. *We keep messages in dedicated systems and this was approved by our team management. In the periodic review of our team it is checked if these repositories meet our requirements.*

The management and distribution of email messages itself can be a challenging element to implement in an organization. However, it is very crucial to have a properly managed flow of email messages to avoid the situation of losing them in the users' inbox due to overload. Depending on the number of emails that are received on a daily basis (whether in terms of users' requests regarding support to take an action on their email account or, for example, generic emails from a data leak service), it is necessary to determine the distribution groups to whom these emails will be delivered. For a smaller organisation with fewer services provided, perhaps segmenting the message flow is not necessary. Otherwise, it is not needed and necessary for every employee to receive all email messages. It may not be suitable or efficient for the policies built within the organization. Assigned email messages need to be segmented into specific groups according to the defined categories, based on which they will be distributed only to certain members of a given distribution group. This assigned list is determined by the organization itself depending on the individual's area of work.

T-4: Incident Tracking System

The official description of the parameter from the SIM3v2 [3]:

A well-designed and tailored ticketing system is important for any CSIRT. In practice, when a team has to handle many incidents, it is near impossible to correctly manage all information and communication between team and involved parties, without such a tracking system. Only really small teams with a small number of incidents are able to manage the incident management process by using a very basic solution like a shared spreadsheet. In most cases, a dedicated solution is in need. Sometimes, the team reverts to using the host organisation's trouble ticket system - this is certainly possible, but similar to the e-mail case, confidentiality may again be a challenge, as most generic trouble ticket systems don't seem to have been designed with security in mind. Many CSIRTs have long term been using their own specific incident tracking systems - specifically open source solutions like RT(IR) (Request Tracker for Incident Response), OTRS (Open Source Ticketing Request System) or (of more recent date) TheHive. All these solutions are scalable and easy to use. Does your team use such an incident tracking system?

Maturity levels:

1. *We solve incidents, we don't have a registration tool for them.*
2. *We have a way of registering and tracking incidents, but have not documented it.*
3. *We have an incident tracking system. Our management has not formally approved this.*
4. *We have an incident tracking system and this was approved by our team management.*
5. *We have an incident tracking system and this was approved by our team management. In the periodic review of our team it is checked if this tracking systems meets our requirements.*

Maintaining the information obtained regarding incidents is essential from several points of view, whether in terms of clarity, usability, or, for example, when handling similar or repeated incidents. The incident tracking system is used for this purpose, allowing all details of incidents to be recorded, whereby reporting of incidents is most commonly done via a phone number as well as email address. The possibilities for a specific service on this system are various, e.g., AlertOps [19] AlienVault OSSIM [20], Wazuh [21] and others. Each service provides a slightly different functionality compared to the others, and the final decision on choosing the one is to be made by the company depending on its needs, the number of incidents per year, or the amount of allocated finances. From open-source tools to enterprise-grade platforms, incident recording is only one component involved. Frequently, incident response software or incident management tools are needed as well. Therefore, we are dealing with a more complex system. This may include alerting when a problem occurs or managing the entire incident response process from initial detection to resolution. The following article [22] on this topic from Cyberlands, a company that specializes in penetration testing for fintech, crypto and SaaS companies, may serve as useful references.

Another incident tracking system dedicated to managing and recording security incidents is called TheHive [23]. TheHive incorporates the Cortex tool, which can be used to analyze IP addresses, URL links, and more. A detailed description of TheHive's functionality and incident management can be found later in Section 6.5 Incident Management - Solution Review.

T-5: Resilient Voice Calls

The official description of the parameter from the SIM3v2 [3]:

Voice calls, be it traditional phone calls or via messaging tools, are a crucial communication tool for CSIRTs. It's part of how the CSIRT team members do their work, and manage incidents and perform their other duties. Therefore the uptime of the voice call tools available needs to support the team's service levels (Parameter O-7). Thus if a team has to be able to react quickly to incidents and solve them expediently, then the uptime of the voice call tools needs to be very high, so that any failure in those tools does not hinder the team's performance. In the case of voice calls, all such tools available to the team, like a classical 'landline', IP telephony, mobile phones, and messaging apps like signal, threema, wire and others, should be taken into consideration - mobile phones, with their multiple apps, often provide good means of resilience, especially when the services of more than just one mobile provider are used. A special, but rare, case is when a team has access to a (usually) national level protected communication system. What are your team's voice call facilities and are they sufficiently resilient for your purposes?

Minimum Requirement: Fallback mechanism for the case of voice call system(s) outages.

Maturity levels:

1. *We don't really know anything about the service levels of our voice call system(s), and we haven't arranged any fallback scheme (e.g. using mobile phones).*
2. *When our voice call system(s) go down we adopt a fallback scheme (e.g. using mobile phones), but we have not documented this.*
3. *When our voice call system(s) go down we adopt a fallback scheme (e.g. using mobile phones) and we documented this. Our management has not formally approved this.*
4. *When our voice call system(s) go down we adopt a fallback scheme (e.g. using mobile phones), we documented this and this was approved by our team management.*
5. *When our voice call system(s) go down we adopt a fallback scheme (e.g. using mobile phones), we documented this and this was approved by our team management. In the periodic review of our team it is checked if this fallback scheme meets our requirements and is sufficiently known.*

Communication among users and the security team/organisation is part of the components necessary for the proper performance of the organisation either during weekdays, when it is possible to contact someone and resolve a particular situation, or in more critical circumstances when telephone contact is essential. For routine administration, email is often the communication channel used. In some circumstances, telephone communication is a quicker approach in terms of problem resolution as it can reduce the time taken to send and respond to email in critical cases. Specifically, VOIP phones are being used as the primary contact in many organizations. Multiple options are possible in the case of an outage. However, in general, there are a minimum of 2 channels that need to be secured in the failure of one of them since one channel may not be sufficient if an outage occurs and it is necessary to ensure that the service level is maintained. One example would be a fixed line and a mobile line. The use of a second telephone in case of emergency is also well proven as an option. All these contacts (as well as email contact) should be publicly obtainable, either via the website in the 'Contact' section or others. However, it is generally crucial to ensure that such contacts are public for users in case of necessity.

T-6: Resilient Messaging

Official description of the parameter from the SIM3v2 [3]:

E-mail and other types of messaging are a fundamental communication tool for CSIRTs. It's part of how the CSIRT team members do their work, receive incident reports, manage incidents and perform their other duties. Therefore the uptime of the messaging tools available need to support the team's service levels (Parameter O-7). Thus if a team has to be able to react quickly to incidents and solve them expediently, then the uptime of the messaging tools needs to be very high, so that any failure in those tools does not hinder the team's performance. In case of e-mail, there is also a reputation aspect here - when an incident reporter or another CSIRT receives an e-mail back indicating that your team's mail facility is not operational, this is bad PR. In the case of e-mail, a (hot) stand-by or fully resilient set-up is a possible (state-of-the art) solution - coupled to good back-up facilities for the mail storage, which will contain important and often sensitive incident data. For end-to-end secure messaging tools like signal, which is increasingly popular among CSIRTs because of its open-source strong cryptography, proper back-up schemes are important as by design there is no cloud storage. What are your team's messaging facilities and are they sufficiently resilient for your purposes?

Maturity levels:

1. *We don't really know anything about the service levels of our messaging system(s).*
2. *The service level of our messaging system(s) is good enough for our purposes, but we have no documentation for this.*
3. *The service level of our messaging system(s) is good enough for our purposes, and we have informal documentation for this. Our management has not formally approved this.*
4. *The service level of our messaging system(s) is good enough for our purposes, and we have documentation for this that was approved by our team management.*
5. *The service level of our messaging system(s) is good enough for our purposes, and we have documentation for this that was approved by our team management. In the periodic review of our team it is checked if this e-mail resiliency is sufficient.*

This parameter refers to the capability of a CSIRT (Computer Security Incident Response Team) to maintain effective communication during crisis situations, especially when regular communication channels are disrupted. This parameter evaluates how well-prepared the team is to ensure continuous and reliable messaging under adverse conditions, such as during cyberattacks, network outages, or other incidents that impact standard communication methods.

Key aspects include:

- **Alternative Communication Channels:** Having backup systems, like secure messaging apps. In addition to email, it is essential to be able to contact the CSIRT via a form, helpdesk or other alternative service. The use of redundant email servers may also be a recommendation.
- **Communication Plans:** Establishing clear procedures for transitioning to alternative channels when primary systems fail, ensuring that critical information is still shared with stakeholders.

- **Security of Communication:** Ensuring that, even in a crisis, communication remains secure and resistant to interception or compromise.

Resilient messaging is crucial for a CSIRT's ability to coordinate effectively and respond swiftly, even under disruptive conditions. The SLA from the email service provider should also be taken into consideration as a guarantee for the prompt restoration of communication.

T-7: Resilient Internet Access

The official description of the parameter from the SIM3v2 [3]:

Sufficiently fast and reliable Internet access is crucial to have for CSIRTs. Without that, the CSIRT can not normally function. Therefore the uptime of the Internet access needs to at least support and preferably exceed the team's service levels (Parameter O-7). Thus if a team has to be able to react quickly to incidents and solve them expediently, then the uptime of the Internet access needs to be very high, so that any failure there does not hinder the team's performance. Ideally, the CSIRT or its host organisation has a fully (even physically) redundant Internet access, but much less expensive solutions like having a back-up Internet access option (using a different technology as the normal one) may also be sufficient to meet your team's service level demands. As most teams depend on their host organisation for Internet access, it's useful that the team is qualified internally as one of the most demanding organisation units in regard Internet access. What are your team's Internet access facilities and are they sufficiently resilient for your purposes?

Maturity levels:

1. *0 We don't really know anything about the service levels of our Internet access.*
2. *The service level of our Internet access is good enough for our purposes, but we have no documentation for this.*
3. *The service level of our Internet access is good enough for our purposes, and we have informal documentation for this. Our management has not formally approved this.*
4. *The service level of our Internet access is good enough for our purposes, and we have documentation for this that was approved by our team management.*
5. *The service level of our Internet access is good enough for our purposes, and we have documentation for this that was approved by our team management. In the periodic review of our team it is checked if this Internet access resiliency is sufficient.*

This parameter evaluates a CSIRT's ability to maintain reliable internet connectivity during critical situations, such as cyber incidents or network disruptions. This parameter assesses the team's preparedness to ensure continuous access to external resources, threat intelligence feeds, and communication channels, even when primary internet connections are compromised.

Key aspects include:

- **Backup Internet Connections:** Having alternative ISPs, redundant connections, or satellite internet to ensure uninterrupted access to critical systems;
- **Failover Mechanisms:** Implementing automatic failover systems that switch to backup connections when the primary internet fails;

- **Security of Backup Connections:** Ensuring that backup internet access methods are secure and resilient against potential attacks or misconfigurations.

Having resilient internet access is essential for maintaining operational continuity, allowing the CSIRT to effectively respond to incidents and coordinate with external parties even during outages or attacks. It is essential to have the technical documentation of the configuration and possible alternatives available.

T-8: Incident Prevention Toolset

The official description of the parameter from the SIM3v2 [3]:

This is about having a well-defined and implemented set of tools that help with incident prevention. These tools are part of the first line of defence for the constituency. A CSIRT should clearly define its role regarding each of those tools. Some of such tools the team may run themselves, in other cases they may be the architect and a user - or they may only be a user of the tool, or have access to the results. Because of the growing number of possible tools, their 'orchestration' plays a more and more important role. It is of primary interest to any CSIRT to be closely involved in this area, or even decide about such tools. Examples of prevention tools: intrusion prevention systems, antivirus software, spam filters or vulnerability scanners. Does your team have a well-defined incident prevention toolset?

Maturity levels:

N/A We are a purely incident coordinating/handling team not involved in prevention.

- 1. We never really discussed this.*
- 2. We have such tools, but have not listed or documented them.*
- 3. We have such tools, and to record this we wrote something for our own purposes. Our management has not formally approved this.*
- 4. We have such tools, have documented these and this was approved by our team management.*
- 5. We have such tools, have documented these and this was approved by our team management. In the periodic review of our team it is checked if these tools are sufficient to meet our requirements.*

Before an incident occurs, a series of steps, especially countermeasures, can be taken to ensure that the incident does not occur or is effectively detected. We are therefore looking at the initial phase of pre-incident prevention. Various tools such as EDR (endpoint detection and response), XDR (extended detection and response), antivirus solutions, firewalls, the use of a spam filter, or services such as Shodan, Nessus and others are used for this purpose. With EDR and XDR solutions, we are referring to more advanced solutions that, in addition to detecting a possible incident, can also respond to the incident in a certain way. Another example involves the use of IPS (intrusion prevention system) devices, which are used to identify intruders based on predefined patterns [7]. The previously mentioned Shodan service [24] can serve as a port scanner - i.e., scan open ports on various web services. The Nessus service [<https://www.tenable.com/products/nessus>], on the other hand, provides automated vulnerability scanning. These are a variety of tools and tactics that can be chosen as an approach in prevention.

T-9: Incident Detection Toolset

The official description of the parameter from the SIM3v2 [3]:

This is about having a well-defined and implemented set of tools that help with incident

detection. These tools are like the ears and eyes of the CSIRT - they bring information about threats and incidents, from potential to exploited. A CSIRT should clearly define its role regarding each of those tools. Some of such tools the team may run themselves, in other cases they may be the architect and a user - or they may only be a user of the tool, or have access to the results. Because of the growing number of possible tools, their 'orchestration' plays a more and more important role. It is of primary interest to any CSIRT to be closely involved in this area, or even decide about such tools. Examples of detection tools: MISP, AbuseHelper, IntelMQ, network packet analysers - but also bear in mind that phone and e-mail are used for receiving incident reports and are thus detection tools too. Does your team have a well-defined incident detection toolset?

Maturity levels:

1. *We never really discussed this.*
2. *We have such tools, but have not listed or documented them.*
3. *We have such tools, and to record this we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have such tools, have documented these and this was approved by our team management.*
5. *We have such tools, have documented these and this was approved by our team management. In the periodic review of our team it is checked if these tools are sufficient to meet our requirements.*

Incident detection is related to the previous section (T-8). In this instance, we are discussing tools that can detect an incident and inform about this incident through an email message or a generated alert. This may be either an antivirus solution that detects (potentially) malicious activity on the device or the use of the above-mentioned EDR, where it is possible to view the alerts created in the console based on the current policies. An example of a service might be Have I Been Pwned [25], where it is possible to enter an email address to be notified about data leaked from a particular constituency. For established community-based networks of organizations, a further possibility is to inform the community using its own resources. Increased protection of systems is not necessarily provided by the use of large numbers of tools. It is therefore advisable to think about what the organisation may need and choose one of the listed tools based on that, deploy it gradually and configure it properly. Improperly configured tools can, in fact, cause many alerts that can potentially mask the crucial ones hiding underneath a number of others.

T-10: Incident Resolution Toolset

The official description of the parameter from the SIM3v2 [3]:

This is about having a well defined and implemented set of tools that help with incident resolution. These tools support what is really core business for any CSIRT - the resolving of incidents. A CSIRT should clearly define its role regarding each of those tools. Because these tools are so mission critical, the team will probably run several of those themselves, or be a prime architect and significant user - but in some cases they may only be a user of the tool, in which case they do need to make sure to be able to give feedback and be heard when doing so. Because of the growing number of possible tools, their 'orchestration' plays a more and more important role. It is of primary interest to any CSIRT to be decisively involved in this area. If a CSIRT deal with some specific types of incidents, it is especially important to create a tailored toolset to suit those specific resolution needs. Bear in mind that this toolset does include software, but can also included dedicated hardware - and in some cases this will go as far as the creation of e.g. an incident resolution lab, e.g. for malware analysis or computer forensics.

Examples of resolution tools: again MISP and IntelMQ, your incident tracking system, forensics kits. Does your team have a well-defined incident resolution toolset?

Maturity levels:

1. *We never really discussed this.*
2. *We have such tools, but have not listed or documented them.*
3. *We have such tools, and to record this we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have such tools, have documented these and this was approved by our team management.*
5. *We have such tools, have documented these and this was approved by our team management. In the periodic review of our team it is checked if these tools are sufficient to meet our requirements.*

In the three sections covering the toolset at different stages of an incident, we discuss the use of different tools after an incident has already been detected and needs to be properly handled. In this case, we are referring to forensic analysis tools that cover:

- Image analysis:
 - Arsenal Image Mounter (<https://arsenalrecon.com/downloads/>)
 - FTK Imager (<https://accessdata.com/product-download/ftk-imager-version-4-5>)
 - OSFMount (<https://www.osforensics.com/tools/mount-disk-images.html>)
- File analysis:
 - WinHex (<http://www.x-ways.net/winhex/index-m.html>)
 - ExifTool – file EXIF extractor (<https://exiftool.org/>)
- OS Windows analysis:
 - EZ Tools - includes shellbags, jumplist, MFT, registry parsers, and more (<https://ericzimmerman.github.io/#!index.md>)
 - USB Detective – USB device parser from registry and related artifacts (<https://usbdetective.com/community-download/>)
 - RegRipper – registry file parser (<https://github.com/keydet89/RegRipper3.0>)
 - ESE Analyst – parses ESE databases (<https://github.com/MarkBaggett/ese-analyst>)
- Network traffic analysis:
 - PE Studio – quick malware analysis triage (<https://www.winitor.com/download/>)
 - Ghidra – malware reverse tool (<https://ghidra-sre.org/InstallationGuide.html#Platforms>)
- Memory analysis:
 - Volatility (<https://github.com/volatilityfoundation/volatility3>)
 - Volatility Workbench (GUI) (<https://www.osforensics.com/tools/volatility-workbench.html>)
- More comprehensive tools:
 - Autopsy (<https://www.autopsy.com/download/>)
 - OS Forensics (<https://www.osforensics.com/>)
 - WSL (<https://docs.microsoft.com/en-us/windows/wsl/install>)

- Other tools:
 - CyberChef (<https://gchq.github.io/CyberChef/>)
 - Sysinternals (<https://docs.microsoft.com/en-us/sysinternals/>)

P: Processes

With **Processes**, we refer to logically sequenced sets of actions which are carried out by humans (Human area) or automated tools (Tools area) to achieve a specific result (defined in the Organisation area). All processes can be characterised by several attributes. By applying such attributes, we can also determine how successful a particular process is (in getting the job done) or how successful a particular organisation is in providing a service (as in getting this process right all the time). In mature organisations, processes are documented, measurable and repeatable. To be able to grow and improve the effectiveness of an organisation, it is also important to build processes that are adaptable. Here, we specifically talk about those processes that support the management of incidents and any other services the CSIRT offers and we adopt the term 'processes' in the broadest meaning of the word, and therefore, in this Processes area, you will also find processes that might sometimes be labelled as 'policies' or otherwise.

P-1: Escalation to Governance Level

The official description of the parameter from the SIM3v2 [3]:

Each team must be able to escalate critical incidents to the appropriate management levels, including the highest level of governance (e.g. board of directors, minister) in case of potential crises or incidents that are at least a significant threat to the reputation of the organisation. In case the team is responsible for an external constituency, it also needs to be able to escalate to the appropriate management level of all constituents; the latter is not only required when the team's normal point of contact does not (timely) react, but also such an escalation may be warranted in case of a significant incident or new threat. Such escalations triggered by security incidents or other events should be defined in accordance with the team's Incident Classification (see O-8), which allows logically basing the escalation on e.g. impact and priority. It is critical that the means to escalate must be available at all times - even though the feedback or reaction will not always be as immediate, as this is defined by higher governance levels in the own organisation, or in constituents' organisations. Can your team escalate in the way meant here?

Maturity levels:

1. *We never really discussed this.*
1. *We have an informal way of escalating, but this was never written down.*
2. *We don't have a formal written escalation process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
3. *We have a formal written escalation process approved by our team management.*
4. *We have a formal written escalation process approved by our team management. In the periodic review of our team it is checked if this process has been used appropriately and how it worked.*

The P-1 parameter refers to the procedures and authority the CSIRT team has for escalating critical incidents to higher levels of management or governance bodies within the organization. This parameter evaluates how effectively and efficiently the CSIRT can

communicate and involve senior management or decision-makers when incidents require strategic decisions, policy changes, or significant resource allocation.

Key aspects include:

- **Clear Escalation Pathways:** Well-defined procedures for when and how incidents are escalated to governance bodies or senior executives;
- **Decision-Making Authority:** The CSIRT's ability to involve individuals or teams with the authority to make decisions on business-critical issues, such as halting operations or engaging external resources;
- **Engagement with Governance:** Regular interaction and communication channels between the CSIRT and governance level to ensure that they are aligned on risk management and incident handling priorities.

From the perspective of CSIRT staff, escalation procedures are typically well-defined and embedded within the overall CSIRT processes. However, operational management must be able to promptly and efficiently alert higher-level management when service quality is at significant risk; relying on monthly or quarterly reports is inadequate. Routine procedures should also include determining whether customers need to be informed about the issue and providing an estimated resolution time.

Escalation criteria, along with the related processes, procedures, and guidelines, should be pre-established and ready for use. These must be regularly reviewed and updated to address evolving requirements, such as new attack methods, incident types, or changes in the organization's environment.

Commonly used criteria for individual escalation include [6]:

- number of sites and systems under attack
- type of data at risk
- severity of attack
- state of attack
- source or target of attack
- impact on the integrity of infrastructure or cost of recovery
- attack on seemingly “secure” systems
- public awareness of incident
- new attack method used
- communication breakdowns
- technical ability, knowledge, and/or expertise of the individual CSIRT staff

P-2: Escalation to Press Function

The official description of the parameter from the SIM3v2 [3]:

Handling the press and public media is required. In case most or all CSIRT members have been tasked to not talk with the press themselves, press requests in regard security incidents must still be handled effectively, wherever they come in. Therefore, The team must be able to reach out to appropriate spokes persons who normally handle press inquiries. To avoid miscommunication and delays that might impact the organisation's reputation, the team needs to be able to reach such press contacts directly and also outside business hours, in order to give them the necessary situational awareness. It is advisable that the team itself designates a limited amount of team members to also be able to talk with the press, e.g. together with an official spokes

person - as such designated team members will be able to give more insight into the technical aspects of a given situation; when such a choice is made it's advisable to give such team members a suitable training. Can your team escalate in the way meant here?

Maturity levels:

1. *We never really discussed this.*
2. *We have an informal way of escalating, but this was never written down.*
3. *We don't have a formal written escalation process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a formal written escalation process approved by our team management.*
5. *We have a formal written escalation process approved by our team management. In the periodic review of our team it is checked if this process has been used appropriately and how it worked.*

To effectively accomplish the Escalation to Press Function parameter in the SIM3, organizations need to implement a structured approach to manage communications with the media during security incidents. Below are key steps and actions to achieve this:

- **Establish Clear Communication Protocols**

Define procedures for when and how the CSIRT will communicate with the press. Identify the types of incidents that necessitate media engagement, such as data breaches, ransomware attacks, or significant service disruptions.

- Route all communication through the spokesperson
- Develop Predefined Messaging Templates

Create templates for press releases and statements that can be quickly customized in response to specific incidents and during crisis situations.

- Implement an Approval Process

Establish a clear workflow for approving communications with the media. Involve relevant stakeholders, such as legal counsel and public relations, to review and authorize messaging before it is released.

- Media Trainings

Provide training sessions for the CSIRT members on media interaction, including handling questions and maintaining composure during interviews. You can also simulate media scenarios to prepare for real-life interactions.

- Develop a Crisis Communication Plan

Outline a comprehensive crisis communication strategy that includes objectives, key messages, and target audiences. Specify roles and responsibilities for team members involved in media relations during an incident.

P-3: Escalation to Legal Function

The official description of the parameter from the SIM3v2 [3]:

Handling legal issues including requests from law enforcement is required. Such requests to the organisation must be handled very effectively in order to avoid that evidence is destroyed or no longer available, e.g. as a result of automated processes removing data routinely - but also, because handling such issues wrongly could lead to reputation damage and financial losses. The team must therefore be able to reach out directly and also outside business hours, to legal experts in their organisation (e.g. lawyers) to inform them about relevant issues, including but not limited to incoming law enforcement requests or orders. The legal experts can then either handle these issues

themselves directly, or in consultation with the team. Can your team escalate in the way meant here?

Maturity levels:

1. *We never really discussed this.*
2. *We have an informal way of escalating, but this was never written down.*
3. *We don't have a formal written escalation process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a formal written escalation process approved by our team management.*
5. *We have a formal written escalation process approved by our team management. In the periodic review of our team it is checked if this process has been used appropriately and how it worked.*

In the case that legal issues are likely to arise in the resolution of a security incident, the incident handler shall contact the legal department identified in advance in the plan. To effectively implement the Escalation to Legal Function Parameter in SIM3, organizations should establish a clear process for identifying incidents that require legal involvement, such as data breaches or compliance violations. This includes defining criteria for escalation, such as the severity of the incident, potential legal implications, and the regulatory requirements. Designate legal representatives to be part of the incident response team, ensuring timely communication between the CSIRT and the legal department. Develop predefined protocols for legal consultations, including the documentation of incidents and decisions made during the response process. Regularly review and update these procedures to reflect changes in the legal requirements and organizational policies, and conduct training for the CSIRT on legal considerations in incident management to ensure that all team members understand the importance of involving legal counsel in relevant situations.

P-4: Incident Prevention Process

The official description of the parameter from the SIM3v2 [3]:

From a risk management perspective, incidents must be avoided, therefore the CSIRT should support appropriate prevention processes internally - or in case of an external constituency - for its constituents. Examples of processes that prevent incidents from happening are: the creation and dissemination of advisories about new security vulnerabilities; port scan activities; the spreading of threat intel; the sharing of lessons learnt from the analysis of incidents. Usually, tools are used to support these processes (see T-8), and then how to do that will be part of the process. Does your team have a process for incident prevention?

Maturity levels:

N/A We are a purely incident coordinating/handling team not involved in prevention.

1. *We never really discussed this.*
2. *We know how we do this, but have not documented this.*
3. *We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a formal written process approved by our team management.*
5. *We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended.*

By proactive activities, we are referring to activities that can be carried out before an incident occurs. Incident prevention is an initial phase that may involve several mechanisms and procedures. However, it is necessary to choose an adequate strategy for these services to be effective. At a non-technical level, this may involve raising security awareness or educating the wider community on information security topics, but in the current context we are mainly focusing on staff education. The most vulnerable element of any organisation lies in its employees. For instance, it may be an unintentional activity, such as the risk of malware on a device (which can spread over the network to other devices) by clicking on a malicious link in a phishing email, or a deliberate activity. The goal of these training sessions may be to educate employees on basic cybersecurity concepts, introduce current trends that may be current in a particular organization, or to point out procedures for dealing with various situations. In terms of the timeframe, it is advisable to regularly repeat these trainings within the period set by the organisation.

Another proactive possibility is vulnerability scanning and analysis. This involves determining the scanning procedure before the actual scanning, the extent to which the network needs to be diversified, the type of scan to choose, and identifying which vulnerabilities need to be analysed and responded to. The nonprofit foundation OWASP provides a list of such vulnerability scanning tools [26], including Nessus [27], Burp Suite [28], and others. Hence, these are the first steps to prevent vulnerabilities in the system from being exploited. With more detailed scan reports, it is necessary to filter out and focus your attention on critical vulnerabilities in particular, which needs to be patched as quickly as possible.

P-5: Incident Detection Process

The official description of the parameter from the SIM3v2 [3]:

Without detecting incidents no CSIRT is able to respond to those. Depending on what type of CSIRT we consider, some operate their own detection capabilities (IDS, firewall logs, honeypots, ...). Others are depending on constituents to receive incident reports, or utilise a SOC to receive potential incidents that need to be analysed - a mixed approach is also possible. How to do that is described in the detection process(es). Triage, the process of judging incoming incident reports and assigning them for further handling, is part of incident detection. Usually, tools are used to support these processes (see T-8), and then how to do that will be part of the process. Note that frequently P-5 and P-6 (P-6 follows next and is about incident resolution) are combined in one process, often called the incident management (or handling) process, which is valid as long as both detection and resolution are done justice. Does your team have a process for incident detection? (If you have a combined process for P-5 and P-6, choose the same level for both)

Maturity levels:

1. *We never really discussed this.*
2. *We know how we do this, but have not documented this.*
3. *We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a formal written process approved by our team management.*
5. *We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended.*

Vulnerability management and threat detection belong to such incident detection activities. Within vulnerability management, it is recommended to regularly check and

search for security vulnerabilities, either acquired by own resources or reported by an external entity. Vulnerability testing itself should be performed multiple times per year, with the resulting reports of the identified vulnerabilities sent to the appropriate department upon completion. These vulnerabilities should then be verified within the system, and if confirmed, remediated, or at least mitigated by other mechanisms. For threat detection, threats can be periodically examined on public sources followed by identification and validation, with management approval.

P-6: Incident Resolution Process

The official description of the parameter from the SIM3v2 [3]:

Any CSIRT that manages incidents needs to develop at least a generic process about how to resolve, handle, mitigate incidents. Because it is generic, each input is processed by the very same process in more or less the same way, although most certainly the results will vary. Instead of focusing on the specifics of an incident (e.g. a malware APT is very different from a DDoS attack), this process focuses on the overall step-by-step approach after the detection process (see P-5). The main steps in the process are: analysis, response actions leading to mitigation, closing and lessons learnt. Following this generic process ensures that all incidents are handled according to the established practice, including the use of the related toolset (see T-10) - this could for example include the logging of all communication with constituents, or the analysis of specific logs, etcetera. Does your team have a process for incident resolution? (If you have a combined process for P-5 and P-6, choose the same level for both)

Maturity levels:

1. *We never really discussed this.*
2. *We know how we do this, but have not documented this.*
3. *We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a formal written process approved by our team management.*
5. *We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended.*

Regarding reference to the toolset (T-9), in the following section we can generally discuss the incident handling and management process. With incident phases, we are referring to a series of individual steps that needs to be completed in one single stage. These are general procedures and steps descriptions to guide and assist the incident handler to handle the incident in a proper manner. In addition to the generic steps, more specific instructions for those steps are provided on a case-by-case basis according to the type of incident. More detailed guidance for incidents such as malware, ransomware, and data leakage is provided in the documents previously submitted to the Soccer project, as well as a general guide to incident handling.

P-7: Specific Incident Processes

The official description of the parameter from the SIM3v2 [3]:

It is very important to have a common process to handle all incidents that are managed by a CSIRT - this is P-6. However, such a generic process ensures the overall workflow and cannot be tailored for specific types of incidents, and thus will more than likely miss out on some relevant technical aspects. As already stated for P-6, an incident caused by a new malware APT is very different from a DDoS attack blocking the Internet for an important client. Not only are the priorities different, but also the technical response. Therefore it is recommend for mature CSIRTs to identify those incident types that are

causing most of the work - and then to write specific incident processes for those. This will allow to leave out some steps or activities, while describing others in more detail or adding new ones (could be sub-steps of the generic process). Additionally, specific incident processes can be written not just for very common incident types, but also for mission critical incidents (high impact, high priority), or for incidents that require a response requiring expertise not commonly present inside the CSIRT itself, like legal expertise. Note that P-7 may be already part of P-6, if the incident resolution process supports sub-processes to deal with some specific incident types or supports various paths for some specific incident types - this is of course perfectly valid. Has your team described specific incident processes, beyond the generic incident resolution process?

Maturity levels:

1. *We treat all incidents the same way, no additional info is available for different types of incidents.*
2. *We have some standard ways of dealing with different incident types, but have not documented this.*
3. *We don't have formal written specific incident processes, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have 1 or more formal written specific incident processes approved by our team management.*
5. *We have 1 or more formal written specific incident processes approved by our team management. In the periodic review of our team it is checked if these process(es) work(s) as intended.*

An important aspect of incident handling is to have established processes for different types of incidents. Whether it is about data leakage, ransomware, or routine monitoring activity, depending on how frequently the organization encounters these incidents. Therefore, it is advisable to have the procedures and manuals written down for the most commonly occurring incidents. For example, if an organization commonly encounters phishing emails, a handbook for analyzing the phishing email and its header is precisely useful in this case. The incident handler's work will become significantly more efficient, and the handbook will serve as an additional help in dealing with the incident. In terms of scope, it depends on the complexity of the incident as well as on the range defined by the organisation. This procedure should cover all the necessary information for the incident handler to be able to assess the incident and, based on its complexity, categorise it according to its extent, the number of affected users and other parameters (in the case of a critical incident, e.g., ransomware, critical management should have been defined). It is also advisable to have a list of personnel responsible for managing the infrastructure, the services used, etc., written in advance, due to the occurrence of the incident, it is no longer necessary to investigate this aspect, and it can reduce the response time. With more sophisticated incidents, a graphical representation of the handling of the incident can also be helpful, as well as a keyword description of the individual steps of the handling.

P-8: Audit & Feedback Process

The official description of the parameter from the SIM3v2 [3]:

All CSIRTs need quality assurance of all critical and sensitive aspects of their operation. While various means exist to help ensure the quality levels (e.g. self-assessment, walk-throughs, peer reviews, internal as well as external audits), the level of scrutiny must be defined, scoped and maintained. Also it needs to be ensured that there is not just 'audit' but also a subsequent feedback to the team, to enable learning and improvement. We call this the audit & feedback process. This process needs to ensure that the appropriate

quality levels are met, and that problems are recognised as soon as possible. The resulting information flow needs to benefit not only the team itself, but also the relevant management layers above the CSIRT. This is especially important for those topics covered by SIM3 Parameters where the team aims to score level 4 - for those, a regular, active form of checking by the higher management (above the CSIRT manager) is required - and it must be documented that they are audited that way and that feedback is given to the team. This involvement of the higher management is a crucial mechanism, as some quality aspects cannot be ensured by the CSIRT itself, not even if controlled by the CSIRT manager or team lead. Unbiased, neutral feedback is mandatory as not to focus on mistakes or errors, but instead to focus on improvement and progress, with the mission of the organisation/constituency in mind. Has such an audit & feedback process been defined for your CSIRT?

Maturity levels:

1. *We never really discussed this.*
2. *We do have reviewing, but have not documented this.*
3. *We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a formal written process approved by our team management.*
5. *We have a formal written process approved by our team management and by higher management, and higher management is leading in this.*

Just as the development of documents is fundamental to the proper functioning of an organization, so is keeping them up to date. This brings us to the very notion of auditing, which refers to the regular review of the competence of a given process. It is necessary to establish a control mechanism process, whose specific points can be identified by the organization itself. It is advisable to make employees aware and explain why this process is necessary. Each organisation is characterised by different procedures and processes, and the depth of the control mechanisms as well as the ability to evaluate them may vary (still, the principle of minimisation in the number of processes needed should be maintained). It is possible to perform such audits by an external entity that regularly reviews the competences and/or the management provides an activity report with statistics and suggestions for improvement. The frequency of auditing depends on the established rules and policies set within the organisation. Statistics on the reported and resolved security incidents should be provided at intervals of a few months. The security incident handling procedures should also be updated and evaluated for effectiveness. Auditing may include infrastructure reviews, employee interviews, or penetration testing (others may be prohibited). However, obtaining approval from upper management is very important before proceeding. Apart from an external party, audits can be performed by upper management to remain up-to-date, or legally required audits.

P-9: Emergency Reachability Process

The official description of the parameter from the SIM3v2 [3]:

Each CSIRT supports a number of communication mechanisms that can be used to send information or incident reports to. Depending on the constituents need, or the mandate of the CSIRT such means are made publicly known, or are only available for constituents or peer CSIRTs (see P-17). In most cases, CSIRTs service windows coincide with standard business hours. Some CSIRTs are on call outside such times, in accordance with their own service levels. However, crisis/emergency situations can and will occur, and may well require the reachability of the CSIRT even outside the normal service windows. To allow constituents or peer teams to contact the CSIRT in such special cases, there needs to be an emergency reachability process that describes telephone numbers, e-mail addresses and possibly also special keywords reserved for

such true emergencies. The process should sanction misuse as reacting outside the normal service windows is usually expensive. On the other hand - given how important it potentially is - the process must be executed from time to time to train all parties involved. Does your CSIRT have such an emergency reachability process?

Maturity levels:

1. *We never really discussed this.*
2. *Key stakeholders know how to reach us in cases of emergency, but we have not documented this.*
3. *We don't have a formal written process, therefore we wrote something for our own purposes and made it available to our key stakeholders. Our management has not formally approved this.*
4. *We have a formal written process available to our key stakeholders and approved by our team management. (Note that published information, either inside the constituency or in some external database (e.g. TI) also counts as level 3.)*
5. *We have a formal written process available to our key stakeholders and approved by our team management. In the periodic review of our team it is checked if this process works as intended.*

To achieve this parameter, the following is recommended:

- Emergency contacts, together with a description of how out-of-hours emergency services operate within the team, if a process is in place.
- Information/a post in a visible/easily accessible place specifying how the constituency can contact the team in an emergency situation.

P-10: Best Practice Internet Presence

The official description of the parameter from the SIM3v2 [3]:

Good communication is at the heart of the work and success of any CSIRT and being able to reach out over the Internet, and be easily reachable are both essential. Besides having available various communication tools (see T-5, T-6 and T-7), all CSIRTs need a process that specifies which Internet media are used in what way, in order to monitor for incoming requests, share information, etcetera, in order to successfully deliver their various services, and fulfil their mandate and responsibility. The process needs to take into account, for the 3 areas mentioned: (1) tracking by the CSIRT of at least the standard e-mail addresses cert@... and security@... - and strongly recommended to take the RFC2142 standard into account and ensure that the relevant mailbox names (postmaster and webmaster deserve special attention) are tracked. And also, that whoever track those mailbox names, know about the CSIRT and how to pass on information to them. (2) a web policy that ensures that all relevant information about the CSIRT is up-to-date and available for the constituency, and a necessary subset including RFC2350 (see O-5) for the world. Additionally it is recommended to consider implementing a slash-security page (example: www.org.tld/security), which can offer a wider range of security related information in regard your (host) organisation, but your CSIRT's info should also be present there. (3) A policy for what social media the team tracks and uses, and how they are to be used. Examples are Twitter, LinkedIn and Facebook. Does your CSIRT have a process that shapes its Internet presence according to the above best practices?

Minimum Requirement: *The process must at least ensure that, for the 3 areas: (1) the mail addresses cert@... and security@... must be tracked by the team; (2) some form of*

web presence for the CSIRT must exist, at least internally; (3) a policy must be present on if and how to deal with social media.

Maturity levels:

1. *We never paid much attention to this.*
2. *We have several of these taken care of, but have not documented this.*
3. *We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a formal written process approved by our team management.*
5. *We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended.*

This parameter focuses on how organizations establish and maintain their online visibility and presence in a way that supports effective incident management. This parameter emphasizes the importance of having clear, accessible, and accurate information available on the organization's website and other online platforms, which can help stakeholders understand the CSIRT's role, services, and contact information.

The following steps are recommended to meet the parameter:

- Determine the set of email addresses used to communicate with external entities and the constituency and perform a response test on them. It is important to have these email addresses in accessible and easy to find places (on the website, on social networks, on the contact form,...), along with their purpose.
- Define the social networks that will be used to make the team visible and communicate public topics and announcements. Define a process to administer and manage these networks.

P-11: Secure Information Handling Process

The official description of the parameter from the SIM3v2 [3]:

Each CSIRT receives and processes information that was labeled confidential by those sending it in - for instance to avoid that the information falls into the hands of attackers, or becomes available on the Internet publicly before appropriate warnings have been distributed. Therefore CSIRTs, but also e.g. vulnerability researchers, are hesitant to share information unless it can be done securely. Now apart from communication security as offered by TLS or security applications like gpg/pgp, the information must also be protected by the receiving CSIRTs (secure storage, backups, etc.) - and this must be done in compliance with relevant legislation, including privacy laws like GDPR. To communicate the restrictions on further distribution of sent information, the TLP (Traffic Light Protocol: see www.first.org/tlp) protocol has been developed - and any CSIRT is strongly advised to use and adhere to TLP - as a minimum a team must be able to deal appropriately with TLP labeled information. Other protocols also exist, that could be applied in a CSIRT context - but will usually need to be explained. Does your team have a process on how to handle information securely?

Minimum Requirement: The process must support the use of TLP, the Traffic Light Protocol.

Maturity levels:

1. *We never really discussed this.*

2. *We know how we do this, but have not documented this.*
3. *We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a formal written process approved by our team management.*
5. *We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended.*

As each organisation collects and operates on different data, the key to information sharing is collaboration between organisations. This allows sharing the information among each other, which increases efficiency and incidents can be detected faster. However, the question remains how relevant this data is and whether it is still valid, although this is a matter for the recipient organisation to assess.

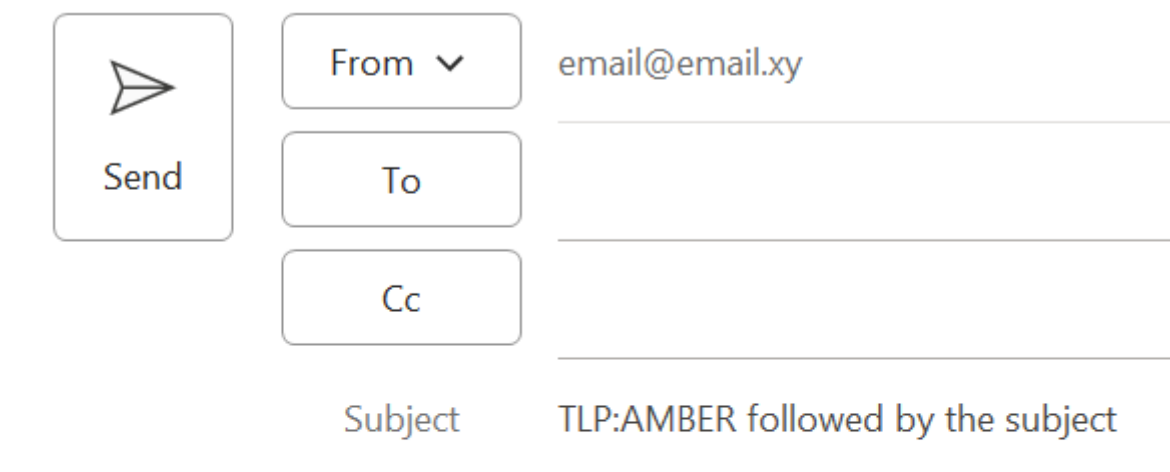
To follow the rules for handling and processing confidential information, it is recommended to use the Traffic Light Protocol 2.0 (TLP) for communication, which determines the distribution group for the information according to each category. TLP is a set of labelings used to ensure that sensitive information is shared with the appropriate recipients. It uses four labels that are individually marked with a different color, whereby the different distribution rules separate these, specifically: TLP:RED, TLP:AMBER, TLP:GREEN, and TLP:CLEAR. In Figure 3, you can find an example of the TLP color-coding in RGB, CMYK and Hex from the organization FIRST, whose document in the Standards section is provided as a resource [29].

	RGB: font			RGB: background			CMYK: font				CMYK: background				Hex: font	Hex: background
	R	G	B	R	G	B	C	M	Y	K	C	M	Y	K		
TLP:RED	255	43	43	0	0	0	0	83	83	0	0	0	0	100	#FF2B2B	#000000
TLP:AMBER	255	192	0	0	0	0	0	25	100	0	0	0	0	100	#FFC000	#000000
TLP:GREEN	51	255	0	0	0	0	79	0	100	0	0	0	0	100	#33FF00	#000000
TLP:CLEAR	255	255	255	0	0	0	0	0	0	0	0	0	0	100	#FFFFFF	#000000

Figure 2 Example of the TLP color-coding in RGB, CMYK and Hex

In the process of sharing information, the source of the information needs to make sure that all recipients understand and will follow the TLP protocol. As a recipient of information, in order to share the information with a wider group than indicated, it is necessary to obtain explicit permission from the original source to do so.

In email messages, when TLP classified information is sent, the specific classification must be clearly readable in the subject of the email, at the beginning of the email before the information, and also at the end (commonly just below the signature) as shown in Figure 4. The labels themselves cannot be translated into the national language and need to be marked in capital letters. Documents containing TLP-classified information need to have the classification label in the header and footer of each page and on the first page under the document title.



The diagram illustrates an email composition interface. On the left is a 'Send' button with a paper plane icon. To its right are three input fields: 'From' (containing 'email@email.xy'), 'To', and 'Cc'. Below these fields is a 'Subject' field containing the text 'TLP:AMBER followed by the subject'. The 'TLP:AMBER' label is highlighted in red in the original image.

TLP:AMBER

Content of the email message followed by a signature.

TLP:AMBER

Figure 3 Example of TLP labelling in an email message

P-12: Information Sources Process

The official description of the parameter from the SIM3v2 [3]:

For each CSIRT it is mandatory to monitor and evaluate appropriate information sources. In addition to public web pages, this could be social media, mailing lists, security vendors, vulnerability databases or exploit sites, portals like pastebin or new alerts sent by information security providers. Regardless how many and what kind of information sources are monitored, the CSIRT needs to develop a process how to do this consistently with the appropriate scrutiny and quality assurance. It must be avoided that the CSIRT acts on wrong or manipulated input, as this will put the reputation of the team at risk. The process must also describe the life-cycle of sources, from being added to the CSIRT's list of information sources - which is T-2 - until removal for reasons of declining quality (or becoming void). Does your team have such a process, linked to the list of sources (T-2)?

Maturity levels:

1. *We never really discussed this.*
2. *We know how we do this, but have not documented this.*
3. *We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a formal written process approved by our team management.*
5. *We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended.*

This parameter focuses on the methods and systems used by a CSIRT to gather, analyze, and utilize information from various sources during incident management. This includes identifying and establishing relationships with internal and external information sources such as threat intelligence feeds, security advisories, and relevant databases. The parameter emphasizes the importance of having a structured process for collecting and validating information to ensure its accuracy and relevance. Additionally, it highlights the need for ongoing analysis to derive actionable insights that can inform incident response strategies and improve overall security posture. By effectively managing information sources, organizations can enhance their ability to anticipate, detect, and respond to security incidents in a timely manner.

P-13: Outreach Process

The official description of the parameter from the SIM3v2 [3]:

As the CSIRT offers service to its constituents, it needs to reach out to all constituents and stakeholders. By doing this, it promotes not only itself, but also the best practices and processes recommended by it. While awareness building might be seen as outreach, it is common to label awareness building as a CSIRT service, as it's part of incident prevention and thus core business. However, it is also essential to make sure that the constituency is actively aware of the CSIRT and the services offered. To 'advertise' the team in this way, is part of the outreach process. Equally important is that this process should allow for a two-way channel: the constituency also needs to be able to provide 'bottom-up' feedback to the team (not to be confused with the P-8 feedback which is 'top-down'). The outreach process should include all forms of activities that raise the visibility and reputation of the CSIRT, varying from webpages, via newsletters, webinars, white papers, conferences, etcetera. For any national CSIRT this would include reaching out to the critical infrastructure sectors and ISACs, again in two-way fashion. Does your team have an outreach process?

Maturity levels:

1. *We never really discussed this.*
2. *We know how we do this, but have not documented this.*
3. *We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a formal written process approved by our team management.*
5. *We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended.*

To meet the Outreach Process Parameter, organizations should focus on a minimum set of actions to ensure effective engagement with the constituency and stakeholders. Here are the possible steps:

- **Identify Key Stakeholders:**

Determine the primary audiences for outreach, including the employees, management, customers, partners, and relevant external organizations;

- **Create Basic Communication Channels:**

Establish at least one reliable communication channel, such as an email newsletter or a dedicated webpage, to disseminate information about security incidents, updates, and best practices;

- **Develop a Simple Outreach Plan:**

Outline a basic outreach plan that includes information about the services CSIRT provides, specific objectives, target audiences, and methods for communication;

- **Establish a Schedule for Regular Updates:**

Create a schedule for regular communications (e.g., quarterly updates) to keep stakeholders informed and engaged. Consistency is key to building trust and awareness.

P-14: Governance Reporting Process

The official description of the parameter from the SIM3v2 [3]:

By managing incidents for their constituency, the CSIRT gains critical insights otherwise not available to stakeholders, policy makers and even information security or data protection officers. As part of situational awareness (scope will be different according to the aim and objective of the particular CSIRT) the lessons learnt are important to be communicated and escalated. The governance reporting process needs to provide up-to-date reports and background explanations in order to better prevent and remedy similar incidents/attacks/risks in the future. Statistics and graphics based on the types (see O-8) and number of incidents, resources spent, funding levels, etc. are all part of the governance reporting process. Providing statistics to constituency or public, is covered by P-15. Does your CSIRT report to higher governance according to a set process?

Maturity levels:

1. *We never really discussed this.*
2. *We know how we do this, but have not documented this.*
3. *We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a formal written process approved by our team management.*
5. *We have a formal written process approved by our team management and by higher management. In the periodic review of our team it is checked if this process works as intended.*

The Governance Reporting Process Parameter outlines the framework for systematically reporting security incidents and incident management activities to the senior management and governance bodies. This process involves defining clear reporting structures, formats, and schedules to ensure the stakeholders are regularly informed about the organization's security posture, incident trends, and the effectiveness of response efforts. By establishing this reporting mechanism, organizations can enhance accountability, support informed decision-making, and align security initiatives with broader organizational goals.

P-15: Constituency Reporting Process

The official description of the parameter from the SIM3v2 [3]:

Whereas P-14 is about reporting to higher governance, P-15 is about reporting to the constituency - or even to the world at large (like e.g. several national teams do, in annual trend reports). Statistics and graphics may be included in such reporting - and just like for P-14, it is useful to base such more detailed reporting on the typology used for incidents (see O-8) - and to do that using a (semi-)automatic export from internal typology and numbers to the required external format(s). Note that there may be other reporting schemes, for example mandatory reporting according to national laws based on different premises. Does your team offer this kind of statistics to constituency or public, and is there a process for doing so?

Maturity levels:

N/A We have made an explicit choice not to report to our constituency or beyond.

1. *We never really discussed this.*

2. *We know how we do this, but have not documented this.*
3. *We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a formal written process approved by our team management.*
5. *We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended.*

The process of reporting incidents in terms of statistical data serves, in addition to internal recording, is an opportunity for the public to view the operations of a particular organisation. This may include educational activities towards raising security awareness, such as in-person and online lectures and workshops focused on various topics in the field of information and cyber security. Other possible activities could be the creation of educational content related to the topic of cybersecurity for all employees. This refers to the training of employees within the scope determined by each company individually. This can also involve practical workshops based on real experiences in handling cyber security incidents. Collaborations with other organisations can also be valuable in terms of contributing to the general awareness of the topic. Raising awareness is nowadays highly effective via social networking platforms such as Facebook, Instagram and LinkedIn. Ranging from basic information security concepts explained, current fraud campaigns, warnings about critical vulnerabilities, or specific days (e.g. backup day).

Within the TheHive system for managing and recording security incidents (T-4), it is possible to regularly produce a report of security incidents for a specified period. This is statistical data (numerical counts with assigned percentages), with segmentation possible based on different categories, e.g., type of incident or specific tags assigned. By selecting one of the chosen categories, it is possible to view the incidents in a particular context. The report also includes a generated graph showing the number of incidents recorded for the selected time.

P-16: Meeting Process

The official description of the parameter from the SIM3v2 [3]:

The CSIRT's internal communication and effectiveness can be greatly improved by regular meetings, usually weekly or even daily. Various needs exist, and also different organisation set-ups (including having people in more than one location), therefore no fixed schedule is imposed. But all teams need to consider the appropriate number of meetings, the scope of such meetings and their modus operandi: live, online or hybrid. As a minimum the meeting process needs to ensure that action points as well as lessons learnt are captured and distributed to all involved. As grounds can easily be found to cancel team meetings, the process must ensure that there is a mandatory minimum number of meetings that take place and are attended by the required mix of roles/persons. Allowing for hybrid team meetings make this goal easier to achieve. Does your team have a well defined meeting process?

Maturity levels:

1. *We never really discussed this.*
2. *We do meet regularly, but have not documented this.*
3. *We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a formal written process approved by our team management.*
5. *We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended.*

Each team should have a defined frequency of meetings that are necessary to achieve its goals. Meeting times should be defined internally with a list of invited participants. As evidence to confirm maturity within this parameter, the minutes of each meeting should be created. An example of what a meeting record might look like is provided below.

Table 2 – Example of meeting record.

Meeting Date: [Insert Date]		Time: [Insert Time]	Location/Platform: [Insert Location/Platform]		
Agenda Item	Discussion Points	Responsible Person	Action Items	Deadline	Follow-Up Date
Incident Review	Review of recent incidents (summary, root cause)	Incident Handler Lead	Prepare incident report	[Date]	[Date]
Threat Intelligence Updates	New threat trends, vulnerabilities	Threat Intelligence Lead	Share relevant threat data with the team	[Date]	[Date]
Policy/Procedure Updates	Review changes in response procedures	CSIRT Manager	Update incident response procedures	[Date]	[Date]
Training/Skill Development	Discuss upcoming training needs or gaps	HR/Training Coordinator	Organize next training session	[Date]	[Date]
Tool and Technology Assessment	Evaluate current tools, new solutions	Tech Lead	Propose upgrades or adjustments	[Date]	[Date]
Team Availability/On-call Rota	Discuss staffing needs, on-call rotation	CSIRT Manager	Finalize next month's rotation schedule	[Date]	[Date]
Action Items from Last Meeting	Status of pending tasks from the previous meeting	CSIRT Manager	Complete unfinished tasks	[Date]	[Date]

P-17: Peer Collaboration Process

The official description of the parameter from the SIM3v2 [3]:

It is important to be a member or part of relevant communities in order to foster trust relationships with other teams, in order to gain better information more timely, and to improve communication, both in terms of speed and of quality. Also, several teams will be part of a more hierarchically structured context - for example a CSIRT in a commercial organisation may need to report into a coordinating CSIRT on the corporate level - or lower level government teams may need to report into a national CSIRT. In all case such 'peer' relationships need to be defined and appropriate processes need to be defined on both sides. If there is a hierarchical structure, the consequences of this need to be clearly documented. When the peers are more like 'fellow' teams in a non-hierarchical context (e.g. the membership of FIRST, or of regional CSIRT cooperations), it still needs to be defined how those 'peers' work together and what expectations and processes are in place. Also it must be taken into account that 'peers' can obviously be other CSIRTs, but can also be found among other types of security teams like SOC, PSIRTs, ISACs, etcetera. Has your team defined what their various 'peers' are, and what the process(es) towards those peers is/are?

Minimum Requirement: The process must define what 'peers' exist and ensure that with those peers a two-way trusted communication is established.

Maturity levels:

1. *We never really discussed this.*
2. *We know how we do this, but have not documented this.*
3. *We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this.*
4. *We have a formal written process approved by our team management.*
5. *We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended.*

One of the essential elements, in addition to focusing on security within the organization, is being able to provide relevant information to other organizations that can support the way they operate. The importance of establishing partnerships with other organizations needs to be discussed either as ongoing cooperation among peers on the CSIRT teams or, more broadly, among organizations that share common characteristics. For instance, there may be organizations focusing on security in the health sector, banking or other sectors at national and/or international scale. However, a frequent area of concern is the question of information sharing. The most common topics include how to share information, what platform will be used for this, or how to share information anonymously. Nevertheless, despite the complexity of the process, some attacks that occurred in one organization were yet prevented in another organization in a time-saving manner.

The important aspect is to have defined how to cooperate and what are the principles that need to be respected by both parties. This can gradually build up a network of peers, whereby if one organization encounters a specific attack in one country, it can inform its surroundings, and the response time will decrease rapidly. For instance, in the case of a data leak, the crucial question is how to inform the organization of an ongoing attack that may not have been detected. If capturing information as a proactive activity, i.e., threat hunting, there is also another possibility, namely to forward it to the relevant organization.

2.2. SIM3 Maturity Assessment Tools

The SIM3 maturity assessment is based on appropriately prepared web forms/applications. A description of the method is presented in the subsection above. The maturity assessment form is available on the ENISA website <https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity/csirt-survey> [30].

A more extensive tool for examining the maturity of incident response in an organization is the SIM3 v2 interim Self-Assessment Tool, offered by the Open CSIRT Foundation, available at <https://sim3-check.opencsirt.org/>. Maturity assessments can be used to assess a CSIRT team, and it can serve as a self-assessment or an external assessment tool. This tool can also be used to improve the organization's cybersecurity services and functions. The tool is available free of charge under an Open-Source license. It is also possible to use the application for commercial purposes. The tool is used in many security organizations around the world.

Using the SIM3 Online Tool

The maturity level is assessed in four areas: (quadrants): O - Organisation, H - Human, T - Tools and P - Processes. The organization/team assessment consists in choosing from 5 levels (from 0 to 4) for the parameters characterizing each area. The concept of building the application assumes that each set of entered data will correspond to an appropriate URL. This approach eliminates the need to save the data entered for the organization as it is enough to save the current URL. To compare two test results, the corresponding URL can be simply copied. This comparison can be a change in the state of an organization or a comparison of two organizations. The creators of the form have provided a tool for comparing two states of the organization.

The maturity assessment process involves selecting the appropriate area (1) (Figure 1) and then determining the level for each parameter (2).

Figure 4 Assessment Form SIM3 v2 interim Self-Assessment Tool

Source: Based on the <https://sim3-check.opencsirt.org/>

The right part of the form contains the results of the assessment. The assessment looks at the relevant profile, from the FIRST Membership Baseline to TI Certification (3). Selecting the first tab (4) allows you to show the results of the evaluation in the form of a Spider-Chart (5). The subsequent tabs allow you to present the results in the form of a table, show the tasks necessary to meet the requirements of the selected profile as well as a comparison table for the two compared levels.

Spider-Chart

The Spider-Chart allows you to present the results of the SIM3 maturity analysis in a clear graphic form. The chart shows all the parameters, labelled and grouped into areas. To make things easier, selecting the appropriate point on the chart shows the selected parameter in the left window, which makes navigation easier. Figure 2 shows examples of parameters from 0-1 to 0-5 at levels 0 to 4, respectively, with the requirements for these parameters (for this profile) at level at least 3.

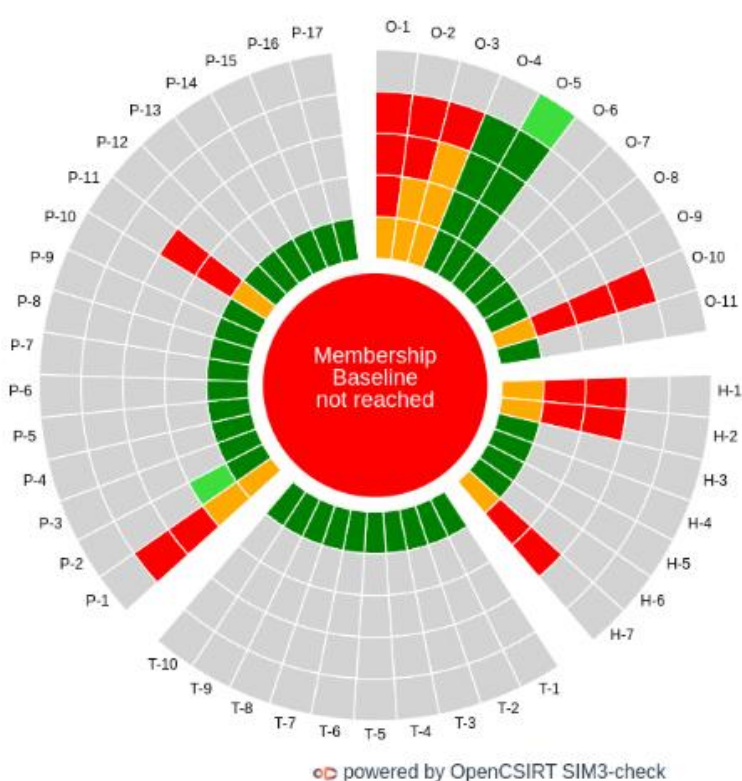


Figure 5 Spider-Chart in SIM3 v2 interim Self-Assessment Tool

Source: [31] Based on the <https://sim3-check.opencsirt.org/>

Appropriate colours indicate the level of implementation of a given parameter, green - the required level has been reached, red - the level below the requirements. In addition, light green indicates the level exceeding the requirements, and orange indicates partial compliance with the requirements. The requirements in the chart depend on the profile you choose, which makes this tool helpful in achieving the target maturity level of your team/organization.

Possibilities of using the tool at the university

The SIM3 online maturity assessment forms/applications can be used to assess the status of your organisation. However, their use can be much wider.

The SIM3 method can therefore be treated as a set of good practices that should be used by an organization that wants to meet appropriate cybersecurity standards. This can be a "reference model" for the application of appropriate practices.

In addition to assessing the current state, the adjustable tool facilitates increasing the level of cybersecurity by meeting the criteria indicated by the form for the appropriate level of organization (selected in the profile application). The application can also make it easier to document changes made to increase the level of security. Finally, demonstrating in the form that the appropriate criteria have been met is the basis for documenting that the team has achieved the appropriate level and, consequently, also enables certification.

Universities are organizations that must use appropriate management support tools to improve their security. One of such tools is SIM3 and an application supporting the organization assessment process. Due to the fact that universities are highly exposed to attacks in the area of cybersecurity, it is very important to be able to detect vulnerabilities in various areas. Performing a self-assessment (maturity) with the help of the presented tool is one of the first steps on the way to increasing the level of security. As a consequence, the detected deficiencies can be corrected, which will lead to an increase in the level of maturity of the university, up to meeting the requirements of the appropriate ENISA profile. The information obtained with the use of the SIM3 tool can be used to select tools designed to increase the level of university security (including software).

Universities can conduct such self-assessment on their own initiative in order to obtain appropriate management information. In the SOCCER project, the SIM3 assessment was considered necessary to carry out tasks aimed at increasing the level of university security. It was assumed that knowing the level of maturity of the organization is the basis for taking further actions.

Additional information on the use of the SIM3 method is discussed in the following chapters of the Toolbox for Academia.

References

- [1] "ENISA CSIRT maturity framework - updated and improved," ENISA, <https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework> [accessed Feb. 13, 2024].
- [2] Sim3 v2 interim standard - opencsirt.org, https://opencsirt.org/wp-content/uploads/2023/11/SIM3_v2_interim_standard.pdf [accessed Feb. 12, 2024].
- [3] Open CSIRT, 2024. SIM3 Check. Available at: <https://sim3-check.opencsirt.org/#/> [Accessed 30 Sept. 2024].
- [4] SIM3: Security Incident Management Maturity Model. Available at: <https://www.trusted-introducer.org/SIM3-Reference-Model.pdf>. [Accessed 30 Sept. 2024].
- [5] IETF, 1998. RFC 2350: Expectations for Computer Security Incident Response Teams (CSIRTs). Available at: <https://www.ietf.org/rfc/rfc2350.txt> [Accessed 30 Sept. 2024].

- [6] Software Engineering Institute, 2003. A Framework for Establishing Computer Security Incident Response Teams (CSIRTs). Available at: https://insights.sei.cmu.edu/documents/1606/2003_002_001_14102.pdf [Accessed 30 Sept. 2024].
- [7] DCAF, 2023. Guidebook for New CSIRT Employees. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/Guidebook_for_new_CSIRT_employees_EN_09032023.pdf [Accessed 30 Sept. 2024].
- [8] FIRST, 2021. CSIRT Services Framework Version 2.1. Available at: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1 [Accessed 30 Sept. 2024].
- [9] Atlassian, 2024. Incident Management: KPIs and Severity Levels. Available at: <https://www.atlassian.com/incident-management/kpis/severity-levels> [Accessed 30 Sept. 2024].
- [10] Trusted Introducer, 2016. Incident Classification Taxonomy. Available at: <https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf> [Accessed 30 Sept. 2024].
- [11] Reference Security Incident Taxonomy Task Force, Available at: <https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/tree/master> [Accessed 24 Nov. 2024]
- [12] European Commission, 2018. Cybersecurity Incident Taxonomy. Available at: https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf [Accessed 30 Sept. 2024].
- [13] TF-CSIRT, 2024. TF-CSIRT: Task Force for Computer Security Incident Response Teams in Europe. Available at: <https://tf-csirt.org/> [Accessed 30 Sept. 2024].
- [14] FIRST, 2024. FIRST: Forum of Incident Response and Security Teams. Available at: <https://www.first.org> [Accessed 30 Sept. 2024].
- [15] Insight Secure, 2024. P-COR Code of Conduct. Available at: <https://www.insightsecure.com/uploads/P-COR-Code-of-Conduct-V01.pdf> [Accessed 30 Sept. 2024].
- [16] CyberArk, 2024. Code of Conduct. Available at: <https://www.cyberark.com/Code-of-Conduct.pdf> [Accessed 30 Sept. 2024].
- [17] CLP Group, 2024. Code of Conduct. Available at: https://www.clpgroup.com/content/dam/clp-group/channels/about/document/value-framework/CLP_Code_of_Conduct_EN.pdf.coredownload.pdf [Accessed 30 Sept. 2024].
- [18] “How to set up CSIRT and SOC,” ENISA, <https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc> [Accessed Feb. 13, 2024].
- [19] AlertOps, 2024. AlertOps: Incident Management Platform. Available at: <https://alertops.com/> [Accessed 30 Sept. 2024].
- [20] AT&T Cybersecurity, 2024. OSSIM: Open Source SIEM. Available at: <https://cybersecurity.att.com/products/ossim> [Accessed 30 Sept. 2024].
- [21] Wazuh, 2024. Wazuh: Security Monitoring and Incident Response. Available at: <https://wazuh.com> [Accessed 30 Sept. 2024].
- [22] Cyberlands, 2024. Top 10 Incident Response Tools. Available at: <https://www.cyberlands.io/top10incidentresponsetools> [Accessed 30 Sept. 2024].
- [23] TheHive Project, 2024. TheHive Project: Open Source Security Incident Response Platform. Available at: <https://github.com/TheHive-Project/TheHive> [Accessed 30 Sept. 2024].
- [24] Shodan, 2024. Shodan: Search Engine for Internet-connected Devices. Available at: <https://www.shodan.io> [Accessed 30 Sept. 2024].
- [25] Have I Been Pwned, 2024. Have I Been Pwned?. Available at: <https://haveibeenpwned.com/> [Accessed 30 Sept. 2024].

[26] OWASP, 2024. Vulnerability Scanning Tools. Available at: https://owasp.org/www-community/Vulnerability_Scanning_Tools [Accessed 30 Sept. 2024].

[27] Tenable, 2024. Web Application Scanning. Available at: <https://www.tenable.com/products/web-app-scanning> [Accessed 30 Sept. 2024].

[28] PortSwigger, 2024. PortSwigger: Web Security Solutions. Available at: <https://portswigger.net> [Accessed 1 Oct. 2024].

[29] FIRST, 2024. TLP: Traffic Light Protocol. Available at: <https://www.first.org/tlp> [Accessed 30 Sept. 2024].

[30] "SIM3v1 self-assessment tool" ENISA, <https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity/csirt-survey> [Accessed Oct. 11, 2024].

[31] "SIM3 v2 interim Self Assessment Tool" Opencsirt, <https://sim3-check.opencsirt.org/#/> [Accessed Oct. 11, 2024].

3. SOC organizational and environmental requirements for Academia

3.1. Context in EU Academia

The operating context of European Union (EU) academia encompasses the multifaceted environment in which universities function, addressing their structural framework, governance, stakeholder interactions, operational paradigms, collaborative dynamics, and the inherent challenges they face.

How universities navigate and fulfil their educational and research missions within the EU landscape

Table 1 – Operating context in EU academia

General Structure	EU universities typically share a common structural framework characterized by a hierarchical organization that includes faculties and schools, departments, research centers, and administrative units. This structure facilitates the division of academic disciplines, promotes specialized research, and ensures efficient management of educational programs. Most universities adopt a modular system, allowing for flexibility in course offerings and degree programs to cater to diverse academic interests and evolving industry demands.
Management and Governance	University governance in the EU is generally a collaborative process involving various bodies such as the university senate, board of trustees, and administrative leadership including vice-chancellors or presidents. Decision-making authority is often distributed among academic and administrative leaders to balance academic freedom with organizational accountability. Governance structures are designed to promote transparency, inclusivity, and responsiveness to both internal and external pressures, ensuring that strategic objectives align with educational standards and societal needs.

Stakeholders:	1. Internal Stakeholders: 1. Students. Central to the academic mission, students drive demand for quality education, diverse programs, and supportive services. 2. Faculty and Researchers. Responsible for teaching, conducting research, and contributing to the university's intellectual capital. 3. Administrative Staff. Support the operational functions, including admissions, finance, human resources, and facilities management. 4. Alumni. Serve as ambassadors, potential donors, and contributors to the university's reputation and networking opportunities.
	2. External Stakeholders: 1. Government and Regulatory Bodies. Influence funding, accreditation, and policy compliance. 2. Industry Partners. Collaborate on research projects, provide funding, facilitate internships and employment opportunities for graduates. 3. Community and Society. Benefit from the university's

	educational services, research outputs, and societal contributions. 4. International Partners. Engage in cross-border collaborations, student exchanges, and joint research initiatives, enhancing the university's global footprint.
Operating Model / Open Model	EU universities predominantly operate under an open model, emphasizing accessibility, inclusivity, and collaboration. This model supports: • Open Access to Education. Promoting diverse entry points for students from various backgrounds. • Collaborative Research. Encouraging interdisciplinary and cross-institutional research efforts. • Knowledge Sharing. Facilitating the dissemination of research findings through open publications and conferences. • Flexible Learning Pathways. Allowing students to tailor their educational experiences to individual interests and career goals.
Flexibility in Scientific Collaboration	Scientific collaboration within EU academia necessitates flexibility to accommodate diverse research agendas, interdisciplinary approaches, and varying institutional priorities. Flexibility in collaboration is crucial for fostering innovation, enhancing research impact, and addressing emergent scientific and societal issues effectively. Key aspects include: • Adaptive Partnerships. Forming dynamic alliances with other universities, research institutions, and industry partners to leverage complementary strengths. • Funding Mechanisms. Utilizing diverse funding sources, including EU grants, private sector investments, and collaborative projects to support flexible research initiatives. • Technological Infrastructure. Implementing robust IT systems and communication platforms to facilitate seamless collaboration across geographical and disciplinary boundaries.

	• Regulatory Compliance. Navigating differing national regulations and standards to enable smooth cooperative research endeavors.
Challenges Arising from Academic and Educational Needs	EU universities face several challenges stemming from their academic and educational mandates, including: 1. Protection Requirements for Infrastructure. Universities must ensure that both their physical and digital infrastructures comply with varying protection standards to safeguard research data, intellectual property, and personal information. This encompasses: a. Data Protection and Privacy. Handling research data and personal information necessitates strict adherence to regulations such as the General Data Protection Regulation (GDPR). Universities must continuously monitor compliance and adapt to new legal requirements to protect sensitive information effectively. b. Cybersecurity. Protecting digital assets from cyber threats requires significant investment in advanced security technologies and practices. This includes implementing robust firewalls, encryption, regular security audits, and training staff and students on best practices to prevent data breaches and cyber-attacks. c. Physical Infrastructure Security. Research facilities and educational spaces must be secured against physical threats like theft, vandalism, and natural disasters. This involves regular risk assessments, implementing security measures such as surveillance systems, access controls, and disaster recovery plans to ensure the safety and integrity of university premises. 2. Balancing Tradition and Innovation a. Innovative Teaching Methods. Incorporating new technologies, such as digital learning tools, interactive platforms, and remote learning options, enhances teaching effectiveness and meets the evolving needs of modern students. This includes adopting blended learning models, leveraging artificial intelligence for personalized education, and utilizing online resources to complement traditional classroom instruction.

	b. Research Practices. Encouraging innovative research methodologies and interdisciplinary projects can lead to groundbreaking discoveries and advancements. Universities must foster an environment that supports creativity, collaboration across disciplines, and the exploration of novel research areas to stay at the forefront of scientific and academic progress.
Efficient distribution of limited resources is essential to support a wide range of academic programs, research projects, and infrastructural needs	• Funding. Optimally allocating budgets across different faculties and research areas ensures that priority sectors receive adequate funding. This involves strategic financial planning, identifying high-impact areas for investment, and balancing short-term needs with long-term institutional goals. • Human Resources. Managing personnel needs, including the recruitment, training, and career development of faculty and researchers, is vital for maintaining high academic standards. Universities must invest in professional development programs, create attractive career paths, and ensure a supportive work environment to attract and retain top talent. • Infrastructure. Investing in research equipment, libraries, laboratories, and other essential infrastructure is necessary for quality education and research. This includes upgrading facilities to incorporate the latest technologies, expanding physical spaces to accommodate growing student populations, and maintaining existing infrastructure to ensure it meets current academic and research demands.
Universities must continuously adapt their curricula and research focus areas to align with evolving labor market demands, technological advancements, and societal challenges	• Curriculum Updates. Integrating new disciplines and skills, such as artificial intelligence, sustainability, and data analytics, prepares students for future job markets. This involves regularly reviewing and updating course offerings, incorporating industry-relevant skills, and fostering critical thinking and adaptability among students. • Research Directions. Focusing on contemporary societal issues, such as climate change, healthcare, and digital transformation, enables universities to contribute to practical solutions and innovations. This requires identifying emerging research areas, securing funding for relevant projects, and promoting interdisciplinary collaborations to address complex challenges.

	• Industry Collaboration. Encouraging partnerships with the business sector helps universities understand market needs and integrate them into academic activities. Collaborations can lead to joint research initiatives, internship opportunities for students, and the development of programs tailored to industry requirements, enhancing employability and practical relevance.
Globalization presents universities with various challenges related to international competition, mobility of students and staff, and maintaining international partnerships amid geopolitical uncertainties	• Striving for high academic rankings and international reputation is essential to attract top students and faculty from around the world. This involves enhancing research output, improving teaching quality, and building a strong global brand through marketing and international collaborations. • Mobility. Managing the movement of students and staff between institutions requires efficient visa processes and the recognition of qualifications across different countries. Universities must facilitate seamless mobility through supportive policies, international offices, and agreements that simplify the exchange and recognition of academic credentials. • International Partnerships. Developing and maintaining strategic partnerships with foreign universities and research institutions is crucial, despite geopolitical instabilities and changes. This involves negotiating agreements that withstand political shifts, fostering long-term collaborations, and ensuring mutual benefits to sustain international cooperation. • Cultural Diversity. Promoting cultural dialogue and integration within the university community creates an inclusive and welcoming environment for all international members. Universities must implement initiatives that celebrate diversity, provide support for international students and staff, and encourage cross-cultural interactions to enhance the overall academic experience.

Security Operations Centers (SOCs) in the EU public academic context

In the context of the EU's academic sector, the establishment and maintenance of Security Operations Centers (SOCs) is critical for safeguarding the integrity, confidentiality, and availability of institutional data and research. A SOC serves as the central hub for monitoring, detecting, responding to, and mitigating cybersecurity threats. Given the unique characteristics of the academic sector, particularly within

public universities, the SOC must adapt to specific operational dynamics and collaborative frameworks.

A **Security Operations Center (SOC)** is a centralized unit that addresses security issues at both organizational and technical levels. In the context of EU public universities, the SOC's primary objectives are as follows:

- a. **Continuous Monitoring:** Monitoring network activities to detect and respond to threats in real time.
- b. **Incident Response:** Coordinating actions to mitigate the impact of security breaches.
- c. **Threat Intelligence:** Collecting and analyzing data to anticipate and prevent potential security incidents.
- d. **Compliance Management:** Ensuring adherence to relevant laws, regulations, and institutional policies.

Sector-specific (academia) needs

Research collaboration within EU public universities involves extensive data transfer, as these institutions frequently engage in projects both internally and with external partners. Such collaborations often require sharing large volumes of data across departments, research centers, and international institutions. The scale of data exchange necessitates robust and efficient data management systems to ensure seamless communication and coordination among all parties involved. Effective handling of high-volume data transfers not only enhances the productivity and outcomes of research projects, but also supports the interdisciplinary nature of modern scientific inquiry, where diverse expertise and resources are pooled to tackle complex global challenges. Research data in public universities is inherently sensitive, encompassing proprietary information, personal data, and valuable intellectual property. Protecting this information requires stringent security measures to prevent unauthorized access, data breaches, and intellectual property theft. Universities must implement comprehensive data protection strategies, including encryption, secure storage solutions, and strict access controls, to safeguard their research outputs. Additionally, compliance with regulations such as the General Data Protection Regulation (GDPR) is essential to ensure responsible and ethical handling of personal data. By prioritizing the security of sensitive research data, universities can maintain the integrity of their research activities and uphold their reputations as trusted institutions of higher education.

Moreover, the dynamic access needs of researchers pose significant challenges for Security Operations Centers (SOCs) in public universities. Researchers often require varying levels of access to different systems and data repositories based on the specific requirements of their projects. This necessitates a flexible and adaptive access management framework that accommodates diverse access permissions while maintaining stringent security standards. Implementing role-based access control (RBAC) and leveraging advanced identity and access management (IAM) solutions can help dynamically assign and revoke access rights as project needs evolve. Additionally, continuous monitoring and auditing of access patterns are essential to detecting and responding to anomalies or unauthorized access attempts. By effectively managing dynamic access needs, SOC's can support a collaborative research environment while ensuring that sensitive data remains protected.

In the EU academic context, universities increasingly integrate Operational Technology (OT) and Internet of Things (IoT) infrastructures into both their research initiatives and

daily operations. OT systems, which control physical devices and processes, are essential in laboratories, smart classrooms, and campus management systems, while IoT devices enhance connectivity and automation across campus facilities. The Security Operations Center (SOC) must address the unique vulnerabilities associated with these technologies. This includes implementing robust network segmentation to isolate OT and IoT devices from the main IT infrastructure, ensuring that any compromise in these systems does not cascade into critical academic or administrative functions. Additionally, regular firmware updates and patch management are crucial to protecting against known vulnerabilities in OT and IoT devices. For example, universities employ specialized monitoring tools within their SOC to continuously oversee IoT device activity, swiftly identifying and mitigating potential threats before they can impact research or campus operations. [1]

Universities often collaborate with a diverse array of external partners, including other academic institutions, scientific organizations, and commercial entities. These collaborations frequently involve a large number of external collaborators and guests who may not be bound by long-term contracts. This transient nature poses significant security challenges, as the SOC must efficiently manage temporary access rights and ensure that external users do not inadvertently introduce vulnerabilities into the university's network. Implementing automated access management systems that can grant and revoke permissions based on predefined criteria is essential for maintaining security without hindering collaborative efforts.

For instance, the University of Helsinki [2] utilizes role-based access control (RBAC) systems that dynamically adjust access levels for external partners, ensuring that sensitive data remains protected while facilitating seamless collaboration. Furthermore, standardized security agreements and non-disclosure agreements (NDAs) are enforced to ensure that all external parties adhere to the university's security protocols, thereby safeguarding intellectual property and proprietary research data.

The organization of public events at universities introduces additional layers of complexity to both IT and physical security. Large gatherings, such as conferences, seminars, and public lectures, can significantly impact the security infrastructure by increasing the number of devices connected to the network and the number of individuals accessing campus facilities. The SOC must implement event-specific security measures to mitigate risks such as Distributed Denial of Service (DDoS) attacks, unauthorized access to sensitive areas, and the potential for physical breaches. This can include deploying temporary network segments for event attendees, enhancing surveillance systems, and coordinating with physical security teams to monitor and control access points.

The SOC coordinates closely with campus security during major events to ensure that both digital and physical security measures are seamlessly integrated, preventing unauthorized access and maintaining the integrity of the university's IT systems during high-traffic periods.

Organizational dispersion, particularly in large universities with multiple campuses and decentralized departments, presents significant challenges for maintaining consistent security protocols and effective SOC operations. Dispersed infrastructures can lead to fragmented security practices, making it difficult to enforce uniform policies and respond swiftly to incidents across locations. To address this, SOC must adopt centralized security management systems that provide comprehensive visibility and control over the entire university network, regardless of geographical dispersion. Implementing unified Security Information and Event Management (SIEM) platforms allows for the aggregation and analysis of security data from all campuses, enabling real-

time threat detection and coordinated incident response. Additionally, standardized security policies and regular training programs ensure that all dispersed units adhere to the same security standards.

Other compliance requirements

In addition to the primary regulations outlined previously, EU public academic institutions must adhere to a variety of additional compliance requirements to ensure comprehensive information security and operational integrity. These requirements encompass international standards, local and national regulations, as well as organizational policies governing critical infrastructure protection. Adhering to these standards not only fortifies the institution's security posture, but also enhances its credibility and trustworthiness among stakeholders. Key standards and frameworks that universities should consider include ISO/IEC 27001 for information security management, ISO/IEC 27701 for privacy information management, and national regulations tailored to protect critical infrastructure within each member state.

Academic institutions are also subject to local, national, and organizational regulations that specifically address the protection of critical infrastructure. These regulations mandate stringent security measures to safeguard essential services and research facilities from potential threats. Compliance with these regulations involves implementing robust risk management practices, conducting regular security assessments, and ensuring that all critical systems are resilient against disruptions. For example, universities must secure their research laboratories, data centers, and campus management systems by adhering to guidelines set forth by national cybersecurity agencies, and aligning with EU-wide directives such as the Network and Information Security (NIS2) Directive. Additionally, organizational policies must be consistently applied across all departments to maintain a unified approach to critical infrastructure protection.

Collaboration with scientific and industrial partners introduces another layer of compliance requirements for universities. Companies and research organizations often impose specific security standards on their suppliers to protect their own data and intellectual property. Universities must meet these supplier requirements to maintain and foster these valuable partnerships. This includes adhering to stringent security protocols, obtaining necessary certifications such as ISO/IEC 27001, and complying with contractual obligations outlined in non-disclosure agreements (NDAs). Effective management of these requirements ensures that collaborative projects proceed smoothly without compromising the security of shared information. Universities must establish clear guidelines and standardized procedures for handling sensitive data and enforcing NDAs to uphold the integrity of their research collaborations.

Data-sharing policies play a crucial role in compliance, especially in the context of international projects funded by EU grants. These policies must address the secure exchange of data between multiple stakeholders, ensuring that all parties adhere to the same security standards and regulatory requirements. Compliance with data-sharing policies involves implementing robust encryption methods, establishing secure data transfer protocols, and ensuring that all data exchanges are logged and monitored for unauthorized access or breaches. Additionally, universities must align their data-sharing practices with the FAIR principles (Findable, Accessible, Interoperable, and Reusable) to enhance the usability of research data while maintaining its security. Proper compliance with these policies not only protects sensitive information, but also ensures the successful execution and funding continuity of international research initiatives.

Ensuring an appropriate level of auditing and monitoring is essential for maintaining compliance with all relevant guidelines and standards. Universities must implement comprehensive auditing frameworks that regularly assess adherence to information security policies, regulatory requirements, and contractual obligations. This involves conducting both internal and external audits to evaluate the effectiveness of security measures, and to identify areas for improvement. Continuous monitoring using Security Information and Event Management (SIEM) systems enables real-time detection of potential compliance breaches and facilitates swift incident response. Additionally, maintaining detailed audit trails and documentation supports transparency and accountability, allowing institutions to demonstrate their compliance efforts to regulators, partners, and funding bodies. By prioritizing rigorous auditing and monitoring practices, universities can proactively address compliance gaps and reinforce their commitment to maintaining a secure and trustworthy academic environment.

3.2. Legal and regulatory environment (EU level and per member country)

Introduction

In an era of increasing cyberthreats and information security incidents, ensuring data protection and the stability of information systems is a priority for every organization, including universities. Security Operations Centers (hereinafter referred to as SOC) play a key role in monitoring, managing, and responding to security incidents. However, to operate effectively, they must function in accordance with applicable laws and regulations, which vary depending on the regional level (European Union) and the national level (individual member states).

The significance of legal regulations for SOC in universities

Universities are particularly vulnerable to cyberthreats due to a wide range of data they process, including personal information of students and staff, research results, and other sensitive information. A breach of this data can lead to serious legal, financial, and reputational consequences. Therefore, adherence to the appropriate legal regulations and standards in the field of cybersecurity is crucial for the proper functioning of a SOC.

Regulations at the European Union level

It is worth emphasizing that, in the context of establishing SOC at the European Union level, there are no clear, dedicated legal provisions that directly specify the requirements for their creation and operation. However, this does not mean that organizations choosing to establish a SOC operate in a regulatory vacuum. On the contrary, SOC must operate in accordance with legal acts and standards related to data protection, cybersecurity, and incident management. These regulations are general in nature and cover various aspects of activities related to the monitoring and protection of information systems, which means that although there are no dedicated legal standards, they indirectly regulate the activities of a SOC.

The European Union, aiming to create a unified digital market and ensure a high level of personal data protection and information security, has introduced several legal acts that directly impact the functioning of SOC. Among the most important of these are:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) – <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) – <https://eur-lex.europa.eu/eli/dir/2022/2555>

Directive NIS 2

The fundamental legal act governing the functioning of SOC is the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (hereinafter referred to as the NIS2 Directive).

In 2016, in response to changing cyberthreats and the need to strengthen resilience against cyberattacks, the European Union introduced a Directive NIS - (Network and Information Systems Directive) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. This directive marked the first step towards enhancing the security of networks and information systems on the EU level. However, in the face of a rapidly evolving threat landscape, in 2022 the European Union adopted an updated version of this directive - Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

The underlying assumption on which the NIS2 Directive is based is that the entities covered are categorized as essential or important, which affects the scope of obligations, potential penalties, and the extent of oversight over the specified entities. In this context, it is important to pay attention to the organizational aspect related to running a SOC by the university. If the SOC is to be established within the internal structure of the university, meaning that the SOC will be an organizational unit within the university, then national regulations adopted to implement the directive should apply. The EU directive binds the state only in terms of the results, which means that each member state has the freedom to choose the form and means of implementation. As an example, it is worthwhile to mention the draft amendment to the Polish Act on the National Cybersecurity System, which implements the provisions of the directive. According to the proposed law, public universities, inter alia, will be categorized as essential entities. Hence, due to the fact that the university should be recognized by the law as an essential entity, all internal structures responsible for information security, such as the SOC, will have to comply with the requirements of this NIS2 Directive abiding by the acts implementing the directive. This means that the SOC will need to implement appropriate procedures and cybersecurity protection measures in accordance with the requirements for risk management, incident reporting, and business continuity that apply to essential entities.

In the case of establishing a SOC as a separate entity, apart from the internal structure of the university, attention should be paid to the wording of Article 3, paragraph 1, item a) of the NIS2 Directive whereby essential entities are considered to be entities of a type referred to in Annex I which goes beyond the framework set for medium-sized

enterprises provided for in Article 2 paragraph 1 of the Annex to Recommendation 2003/361/EC. According to the relevant recommendation, a medium-sized entrepreneur is defined as one who employs up to 250 employees, has a turnover not exceeding 50 million euros, and a total annual balance not exceeding 43 million euros.

At this point, reference should be made to Annex I of the NIS2 Directive. NIS2 Directive lists among the essential entities also the ICT service management sector, including managed security service providers. According to Article 6 item 40, a managed security service provider is defined as a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management. Such entities can be recognized as organizations like Security Operations Centers, Computer Security Incident Response Teams, and Computer Emergency Response Teams. It is essential to note, however, that even if an entity is not categorised as an essential entity, it can still operate as an important entity under the NIS2 Directive. The NIS2 Directive in Article 3 paragraph 2, adopted the principle whereby entities of the type referred to in Annex I or II which do not qualify as essential entities pursuant to paragraph 1 of this Article shall be considered to be important entities.

Whether the entity is categorized as essential or important does not really affect the scope of its obligations. Under the NIS2 Directive, essential entities and important entities have the same obligations. They mainly focus on implementing appropriate risk management measures, outlined primarily in Article 21, as well as fulfilling incident reporting obligations in accordance with the provisions of Article 23 of the NIS2 Directive. Differences in subjective classification are mostly revealed in the supervisory measures that authorities can exercise over essential or important entities, as well as the scope of penalties that can be imposed on individual entities. Thus, when creating a SOC, it is necessary to consider not only the NIS2 Directive but also the national regulations adopted so that the directive should be implemented on the national level.

It should also be emphasized that according to Article 21 paragraph 5 of the NIS2 Directive, by October 17, 2024, the European Commission will adopt implementing acts specifying the technical requirements and methodology regarding cybersecurity risk management measures, including those related to managed security service providers. Implementing acts are aimed to ensure uniform conditions for the execution of legally binding acts within the European Union. In this regard, the Commission Implementing Regulation 2024/2690 provided rules for the application of Directive (EU) 2022/2555 relating to technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers. The main objective of this regulation is to define the technical and methodological requirements concerning the measures referred to in Article 21 (2) item (a) to (j) of the NIS2 Directive. These are cybersecurity risk management measures that have been specified and detailed in the annex to the Implementing Regulation. According to Article 2 (2) of the Commission Implementing Regulation relevant entities shall take a due account of the degree of their exposure to risks, their size and the likelihood of occurrence of incidents and their severity, including their societal and economic impacts, when complying with the technical and methodological requirements of cybersecurity risk-management measures set out in the Annex to this Regulation. System protection must be appropriately tailored to handle the threats and their potential consequences, taking into account the specifics of the given entity. SOC, as an entity subject to the NIS2 Directive, must take into account the provisions of the relevant Implementing Regulation. One has to bear in mind that the

technical and methodological requirements concerning risk management measures in cybersecurity specified in the annex to the Commission Implementing Regulation are based on European and international standards such as ISO/IEC 27001, ISO/IEC 27002, ETSI EN 319401 and technical specifications such as CEN/TS 18026:2024.

GDPR Regulation

When organizing a SOC, of major importance is the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - General Data Protection Regulation (hereinafter referred as GDPR). SOC collects and processes various data to monitor, analyze, and respond to security incidents in IT systems. These data are crucial for the functioning of this organization, namely identifying threats, analyzing trends, and securing infrastructure. In the context of GDPR, the SOC must pay particular attention to what personal data is being collected and how it is being processed.

One type of data collected by the SOC is the system and network logs. These are some of the fundamental data sources in a SOC. They include, inter alia:

- a) IP addresses – identifiers of devices on the network;
- b) Time stamps – information about login times, access attempts, data operations, and similar activities and such like;
- c) User identifiers: usernames, account identifiers, computer names;
- d) Details regarding the session: information about the start, end, and duration of the user's session.

From the perspective of GDPR, the scope of information recorded in the event logs, as detailed above, can be considered personal data. The motive number 30 of the GDPR, is recalled, which has it that: “Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them”. Information that is associated with a specific person – even indirectly – carries a certain message about them. In practice, this means that while monitoring activities in the SOC system, such data may be processed yet in compliance with GDPR requirements.

In the context of the SOC, it is important to examine who will serve as the controller and the entity processing personal data. The controller is the entity that determines the purposes and means of processing personal data. In the case of universities, the controller will usually be the university itself, as it decides what type of data is processed, for what purpose (e.g., to ensure the security of systems), and how long it is retained. The SOC, which operates as a technical unit responsible for monitoring systems and processing data in tasks related to IT security will act as a data processor. The SOC does not independently decide the purpose for which data is processed and what type of data is collected – these decisions are made by the controller, that is the university. The SOC only performs tasks related to data analysis and processing at the request of the university.

At this point, one should bear in mind that if the SOC is managed by an external entity (e.g., a company providing IT security services), it is necessary to conclude a data processing agreement between the university (the controller) and the company

operating the SOC (the data processor). In specific situations, the SOC may become the controller, but only when:

- independently decides on the purposes and means of data processing,
- when conducting separate activities, independently of the university's guidelines, regarding the collection and processing of data.

However, such situations are rather rare, especially in the context of universities, where the SOC usually serves a technical and executive role on behalf of the university as a controller.

In this respect a SOC as a data processor should:

- a) process data based on the controller's instructions – the SOC can operate only according to the controller's instructions,
- b) ensure data protection measures – the SOC should implement appropriate technical and organizational measures to protect the data it processes,
- c) ensure confidentiality – SOC employees must be obligated to maintain confidentiality regarding the processed data,
- d) reporting a personal data breach – the SOC must immediately inform the controller of any personal data breaches.

Another regulation which needs to be recalled when we creating a SOC is the Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act, hereinafter CRA).

CRA is a legislative initiative designed to improve the cybersecurity of goods that contain digital components. In order to guarantee that software and hardware are developed, produced, and maintained with strong cybersecurity safeguards throughout their whole lifecycle, CRA creates consistent regulatory frameworks. Manufacturers are required by CRA to perform risk assessments, issue security upgrades, and adhere to basic cybersecurity regulations. The provisions of this act may have an indirect impact on how a SOC operates, even while its primary goal is to guarantee high security standards for products with digital components, including obligations for producers to obtain certification and criteria for resilience to cyberattacks. CRA can influence the SOC operations through:

- Integration with digital products: in the case of using solutions or services that are subject to the CRA, the SOC should take into account the certification and compliance requirements for these products
- Supply chain risk management: The CRA introduces requirements aimed at increasing the security of the entire supply chain of digital products, which may impact on risk assessment and security policy within the SOC.

In summary, although the CRA does not directly regulate the operational activities of a SOC, the relevant provisions have to be recalled when selecting technology, managing risk and designing security processes to enhance the organization's overall cybersecurity.

Legal and regulatory environment per member country

Cybersecurity and data protection in Slovakia

The applicable national and European cybersecurity legislation

- Act No. 69/2018 Coll. on cybersecurity as amended
- Act No. 95/2019 Coll. on information technology in public administration as amended
- Act No. 18/2018 Coll. on personal data protection as amended
- Act No. 452/2021 Coll. on electronic communications
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

and corresponding decrees implementing the applicable legislation

Position of CSIRT and SOC

The term **CSIRT (Computer Security Incident Response Team)** refers to a security team whose operation falls within the scope of cyber security. The main task of security teams formed within specific organizations is primarily to deal with security incidents that have arisen within the organization concerned (so-called reactive activities). Other tasks of security teams include preventive activities aimed at averting the occurrence of security incidents in various ways, for example by educating those working within the organization, introducing technologies capable of preventing the leakage of sensitive data, etc.

The term **SOC (Security Operations Center)** refers to a security operations center whose activities are focused on continuous monitoring and data collection for the purpose of identifying potential security events and incidents in monitored organizations and thus for the purpose of obtaining information about the overall state of the respective organization. The said monitoring includes the monitoring of the infrastructure used within the organization as well as the activities of individual users making use of this infrastructure.

Personal data protection

In this context, questions arise in relation to the application of different legal regimes. Of particular importance is **regulation of the protection of personal data** that will necessarily be processed as a part of the monitoring, taking into account the limits set by the relevant legislation, in particular the definition of the applicable legal framework for the processing and the provision of transparent information to users about the

monitoring realized to the extent required by the legislation. The relevant legal framework is provided in the following legislation:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
- Act No. 18/2018 Coll. on personal data protection as amended

Underlying the legal framework for personal data processing are the legal bases applicable in the examined context:

- **processing is necessary for compliance with a legal obligation** to which the controller is subject, specifically with a legal obligation stemming from the specific national legislation or international agreement, to which the Slovak republic is subject to under Article 13 (1) (c) of the Act No. 18/2018 Coll.
- **processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child; this legal basis does not apply to the processing of personal data by public authorities in the performance of their tasks according to Article 13 (1) (e) of Act No. 18/2018 Coll. In the case of reference to the legitimate interest of the operator as the legal basis for the processing of personal data, the prerequisite for its use will be the **performance of a proportionality test** for each type of monitoring activity, in order to assess whether the interests or fundamental rights of the data subject requiring the protection of their personal data do not prevail over the legitimate interests of the controller – UPJŠ.

A specific feature of the national legislation is the **dual regulation of personal data protection** contained on the one hand in the General Data Protection Regulation (GDPR), which is directly applicable in the Slovak legal order due to the very nature of this legal act, and on the other hand in the special Act No. 18/2018 Coll. As regards the relationship between these legal acts, according to the Office for Personal Data Protection of the Slovak Republic (hereinafter referred to as the "Office"), the adoption of the Act in question is the result of the alignment of the Slovak national legislation with the GDPR. Concurrently, given the wording of Article 2 (2) (a) GDPR, according to which the Regulation does not apply to the processing of personal data in the course of an activity which does not fall within the scope of Union law, the legislator decided to adopt a specific national law (its wording almost to GDPR) regulating these unique processing activities in order that processing of personal data should be subject to the same rules as those provided in the GDPR. In this context, the Office distinguishes three possible situations that may arise:

- **Processing of personal data in the course of an activity falling under the scope of EU law:** if the processing of personal data is in the course of an activity of the controller that falls under EU law, the GDPR will apply to the controller, but Act No.18/2018 Coll. will also apply with the exception of its Section 2 and 3. The Act

No. 18/2018 Coll. will therefore apply as regard its Section 1 (with the exception of Articles 2 and 5) and Section 4, 5 and 6. This has relevance, for example, to the processing of personal data by banks, schools, health care institutions, processing of personal data in e-shops.

- **Processing of personal data within the framework of an activity that does not fall within the scope of Union law:** if the processing of personal data takes place within the framework of an activity of the controller that does not fall within the scope of Union law and the controller is not a competent authority, Act No. 18/2018 Coll. (with the exception of its Section 3) will apply.
- **Processing of personal data for law enforcement purposes:** In the case of processing the personal data by the controller in the capacity of a competent authority, it shall proceed with the processing of personal data of natural persons for the purposes of prevention, investigation, detection or prosecution of criminal offenses or for the purposes of execution of criminal penalties pursuant to Act No. 18/2018 Coll., specifically Section 1, 3, 4, 5 and 6 with regard to specific provisions of Section 2. This relates, for example, to the processing of personal data of a person accused of a criminal offense, when their personal data is processed by the public prosecutor's office or by a court of law.

For better clarity, Table 2 provides an overview of the Act No. 18/2018 Coll. on personal data protection as amended.

Table 2 - Overview of the Act No. 18/2018 Coll. on personal data protection as amended

The division of the Act No. 18/2018 Coll. on personal data protection as amended	Processing of personal data in the course of an activity falling under the scope of EU law	Processing of personal data within the framework of an activity that does not fall within the scope of Union law	Processing of personal data for law enforcement purposes
SECTION 1: Main provisions (Articles 1 – 5)	Articles 1, 3 and 4	The whole section is applied.	The whole section is applied.
SECTION 2: General data protection rules (Articles 6 to 51) Principles of personal data processing Rights of the data subject Rights and obligations of the controller and the processor Transfer of personal data to a third country or international organization	This Section does not apply.	The whole section is applied.	Only these Articles are applicable: 6, 8, 9, 11, 12, 13 (2), 29, 31, 32, 33 (1) (3), 34, 36, 37, 39, 40, 41, 42 (1 to 5 and 7, 44, 45, 46, 48 (1) and 50
SECTION 3: Special rules for the protection of personal data of natural persons when processed by competent authorities (Articles 52 to 77)	This Section does not apply.	This Section does not apply.	The whole section is applied.

Principles for personal data processing Rights of the data subjects Rights and obligations of the competent authority and the processor Transfer of personal data to a third country or international organization			
SECTION 4: Specific situations of lawful processing of personal data (Articles 78 and 79)	The whole section is applied.	The whole section is applied.	The whole section is applied.
SECTION 5: The Office (Articles 80 to 106) Position, powers and organization of the Authority Code of conduct, certificate and accreditation Inspection Data protection proceedings Administrative offenses	The whole section is applied.	The whole section is applied.	The whole section is applied.
SECTION 6: Common, transitional and final provisions (Articles 107 to 112)	The whole section is applied.	The whole section is applied.	The whole section is applied.

As regards the differences of the national legislation contained in Act No. 18/2018 Coll. compared to the GDPR, these are highlighted in Section 4 of Act No. 18/2018 Coll., which regulates the processing operations that the GDPR explicitly imposes or allows individual Member States to regulate by a specific national regulation; this is a regulation of the Member State making use of the so-called enabling provisions of the Regulation. In particular, there is specific regulation on the processing of personal data defined in Article 78 of Act No 18/2018 Coll. having relevance to the following cases:

- **the processing of personal data for academic (especially pedagogical), artistic or literary purposes.**
The controller shall be entitled to process personal data for the above purposes, except where the processing of personal data for such purpose infringes on the data subject's right to protection of his or her personality or right to protection of privacy or where such processing of personal data without the data subject's consent is excluded by a special regulation or an international treaty to which the Slovak Republic is a party;
- **the processing of personal data when the processing is necessary for the purposes of informing the public by means of mass communications;**
- **processing of personal data in the context of employment;**
- **processing of a national identification number – birth registry number;**
- **specific rules on the processing of genetic data, biometric data and data relating to health;**
- **processing of personal data in an information system;**
- **processing of personal data for scientific purposes, historical research purposes or statistical purposes.**
When processing personal data for those purposes, the controller and the processor shall adopt appropriate safeguards to protect the rights of the data subjects. These safeguards shall include the implementation of appropriate and effective technical and organizational measures, in particular to ensure compliance with the principles of data minimization and pseudonymization. The

controller and processor shall take appropriate steps to comply with international standards and standards of security when adopting safeguards and when assessing their impacts on the protection of personal data.

Consequently, Article 78 of Act No. 18/2018 Coll. provides for a specific obligation for the controller and processor to maintain confidentiality of the personal data they process, which continues even after the processing of personal data has ceased. Concurrently, the legislation imposes an obligation on these entities to bind natural persons who come into contact with personal data at the controller's or processor's to maintain confidentiality of personal data, even after the termination of the employment, civil servant relationship, service relationship or other employment relationship of that natural person.

Labor law considerations

Another relevant aspect is the consideration of applicable **labor law provisions**, which also limit the **permissibility of monitoring employees and their activities**, in particular with regard to the control of their email and other communications carried out through their employer's infrastructure. The technologies listed below, which are used to monitor security threats in the organization, may also be considered as technologies monitoring UPJŠ employees – these will have to be evaluated in relation to individual technologies implemented. The condition for the use of monitoring technologies against employees is the initial notification of the employee and the appropriateness of the intervention in question. In accordance with the internal regulations of the UPJŠ, students and employees of the UPJŠ may use their email addresses only for work and study purposes. In this context, it will also be necessary to take into account the different status of an employee of UPJŠ, who is subject to the provisions of Act No 311/2001 Coll. Labor Code, and that of a student, who is not subject to the above mentioned Act.

Problematic areas identified

Among most problematic aspects of the activities realized by the CSIRT security teams within the UPJŠ organization are:

- the implementation and use of the so-called **SIEM (Security Information and Event Management) technology** that enables organizations to identify and react to potential security threats and vulnerabilities before they threaten the organization's operations on the basis of identification of anomalies in the behavior of organization infrastructure users', the implementation of which is one of the main objectives of the CSIRT team and the SOCCER project itself. The main objective of this technology is to collect data from different sources, especially from servers, networks, firewalls, IP addresses and data related thereto (place of assignment, time stamp) (collection of logs), and their following evaluation.
- **monitoring of user accounts in the Microsoft 365 service**, the administrator of which within the UPJŠ organization is the Centre for information and communication technologies (Centrum informačných a komunikačných technológií - ClaKT). The tasks of the security teams also include monitoring and controlling of user logins to their Microsoft 365 accounts (location of logins, device from which the user logged in, activities performed within the account, etc.). This monitoring enables the identification of possible **compromise of the user's identity** and to react accordingly (reactive action) by blocking the user's account manually or in an automated manner. This monitoring also includes the identification of metadata relating to email messages received and sent in Microsoft Outlook such as the date and time the message was sent or received,

the location where the message was sent or received, whether the message contained attachments, etc. **The content of the email message itself is not monitored.** Based on the above, the nature of the email message can be evaluated and classified (based on a scoring system) as e.g. spam (Outlook also offers automated spam message detection), a message containing malware or other malicious content, and their subsequent blocking in order to protect users from fraudulent activity. It is also essential to manually check the true nature of incoming email messages and then reclassify them if necessary. The relevant security team only gains access to the content of an email message if it is quarantined (if it receives a significantly negative score of harmfulness). In these instances, it is necessary to evaluate the legitimacy of the message on the basis of its content examination.

- the implementation of the so-called **DLP (Data Leak Protection) technology**, the purpose of which is the protection from data leakage from organization; the data in question is of different nature and may include personal data, including sensitive data. This technology enables the prevention of sending of a message containing such data and alerts the administrator (CSIRT team) of an attempt to send such a message. Obviously, alerting the administrator to the fact that an email message contains data that should not be disclosed externally from the organization requires disclosure of part of the content of the message in order to provide the relevant context, that is why implementation of such technology in practice is rather problematic. If such technology were to be implemented, the ideal situation would be a low number of notifications, of which a high number are relevant (as few false positives as possible in order to limit the security team's access to the content of the affected email messages).
- the implementation of the so-called **EDR (end point response) / XDR (extended) technology**, which is a technologically superior anti-virus program capable of flagging instances of malicious code identification and circumstances related to it (how the attacker operates, efforts to eliminate his activity, activity in the cloud).
- the implementation of a **two-factor authentication system**, which is one of the security measures envisaged by the applicable legislation. In this context, the aspect of compliance, i.e. achieving the implementation of the two-factor authentication system by all users operating in the organization concerned, may be problematic. Moreover, one has to bear in mind that the employer is obliged under the Labor Code to ensure the security of such a connection for an employee who remotely connects to the employer's network.

Another aspect that needs to be considered in this context is **how data is captured** (from users' devices, from the server in operation, etc.) for the purposes of **digital forensic and incident response (DFIR) forensic analysis**. In this context, **UPJŠ employees are obliged to provide assistance to the CSIRT team in the forensic analysis of their working devices**. However, given the fact that a lot of UPJŠ employees also use non-work devices, it will be necessary to analyze their obligations in the event when data needs to be captured from their private devices. In doing so, it will be necessary to identify the legal basis for the collection of data from such devices as well as the necessity to provide the consent of the employee concerned for such data capture from the device they used. The assessment in question is hampered in particular by **the absence of the applicable legal regulations** in this regard, which, on the one hand, imposes an obligation to provide evidence in the case of identified illegal activity, in particular the obligation to provide assistance to the competent law enforcement authorities (obligation to report identified criminal activity) or possibly to other competent authorities (e.g. the Office for Personal Data Protection of the Slovak Republic), but on the other hand, does not specify

the organization's competences to act in this regard. Given that the CSIRT-team will have to analyze large amounts of data (e.g. information on websites visited, applications used, etc.) in the course of forensic analysis, it will be necessary to identify **the scope of the CSIRT-team's competence in terms of the extent of their authority to access such content**. For example, security teams will need to identify the so-called **Indicators of Compromise (IOCs)**, which identify what IP addresses the attacker logged in from, digital fingerprints, IP addresses, domain names, what domain the attacker accessed, where they downloaded the necessary applications from, etc. The CSIRT-UPJŚ aims to **share the data thus obtained with other organizations within the framework of the established common platform (threat intelligence and sharing platform)** in order to cooperate with security teams operating in other organizations. The admissibility of the above (e.g. from the perspective of data protection legislation) and the conditions of such data sharing (which data can be shared, to what extent) require additional analysis.

Another relevant aspect to be considered is **the evaluation of the nature of electronic communications** between users of the UPJŚ organization within a computer or mobile network, which may fulfill the conditions of the so-called **telecommunication secret**. The relevant legal framework in this respect is provided in the Act No. 195/2000 Coll. on Telecommunications. In this context, it will be necessary to take into account the position of the UPJŚ itself, which is part of SANET - an undertaking under the Electronic Communications Act that provides services on a computer network and is therefore under an obligation to respect telecommunication secrecy. It will be necessary to assess the status of UPJŚ itself as an undertaking, since UPJŚ serves as an intermediary channel and connects other schools to the SANET system. According to the status quo, the UPJŚ should not be covered by the legislation in question because of the closed network of members of the system; the element of for-profit activity is also absent, which excludes the possibility of classifying the UPJŚ as an enterprise. However, the fact that SANET also includes commercial entities in its network is problematic. Another problematic issue is the admissibility of monitoring of organizations connected to this network in order to ensure the security of the data transmission infrastructure used and the applicability of the mere conduit liability exemption in this context. Internet connection providers (including SANET) are providers of a basic service, i.e. in practice there is a tendency for the National Security Authority to impose the obligation to resolve security incidents on the entities or organizations connected to SANET. There is also the question of the permissibility of monitoring the organizations' own facilities or the data of the connected organizations (primary or secondary schools) and the possible provision of SOC services as a service in this regard.

Transparency is another essential aspect of CSIRT team' activities. However, a closer analysis will be required to assess the possibility to refuse to provide information for security purposes in the event of a request for information under the Act No. 211/2000 Coll. on Free Access to Information as amended (Freedom of Information Act).

Cybersecurity and data protection in Poland

In Poland, the main legal act governing the issues related to SOC activity is the Act on the National Cybersecurity System. It is a legal act incorporating the NIS1 directive into the Polish legal system. Currently, the Ministry of Digital Affairs has published a draft amendment to the aforementioned act, which will transpose the provisions of the NIS2 directive into the Polish legal system. Article 14 (2) of the currently applicable Act on the National Cybersecurity System states that internal structures established by the operator of essential services (the equivalent of a essential entity) responsible for cybersecurity and entities providing cybersecurity services (i.e., entities of the SOC type) are required to:

- meet the organizational and technical conditions necessary to ensure cybersecurity for the operator of essential services;
- to have facilities for providing incident response services, secured against physical and environmental threats;
- apply security measures to ensure the confidentiality, integrity, availability, and authenticity of processed information, taking into account personnel security, operation, and system architecture.

The Polish legislator decided to regulate in detail the issues concerning entities providing cybersecurity services and the internal structures responsible for cybersecurity. In this regard, a special regulation was issued listing the organizational and technical conditions for entities providing cybersecurity services and the internal organizational structures of operator of essential services responsible for cybersecurity, dated December 4, 2019. This legal act regulates, inter alia, the organizational and technical conditions that must be met by entities providing cybersecurity services, the security of premises that must be applied by the specified entities, and the range of skills that the personnel must possess.

In connection with the implementation of the NIS2 directive, the Polish legislator has presented a draft amendment to the aforementioned Act on the National Cybersecurity System. In the draft law, Article 14 states that essential and important entities, in order to fulfill their obligations arising from the law, are required to establish internal structures responsible for cybersecurity or will be required to enter into an agreement with a managed cybersecurity service provider. This means that every essential and important entity will have to either enter into an agreement with a provider of cybersecurity services or establish appropriate units responsible for cybersecurity within its internal structure.

SOC, in order to effectively achieve its goals, can undertake a range of different actions, including monitoring the activities of the organization's employees. These activities typically focus on reviewing logs, analyzing network usage, and controlling access to systems. In this regard, the SOC must operate in full compliance with labor law regulations, particularly the Polish Labor and Employment Code, which specifies, inter alia, the rules for monitoring employees. Labor and Employment Code allows the use of monitoring of the employee's work email if it is necessary to ensure the organization of work that enables full utilization of working hours and proper use of the tools provided to the employee. Monitoring of email cannot violate the confidentiality of correspondence and other employee rights. In addition to monitoring corporate email, the labor code permits the use of other forms of monitoring, such as network traffic monitoring (Art. 22 (3) §1-4 Labor and Employment Code).

Before implementing the monitoring of employees' use of company computers, the employer ought to:

- inform employees about the introduction of monitoring no later than 2 weeks before its activation,
- provide new employees with written information about the purposes, scope, and method of monitoring before allowing them to start work,
- mark the monitored devices (computers) in a visible and legible manner, using appropriate signs or audible announcements.

Cybersecurity and data protection in Czechia

Personal data protection

On April 24, 2019, the Act No. 110/2019 Coll. (Law on Processing of Personal Data), came into effect in Czechia, adapting the Czech legal system to the General Data Protection Regulation (GDPR). The Act. No. 110/2019 Coll. redefines the mandate of the Agency for Personal Data Protection including the definitions of the administrative proceedings for offenses related to the processing of personal data, including the imposition of fines for such offenses. This Act also transposes Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

The cybersecurity act

The regulation of cybersecurity is currently governed by Act No. 181/2014 Coll., on Cybersecurity, and its obligations apply only to current designated entities. The work on the new cybersecurity law is now in progress. Under the new law, organizations will be required to meet specified obligations only once the new law comes into effect, most probably at the beginning of 2025. The new law is based on the existing Cybersecurity Act and also meets the minimum requirements set by the European security directive NIS2. The goal of the Act. is to adapt the Czech legal system to the NIS2 directive.

Other laws that impact the SOC Operations in Czechia

In this section we summarize selected paragraphs from other legal regulations applicable to the operations of SOC at university or those that are affecting the organization posing additional demands on the SOC.

The organization and SOC should refer to the **Act No. 127/2005 Coll. – Act on Electronic Communications and on Amendments to Certain Related Acts** (Electronic Communications Act). Specifically, the university should analyse whether this law applies to them or not as it is intended primarily for ISPs and telecommunication providers (e.g., cell phones). Yet bigger universities often provide many services that are regulated by the Electronic Communication Act.

During an investigation of criminal activity, the Police may contact the university to collect digital evidence or identify a user behind the university IP address or account. Such requests could come in many forms and the security team is obliged to provide assistance if the law is used appropriately:

a) Act No. 141/1961 Coll. – Criminal Procedure Act (Criminal Procedure Code)

§ 8 Cooperation between state authorities, individuals and legal entities
„State authorities, legal entities and individuals are obliged without undue delay and, unless a special regulation stipulates otherwise, to comply with the requests of law enforcement authorities in the performance of their tasks, even free of charge.“
 § 88a Interception and recording of telecommunications traffic
“If, for the purposes of criminal proceedings conducted for an intentional crime,, it is necessary to determine data on telecommunications traffic that are subject to telecommunications secrecy or to which the protection of personal and intermediary data applies, and if the intended purpose cannot be achieved otherwise or if its achievement would otherwise be significantly impeded, the presiding judge of the court shall order their release to the court in proceedings before the court, and in preparatory proceedings the judge shall order their release to the public prosecutor or police authority at the proposal of the public prosecutor.”

b) Act No. 273/2008 Coll. – Law on the Police of the Czech Republic**§ 18 Requesting assistance from persons and authorities**

“A police officer is entitled to request material and personal assistance from the authorities and persons referred to in Section 14, in particular the necessary documents and information, including personal data, to the extent necessary for the performance of a specific police task. These authorities and persons are obliged to provide the requested assistance;”

Another category of laws and regulations are those stipulating the mandatory blocking or restricting user access to specified domains or communication with specified organizations. The details of who issues the list of blocked domains/organizations may differ in specific regulations, though the obligation remains the same:

c) Act No. 186/2016 Coll. - Gambling Act**UNAUTHORIZED INTERNET GAMES****§ 84a Blocking unauthorized internet games**

“(1) An internet access service provider pursuant to the Act regulating electronic communications (hereinafter referred to as the “internet access service provider”) is obliged to block access to a website listed on the list of unauthorized internet games.”

d) Act No. 378/2007 Coll. – Act on Pharmaceuticals**INFORMATION, CONTROL ACTIVITIES, MEASURES AND SANCTIONS****§ 101c Blocking of illegal websites**

“The internet connection provider in the Czech Republic is obliged to block access to websites listed in the list of websites offering illegal medicinal products within 15 days of the date of publication of the website in the list of websites offering illegal medicinal products.”

§ 101d Websites offering illegal veterinary medicinal products

*“(1) The list of websites offering illegal veterinary medicinal products contains data pursuant to § 101a, mutatis mutandis.
(2) In matters of maintaining the list of websites offering illegal veterinary medicinal products, the Veterinary Institute shall proceed mutatis mutandis pursuant to § 101b.
(3) For the blocking of websites offering illegal veterinary medicinal products, § 101c shall apply mutatis mutandis.”*

e) Act No. 146/2002 Coll. - Act on the State Agricultural and Food Inspection Authority**§ 3d**

„A provider of Internet access services in the Czech Republic is obliged to block access to websites listed in the list of websites within 15 days of the date of publication of the website in the list of websites. “

f) Act No. 1/2023 Coll. - Act on restrictive measures against certain serious acts applied in international relations (Sanctions Act)**§ 13 Implementation of restrictive measures**

„The implementation of restrictive measures included in the national sanctions list shall be carried out in accordance with the law governing the implementation of international sanctions. “

g) Act No. 69/2006 Coll. - Act on the Implementation of International Sanctions

RESTRICTIONS OR PROHIBITIONS IMPOSED BY DOMESTIC LEGAL ACT

§ 6 Transport and communications

„ (2) In the field of communications, sanctions may consist of a restriction or prohibition

b) the provision of electronic communications services for the purpose of connecting with an entity subject to international sanctions or with a person subject to international sanctions, or in a territory subject to international sanctions. “

Cybersecurity and data protection in Lithuania

MAIN NATIONAL LEGAL ACTS

The State Data Protection Inspectorate participates in the development of policy in the field of personal data protection - preparing drafts of laws and other legal acts. In this regard, the State Data Protection Inspectorate has prepared proposals for draft laws related to the personal data protection reform. These include proposals for the amendment of the Law on the Legal Protection of Personal Data of the Republic of Lithuania No. I-1374 and the amendment of the Law on the Legal Protection of Personal Data Processed in the Context of Police and Judicial Cooperation in Criminal Matters No. XI-1336, which were submitted to the Ministry of Justice in the fourth quarter of 2016.

- On July 16, 2018, the new version of the Law on the Legal Protection of Personal Data (ADTA) came into force.
- On July 16, 2018, the new version of the Law on the Legal Protection of Personal Data Processed in the Context of Police and Judicial Cooperation in Criminal Matters (Law Enforcement ADTA) came into force.

Cybersecurity and data protection in Estonia

In Estonia, the legal framework consists of a combination of directly applicable EU laws and regulations, as well as national laws and regulations. Understanding only specific laws or regulations provides an incomplete picture of the overall legal system.

Information security and cybersecurity are addressed in several regulations, the most important ones are outlined below. To ensure simplicity and clarity, this summary focuses solely on Estonian laws, excluding EU laws and regulations. This overview provides a high-level snapshot as of December 2024 and should be interpreted with caution. For instance, several Estonian laws are currently being amended to align with the implementation of the NIS2 Directive.

Estonian Personal Data Protection Act - Isikuandmete kaitse seadus (IKS)

The Personal Data Protection Act is a law in Estonian legislation that regulates the protection of natural persons in the processing of personal data. The Personal Data Protection And Implementation Act came into force on 15.03.2019. The law regulates the processing of personal data, protecting the fundamental rights and freedoms of natural persons, particularly their right to privacy.

The law defines the conditions and procedures for processing personal data, as well as the framework for state supervision of data processing activities. Additionally, it outlines penalties for violations of personal data processing regulations.

The law also sets requirements for various aspects of personal data management, including data retention periods, logging of activities involving personal data, the

content and retention of logs, and the registration of processing operations, among other provisions.

Since the SOC center handles personal data, it is essential that at least an impact analysis should be conducted to define the scope and categories of personal data, establish data retention periods, and register personal data processing activities. If the SOC service is provided to third parties, the roles of the controller and the processor must be clearly defined, and the rights and responsibilities of all parties must be explicitly established. End users must be informed about how their data is handled and by whom. This includes providing clear information about the collection and analysis of personal data by the SOC center, the related activities, and the retention periods for the data.

The official act is available at:

<https://www.riigiteataja.ee/akt/104012019011?leiaKehtiv>

Estonian Cybersecurity Act - Küberturvalisuse seadus (KüTS)

It sets out the requirements for maintaining network and information systems critical to the functioning of society, including those in the public sector. The law also establishes the framework for liability, state supervision, prevention and resolution of cyber incidents.

The law outlines obligations to ensure cybersecurity, identify and mitigate risks, and report cyber incidents. It also covers cybersecurity certification, as well as state and administrative supervision.

The official act is available at:

<https://www.riigiteataja.ee/akt/106082022018?leiaKehtiv>

Cybersecurity requirements for network and information systems - Võrgu- ja infosüsteemide küberturvalisuse nõuded

The regulation authorizes the minister responsible for organizing nationwide cybersecurity to establish the Estonian Information Security Standard (E-ITS), In accordance with the Cybersecurity Act (KüTS), it sets:

1. General requirements for security measures.
2. Specific requirements for system security measures and the scope of their application.

The official regulation is available at:

<https://www.riigiteataja.ee/akt/113122022030?leiaKehtiv>

Estonian Information Security Standard - Eesti Infoturbestandard (E-ITS)

The Estonian Information Security Standard (E-ITS) is mandatory for many private and public sector organizations. It is based on the German BSI IT-Grundschutz reference security method and has been developed to align with the requirements of the ISO/IEC 27001 standard. E-ITS follows a risk management approach and helps organizations determine information system protection measures.

The implementation of E-ITS is mandatory for public sector organizations, providers of vital and essential services, and other entities specified in the Cybersecurity Act (KüTS).

The structure of E-ITS is similar to the ISO/IEC 27001 standard and follows a similar approach to auditing and compliance requirements.

The requirement to implement E-ITS does not apply if the organization has implemented security measures that comply with the ISO/IEC 27001 standard and has submitted a certificate of compliance to the administrative supervision authority.

The official regulation is available at:

<https://www.riigiteataja.ee/akt/121122022034?leiaKehtiv>

E-ITS: <https://eits.ria.ee/>

Requirements for network and information system security measures and the scope of their application when using cloud services - Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel

The purpose of the regulation is to establish uniform principles for public sector institutions when using cloud services. It also consolidates existing principles related to ensuring the security of network and information systems, managing business process risks, and protecting public information, all of which must be adhered to when utilizing cloud services in the public sector. The regulation harmonizes the approach to managing risks as a user of cloud services.

The regulation outlines the necessary actions in the following scenarios:

1. when an institution intends to move public information processing to the cloud,
2. when a decision has been made to transition to the cloud,
3. when changes occur within the cloud environment, and
4. when the use of the cloud is terminated, or the service provider is changed.

The official regulation is available at:

<https://www.riigiteataja.ee/akt/109012024025>

Regulation on the data exchange layer of information systems - Infosüsteemide andmevahetuskihi määrus

The regulation establishes requirements for the data exchange layer of information systems, including its use and management. It governs the operation of the X-Road data exchange layer, which has been in use in Estonia for approximately 20 years. X-Road is a technical and organizational environment that enables secure and verifiable internet-based data exchange between state institutions and also with the private sector.

The official regulation is available at:

<https://www.riigiteataja.ee/akt/127092016004?leiaKehtiv>

Information Society Services Act - Infoühiskonna teenuse seadus

The Act sets out the requirements for an information society service provider.

An information society service is a service provided in the course of economic or professional activity at the direct request of the service user, where data is processed, stored, and transmitted digitally through electronic means designed for such purpose. In these services, the parties involved are not simultaneously present in the same location.

The service must be entirely transmitted, received, and processed using electronic communication methods. Information society services do not include services transmitted via fax or telephone call, nor do they encompass television or radio services.

Among other things, it specifies the information that the service provider ought to make available to the service user.

The official act is available at:

<https://www.riigiteataja.ee/akt/106082022022?leiaKehtiv>

Electronic Communications Act - Elektroonilise side seadus

It establishes requirements for publicly available electronic communications networks and services, the use of electronic contact details for direct marketing, the maintenance of radio communications, the management of radio frequencies and numbering, and radio equipment. It also outlines state supervision to ensure compliance with these requirements and specifies liability for violations.

The official act is available at:

<https://www.riigiteataja.ee/akt/127022022003?leiaKehtiv>

Emergency Act - Hädaolukorra seadus

The purpose of the Emergency Act is to establish a legal framework for the structure and organization of the state's crisis management system. Under the Act, crisis management encompasses the prevention, preparation for, and resolution of emergencies.

The official act is available at:

<https://www.riigiteataja.ee/akt/117052020003?leiaKehtiv>

Penal Code - Karistusseadustik (KarS)

The law defines various offences and their corresponding punishments. These offences include, but are not limited to, interference with computer data, illegal removal or modification of terminal device identification means, obstruction of computer system functionality, computer fraud, preparation for a computer crime, illegal access to a computer system, and more.

The official act is available at:

<https://www.riigiteataja.ee/akt/104072024025?leiaKehtiv>

Public Information Act - Avaliku teabe seadus

Public information refers to information that is recorded and documented in any form or medium, which is obtained or created in the course of performing public duties as specified in the Act or related legislation. This includes, inter alia, access to public computer networks and state databases.

The official act is available at:

<https://www.riigiteataja.ee/akt/107032023011?leiaKehtiv>

Estonian cybersecurity strategy - Küberturvalisuse strateegia

The strategy document outlines goals for 2024–2030 across four main areas:

1. managing the development of national cybersecurity,
2. increasing the cyber resilience of society,
3. strengthening the cyber shield (including incident monitoring and prevention), and
4. shaping a secure cyber environment in Estonia and globally.

2024-2030 cybersecurity strategy:

https://www.mkm.ee/sites/default/files/documents/2024-07/Kyberturvalisuse%20strateegia%202024-2030_labivalt_IT_vaatlik_Eesti.pdf

Council of Europe Convention on Cybercrime - Euroopa Nõukogu Arvutikuritegevusvastane konventsioon

Cybercrime knows no borders, and criminals can often launch attacks from anywhere in the world, making the fight against this type of crime dependent on close international cooperation. In addition to domestic laws, many countries have entered into international agreements addressing cybersecurity. For instance, Estonia has signed the Council of Europe Convention on Cybercrime, commonly referred to as the Budapest Convention.

The official convention is available at <https://www.riigiteataja.ee/akt/550359>

3.3. Personnel/ Roles and requirements

Introduction

Every SOC team is made up of people. The responsibilities of SOC team members are diverse and associated with different areas of IT and cybersecurity. That is why SOC team need to people with a wide range of skills, and with distinct experience. In most of cases, SOC teams consist of people serving the following roles:

- SOC Manager/SOC Leader – person who will be the team leader. This person is responsible for managing the SOC team work.
- SOC level 1 engineer (ECSF: Security Operation Center Analyst) – person who will be responsible for responding to automatic alerts, sending information about possible threats.
- SOC level 2 engineer (ECSF: Cyber Incident Responder) – person who will be responsible for responding to alerts forwarded from the 1 level engineer. This person is also a part of the Incident Response Team.
- SOC level 3 engineer (ECSF: Cyber Incident Responder) – This person is responsible for analysis of events in a broader perspective, creating and improving automatic alerts. This person is also a part of the Incident Response Team.
- Threat Hunter (ECSF: Cyber Threat Intelligence Specialist) – This person is responsible for proactively searching for suspicious behavior in logs.
- System architect (ECSF: Cybersecurity Architect, Cybersecurity Implementer) – This person is responsible for creating and configuring SIEM systems. In many cases, this person is also a SOC level 3 engineer.

- DFIR engineer (ECSF: Digital Forensics Investigator) – This person is responsible for digital forensics tasks.

Requirements for Specific Roles

SOC Leader

Technical requirements:

- Minimum of 5 years of experience in cybersecurity.
- Technical and cyber literacy.
- Master's degree in information security, Computer Science, or a related field.
- Familiarity or experience in Intelligence Driven Defense, Cyber Kill Chain methodology, and/or MITRE ATT&CK framework.

Certificates:

- CISSP
- CISM
- GIAC

Soft Skills:

- Qualities to be shared by every leader, such as people management skills
- Orientation toward high-ops tempo, high-stress positions requiring “guts” to make tough decisions and negotiate difficult decisions with leaders at all levels of the food chain
- Ability to communicate effectively with all levels of staff, management, and business units both verbally and in writing.

SOC level 1 engineer

Technical requirements:

- Formal training in IT, computer science (CS), electrical or computer engineering, cybersecurity, or a related field
- Basic Knowledge of network protocol stack, including major protocols such as IPv4, IPv6, Transmission Control Protocol (TCP), User Datagram Protocol (UDP)
- Understanding of how web applications, email applications, and other common internet-facing applications work.
- Basic cybersecurity knowledge (e.g. typical attacks).

Soft skills:

- Ability to thrive in high ops tempo, high-stress environments
- Good communication skills
- Emotional intelligence and stress management
- 24/7

SOC level 2 engineer

Technical requirements:

- Formal training in IT, computer science (CS), electrical or computer engineering, cybersecurity, or a related field
- Knowledge of OS internals (such as Windows, macOS, Linux, Android, iOS).
- Working knowledge of Open Systems Interconnection (OSI) network protocol stack, including major protocols such as IPv4, IPv6, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), HTTP/2, HTTPS, Server Message Block (SMB)/Common Internet File System (CIFS), Secure Sockets Layer/Transport Layer Security (SSL)/(TLS), Remote Desktop Protocol (RDP).
- Understanding of how web applications, email applications, and other common internet-facing applications work.
- Knowledge of common networking services such as network address translation (NAT), DHCP, DNS, and network time protocol (NTP).
- Familiarity with Mobile architectures, protocols, and security.
- Ability to tear apart a suspect file and formulate a working understanding of its attack vector and likely purpose.
- Minimum of 1 year working experience in the area of:
 - IT help desk
 - Cybersecurity
 - Software and system development
 - System administration
- On-the-job experience in IT operations, cloud-based services and systems, system/network administration, or software development, incident response, malware analysis

Certificates:

- BTL1

Soft skills:

- Ability to thrive in high ops tempo, high-stress environments
- Good communication skills
- Emotional intelligence and stress management
- Good intuition and ability to think “outside the box”
- Critical and creative thinking
- Ability to respond to emergency calls during non-business hours, as needed.

SOC level 3 engineer

Technical requirements:

- SOC level 2 requirements
- Understanding of modern, distributed authentication and access control mechanisms and architectures like SSAML, OAUTH, and ADFS.
- Working knowledge of cryptography basics, protocols, and concepts such as Public Key Infrastructure (PKI), asymmetric key exchange, and symmetric cryptography.

- Hands-on understanding of using major cloud service providers such as Amazon AWS, Microsoft Azure, or Google Cloud as well as a good understanding of how to configure, secure, and monitor systems and data in these environments.
- Knowledge of common threat models such as the Diamond Model of intrusion analysis Cyber Kill Chain and MITRE ATT&CK; also, a good understanding of public and private data sources to support cyber threat analysis along with strong report writing skills.
- The ability to tear apart a suspect file and formulate a working understanding of its attack vector and likely purpose, and ability to break down executables using disassemblers, debuggers, and hex dump.
- Scripting ability (Powershell, Python, Bash)
- Ability to read, understand and create technical design documentation
- Linux OS administration
- Knowledge of virtualization systems (e.g. VMware, KVM)

Certificates:

- BTL2
- eCTHP
- SSCP
- Security+
- CCTHP

Soft skills:

- Ability to lead an Incident Response Team and respond to emergency calls during non-business hours, as needed.
- Communicate, present and report to relevant stakeholders

Threat Hunter

Technical requirements:

- SOC level 2 requirements
- Understanding of modern, distributed authentication and access control mechanisms and architectures like SSAML, OAUTH, and ADFS.
- Working knowledge of cryptography basics, protocols, and concepts such as Public Key Infrastructure (PKI), asymmetric key exchange, and symmetric cryptography.
- Hands-on understanding of using major cloud service providers such as Amazon AWS, Microsoft Azure, or Google Cloud as well as a good understanding of how to configure, secure, and monitor systems and data in these environments.
- Knowledge of common threat models such as the Diamond Model of intrusion analysis Cyber Kill Chain and MITRE ATT&CK; also, a good understanding of public and private data sources to support cyber threat analysis along with strong report writing skills.
- Scripting ability (Powershell, Python, Bash)

Certificates:

- BTL2
- eCTHP
- SSCP
- Security+
- CCTHP

Soft skills:

- Collaborate with other team members and colleagues
- Communicate, coordinate and cooperate with internal and external stakeholders
- Communicate, present and report to relevant stakeholders

System architect

Technical requirements:

- Formal training in IT, computer science (CS), electrical or computer engineering, or a related field
- Scripting ability (Powershell, Python, Bash)
- Ability to read, understand and create technical design documentation
- Linux OS administration
- Knowledge of virtualization systems (e.g. VMware, KVM)
- Working knowledge of Open Systems Interconnection (OSI) network protocol stack, including major protocols such as IPv4, IPv6, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP, HTTPS, Secure Sockets Layer/Transport Layer Security (SSL)/(TLS).

Certificates:

- Supplier certificates (VMware, AWS, Linux, SIEM vendors)

Soft skills:

- Ability to thrive in high ops tempo, high-stress environments
- Good communication skills
- Critical and creative thinking

DFIR engineer

Technical requirements:

- Formal training in IT, computer science (CS), electrical or computer engineering, cybersecurity, or a related field
- Knowledge of digital forensics (PC, mobile) and investigating response.
- Hands-on experience with popular incident response tools.
- Experienced in conducting malware analysis.
- Knowledge of SIEM systems and log analysis.
- Understanding of sophisticated threat actors and their TTPs, including MITRE framework.

Certificates:

- GCFE
- GNFA
- GCIH

Soft skills:

- Willingness to work off-shift hours, or work as needed, during incidents.
- Ability to maintain a high level of discretion and personal integrity in the exercise of duties, including the ability to professionally address confidential matters.
- Ability to thrive in high ops tempo, high-stress environments
- Good communication skills
- Emotional intelligence and stress management
- Good intuition and ability to think “outside the box”
- Critical and creative thinking

- Work ethically and independently; not influenced and biased by internal or external actors

Alternatives

An alternative approach to defining responsibilities for the SOC team is also possible. Nowadays, the concept of non-level/non-line SOC is gaining popularity. The idiosyncrasy of this approach is that each SOC analyst has the expertise and capabilities to take up any query and handle it from start to finish. This approach makes each analyst equal to the others (of course, further there may be differences in experience between them), it does not come to a situation where analysts on one line do not have any requests to deal with and therefore remains idle, while at the same time on another line analysts handle a number of requests. Implementing such a model requires spending much more time on employee training at the beginning. With such a model adopted, there are the following roles in the team:

SOC Leader

Skills and requirements are the same as in traditional SOC.

Security Operation Center Analyst

Technical requirements:

- Formal training in IT, computer science (CS), electrical or computer engineering, cybersecurity, or a related field
- Knowledge of OS internals (such as Windows, macOS, Linux, Android, iOS).
- Working knowledge of Open Systems Interconnection (OSI) network protocol stack, including major protocols such as IPv4, IPv6, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), HTTP/2, HTTPS, Server Message Block (SMB)/Common Internet File System (CIFS), Secure Sockets Layer/Transport Layer Security (SSL)/(TLS), Remote Desktop Protocol (RDP).
- Understanding of how web applications, email applications, and other common internet-facing applications work.
- Knowledge of common networking services such as network address translation (NAT), DHCP, DNS, and network time protocol (NTP).
- Familiarity with Mobile architectures, protocols, and security.
- Ability to tear apart a suspect file and formulate a working understanding of its attack vector and likely purpose.
- Minimum of 1 year experience in work as one of:
 - IT help desk
 - Cybersecurity
 - Software and system development
 - System administration
- On-the-job experience in IT operations, cloud-based services and systems, system/network administration, or software development, incident response, malware analysis
- Understanding of modern, distributed authentication and access control mechanisms and architectures like SSAML, OAUTH, and ADFS.

- Hands-on understanding of using major cloud service providers such as Amazon AWS, Microsoft Azure, or Google Cloud as well as a good understanding of how to configure, secure, and monitor systems and data in these environments.
- Knowledge of common threat models such as the Diamond Model of intrusion analysis Cyber Kill Chain and MITRE ATT&CK; also, a good understanding of public and private data sources to support cyber threat analysis along with strong report writing skills.
- The ability to tear apart a suspect file and formulate a working understanding of its attack vector and likely purpose, and ability to break down executables using disassemblers, debuggers, and hex dump.
- Scripting ability (Powershell, Python, Bash)
- Ability to read, understand and create technical design documentation
- Understanding of modern, distributed authentication and access control mechanisms and architectures like SSAML, OAUTH, and ADFS.
- Working knowledge of cryptography basics, protocols, and concepts such as Public Key Infrastructure (PKI), asymmetric key exchange, and symmetric cryptography.
- Knowledge of digital forensics (PC, mobile) and investigating response.
- Hands-on experience with popular incident response tools.
- Experienced in conducting malware analysis.
- Knowledge of SIEM systems and log analysis.
- Understanding of sophisticated threat actors and their TTPs, including MITRE framework.

Certificates:

- BTL2
- eCTHP
- SSCP
- Security+
- CCTHP
- GCFE
- GNFA
- GCIH

Soft skills:

- Ability to thrive in high ops tempo, high-stress environments
- Good communication skills
- Emotional intelligence and stress management
- Good intuition and ability to think “outside the box”
- Critical and creative thinking
- Ability to respond to emergency calls during non-business hours, as needed.
- Collaborate with other team members and colleagues
- Communicate, coordinate and cooperate with internal and external stakeholders
- Communicate, present and report to relevant stakeholders

System architect

Skills and requirements are the same as in traditional SOC.

3.4. Cyber Threat Intelligence and data sharing – compliance, legal and organizational issues

Cyber Threat Intelligence (CTI) and data sharing play a fundamental role in enhancing the cybersecurity posture of different organizations, including universities. The academic community always promoted sharing of CTI and cybersecurity data in general. Therefore, the university Security Operations Centers (SOC) should be integral to this process. Indeed, at some universities (usually those which boast a large IT faculty) the SOC team will partially overlap with the research team or these two will closely cooperate. Unfortunately, the effectiveness of CTI and data sharing is often impeded by a variety of organizational and legal issues, such as privacy concerns, data protection regulations, and issues related to trust and collaboration among the entities involved.

Sharing information about cyber threats is not merely reporting incidents; it's a proactive measure that aims to prevent potential breaches and improve a collective cybersecurity environment. When university SOC's participate actively in CTI and data sharing, they serve a dual purpose, they receive valuable threat intelligence from other entities and contribute to the collective knowledge of existing and emerging cyber threats and actors. This shared responsibility, however, is distinct from compliance with regulatory reporting requirements such as those defined in NIS 2 Directive [3]. The Directive mandates reporting of any significant incidents to the appropriate relevant national authorities. We do not consider such a reporting to be part of sharing, as sharing involves a voluntary action.

Specifically, the CTI sharing and the data sharing refers to the distribution of different types of information for varied use cases. CTI sharing fundamentally involves the distribution of information about potential or active cybersecurity threats. This includes vulnerabilities, indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs) used by threat agents, contextual data about attacks, and more. The objective of the CTI sharing is to help organizations proactively identify and guard against cyber threats, often facilitating collaborative defense efforts. On the other hand, the data sharing is a broader concept. This involves sharing diverse sets of data that can help, for example, to visualize current cybersecurity status (e.g. a map of network attacks) or to train ML models. These data are not directly actionable within the SOC but may support SOC operation on the background, e.g. by training classifiers to automate cybersecurity tasks (processing, detection, decisions) more accurately.

Both CTI and data sharing share common challenges related to privacy and data quality, but certain issues are of particular importance in each case.

Privacy

CTI sharing involves exchanging detailed information about threats, vulnerabilities, and entities involved in the attack, making privacy a high concern, especially in the context of GDPR [4] and other data protection regulations implemented at the national levels, including directives issued by relevant agencies such as Agency for the protection of private data. It may be difficult to ascertain whether certain information falls under the category of personal data, as online identifiers such as IP addresses or email addresses are regarded as personal data (Personally Identifiable Information under GDPR) in certain cases, though not in others. Availability of further data to the subject already in possession of such information will have to be considered before the decision on the

nature of data in question. At the same time, removing a piece of PII renders the shared information useless. For example, let us consider sharing information about a spammer without revealing its IP address- in such case there would be no spam block lists.

GDPR emphasizes data minimization, i.e. data collected should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. In CTI sharing, it is tricky to balance the need to share enough data to provide useful intelligence. Moreover, CTI sharing also needs to follow the principle of purpose limitation, another crucial aspect of GDPR. This rule states that data collected for specific purposes should not be further processed in a manner incompatible with those purposes, e.g. CTI must not be used for marketing.

In the case of alert sharing system the possible legal issues having relevance to GDPR were analyzed in [<https://doi.org/10.1145/3098954.3105822>] and the university SOC should refer to this publication to derive and assess its legitimate reasons to share its CTI data. The proportionality test criterion is suggested as the most effective solution when sharing CTI. In particular the it is stated that :

"If we want to justify processing and sharing of personal data in alert sharing platforms by "legitimate interest" of peers, we need to take following steps: (1) determine, if this interest is legitimate, (2) determine whether the processing is necessary to achieve the interest pursued, (3) establish a provisional balance by assessing whether the data controller's interest is overridden by the fundamental rights or interests of the data subjects, (4) establish a final balance by taking into account additional safeguards, (5) demonstrate compliance and ensure transparency.

In both the opinion of the Article 29 with reference to working party and the GDPR it is mentioned that cyber security is one of the fields in which it is likely that the personal data will be processed due to legitimate interest of the controller. Recital 49 of the GDPR specifically states that "the processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, [...] constitutes a legitimate interest of the data controller concerned" [3]. So it is probably safe to say that so called CIA triad (confidentiality, integrity, authorization) of data and information systems is a legitimate interest within the meaning of the GDPR."

GDPR as a regulation does not have to be transposed to the national legislation but the national legislation may extend or detail the GDPR in specified instances. Therefore, the relevant national regulations should also be considered when sharing CTI or data. The table below depicts the national legislation framework with respect to GDPR in the countries participating in the SOCCER project, a subjective comparison to GDPR is given in the last column.

Table 3 - Depicts the national legislation framework with respect to GDPR in the countries participating in the SOCCER project.

Country	National law	Comparison to GDPR
Czechia	Act No. 110/2019 Coll. Act on the Processing of Personal Data [https://uouu.gov.cz/media/act-no-110-2019-coll.pdf]	This law focuses on operational aspect of data protection such as in establishing the Agency for Data Protection and details specific procedures.
<u>Estonia</u>	Personal Data Protection Act [https://www.riigiteataja.ee/en/eli/507112023002/consolide]	This law came to effect in 2019, and it specifies how the GDPR regulation applies in Estonian legal space. It clarifies when personal data can be processed without the consent of the subject

		(e.g., for journalistic, academic, artistic, research archiving purposes), how and when law enforcement is allowed to process personal data, how long the data can be stored, clarifies rights of data subjects to request their data or its deletion. It also covers the obligations of personal data processors and database maintainers, and required standards of data transmission, logging and record keeping. In addition, it defines when Estonian Data protection Inspectorate must be consulted and defines the Data Protection Specialist position, tasks and roles. The law outlines the security measures for processing personal data, when local data can be transferred to third countries and how its provisions are supervised by the state.
Slovakia	Act No. 18/2018 Coll. on the Protection of Personal Data and on the Amendment and Supplementing of Certain Acts.	§ 78 (1) The controller may process personal data without the consent of the data subject if the processing of personal data is necessary for academic, artistic, or literary purposes; this does not apply if the processing of personal data for such a purpose violates the data subject's right to the protection of their personality or right to privacy, or if such processing of personal data without the data subject's consent is excluded by a specific regulation or an international treaty binding the Slovak Republic. § 78 (7) When processing personal data for archiving purposes, scientific purposes, historical research purposes, or statistical purposes, the controller and the processor are obliged to adopt appropriate safeguards for the rights of the data subject. These safeguards include the implementation of appropriate and effective technical and organizational measures, particularly to ensure compliance with the principle of data minimization and pseudonymization. § 78 (10) The controller and the processor, when adopting security measures and assessing the impact on personal data protection, shall proceed in accordance with international security norms and standards. § 79 (1) The controller and the processor are obliged to maintain confidentiality of the personal data they process. The duty of confidentiality persists even after the termination of the processing of personal data. § 79 (2) The controller and the processor are obliged to bind the individuals who come into contact with personal data at the controller or the processor to maintain confidentiality. The obligation to maintain confidentiality according to the first section persists after the termination of the employment relationship, civil service

		relationship, service relationship, or similar employment relationship of such individuals.
Poland	The Act of 10 May 2018 on the Protection of Personal Data [https://uodo.gov.pl/en/660/1464]	The Act on the Protection of Personal Data in Poland, effective since 2018, aligns national data protection requirements with the GDPR. This law sets conditions for processing personal data without explicit consent, such as for research or security purposes, and includes provisions for handling data within cyber threat intelligence (CTI) contexts. It outlines controllers' and processors' duties, emphasizing measures for data accuracy, secure transmission, and record-keeping. The Act also mandates the designation of Data Protection Officers (ODO) for entities processing sensitive information, defines their responsibilities, and imposes an obligation to consult the Personal Data Protection Office (UODO) in cases of high-risk processing. Additionally, it regulates cross-border data transfers, setting supervisory measures to ensure GDPR-compliant processing standards. From the controller's perspective, of particular importance for practical applications are the following aspects: - The procedure to designate a data protection officer and notify the President of the Personal Data Protection Office about it – chapter 2 - Procedure in case of infringement of the personal data protection provisions – chapter 7 - Inspection of compliance with personal data protection regulations conducted by the President of the Personal Data Protection Office The Act on the Protection of Personal Data in Poland does not regulate issues such as basic definitions (e.g., the definition of "personal data," "processing," etc.), data processing principles, legal bases, mandatory elements of the information obligation, or the rights of data subjects. These issues are described solely in the GDPR
Lithuania	Law No. XIV-2626 amending the Law on the Legal Protection of Personal Data of the Republic of Lithuania No. I-1374 https://www.e-tar.lt/portal/lt/legalAct/66824d50177611efbcbfb318996800a8	The national legal framework in Lithuania fully complies with the GDPR, ensuring adherence to all its core principles and requirements. However, it introduces additional clarifications and detailed provisions in the following areas: Additional Competencies for National Supervisory Authorities. The State Data Protection Inspectorate (SDPI) and the Inspector of Journalist Ethics have specific roles and responsibilities, including public disclosure of decisions, the right to request information, and

		conduct inspections, as outlined in the Lithuanian law. These competencies complement the GDPR framework without altering its fundamental provisions. 2. Processing of Employee and Candidate Data. The law establishes specific conditions for processing data on convictions and criminal offenses of employees and candidates, such as requiring employers to perform a written assessment and consult with a Data Protection Officer. While this is beyond the scope of GDPR's general principles, it ensures flexibility in terms of national measures. 3. Collaboration and Information Sharing. Lithuanian supervisory authorities are empowered to exchange information, including confidential data, during investigations to enforce GDPR and other related laws. This ensures efficient implementation of GDPR's cooperation requirements. 4. Administrative Procedures and Deadlines. The Lithuanian law specifies strict deadlines for handling complaints and imposing administrative fines. These procedural details enhance clarity while remaining consistent with the GDPR's overarching framework. 5. Public Disclosure of Decisions. Supervisory authorities are required to publish their decisions on investigations and complaints, increasing transparency. This complements the GDPR but is not explicitly mandated by it. 6. Sanctions for Violations of Other EU Laws. The law extends the scope of sanctions to violations of other EU legal acts involving data processing, ensuring a comprehensive approach to data protection. 7. Specific Document Delivery Procedures. Detailed provisions for notifying individuals about decisions or requirements by supervisory authorities are included in the Lithuanian law. These provisions ensure procedural clarity while aligning with GDPR standards. These additions provide clarity and operational efficiency in implementing GDPR provisions in
--	--	---

	Lithuania without deviating from the regulation's core principles. <i>On May 14, 2024, the Seimas of the Republic of Lithuania adopted the Law No. XIV-2626 amending the Law on the Legal Protection of Personal Data of the Republic of Lithuania No. I-1374, which introduces certain innovations in Lithuania starting from July 1, 2024. The intended changes aim to:</i> <i>Supplement the Law on the Legal Protection of Personal Data (LLPPD) with provisions to ensure the promptness and efficiency of complaint reviews and investigations or inspections, thereby enabling the protection of the rights and interests of a broader range of data subjects;</i> <i>Grant employers the permission (but not the obligation) to process the criminal record data of employees and job applicants based on the employer's legitimate interests, while establishing corresponding obligations for employers and safeguards for the rights and freedoms of data subjects;</i> <i>Oblige personal data protection supervisory authorities—the State Data Protection Inspectorate (SDPI) and the Inspector of Journalist Ethics—to publish their decisions.</i> <i>Below, the key changes are reviewed:</i> <i>Information for Employers – Processing of Criminal Record Data</i> <i>As of July 1, 2024, under the amended LLPPD, employers will be permitted to lawfully process the criminal record data of candidates applying for positions or performing work functions, as well as employees (hereafter collectively referred to as “employees”), if:</i> <i>The processing of such data is necessary to achieve the legitimate interests of the employer, except where the interests of employees should override those of the employer; and</i> <i>The processing is necessary to fulfill a legal obligation to verify whether an individual meets the requirements established by law or implementing acts.</i> <i>The SDPI emphasizes that while the law broadens the possibilities for processing criminal record data, such processing will only be lawful if employers comply with the requirements of the General Data Protection Regulation (GDPR) and the safeguards for the rights and freedoms of data subjects established in the amended LLPPD:</i> <i>An assessment of the legitimate interest in processing criminal record data will need to be conducted, and a report of this assessment must be prepared in writing (consultation with a data</i>
--	--

		protection officer is mandatory, if there is one appointed); Employers must confirm and publish on their website, if available, a list of positions or work functions requiring the absence of a criminal record for certain offenses, specifying the offenses for which individuals must not have a criminal record; Only the criminal record data of employees performing functions listed in the above-mentioned list will be processed; Employees themselves will provide specific information on criminal convictions and offenses.. To ensure proper implementation of the amended LLPPD provisions, the SDPI plans to prepare methodological guidance on processing criminal record data. <i>Information for Data Subjects – Submitting Complaints to the SDPI</i> Starting July 1, 2024, amendments to the LLPPD introduce changes regarding complaints submitted to the SDPI related to the legality of video surveillance and the exercise of data subjects' rights. The LLPPD amendment establishes the following procedure for complaints regarding the legality of video surveillance submitted to the SDPI: Before submitting a complaint to the SDPI regarding the legality of video surveillance, a person (data subject) must first contact the individual conducting the video surveillance (if known) to obtain information about the surveillance. If the individual conducting the video surveillance fails to provide information within one month, or the provided information proves unsatisfactory, or it is impossible to contact the individual, the person has the right to submit a complaint to the SDPI. The complaint must include information about the attempt to contact the individual conducting the video surveillance and, if available, a copy of their response, or reasons why it was impossible to contact them. For complaints concerning rights established under Articles 15–22 of the GDPR (e.g., the right to access data), the complainant must provide information about attempts to contact the data controller or processor, including a copy of their response, if available. If this information is not provided in the complaint, the SDPI will have the right to refuse to investigate it.
--	--	---

		<i>Other Changes Related to Violation Investigations</i> <i>The amended LLPPD also introduces other changes to the procedure for handling violations, effective July 1, 2024:</i> <i>The group of entities eligible to submit complaints to the SDPI is expanded to include non-profit institutions, organizations, or associations operating in the field of personal data protection, which may submit complaints independently of data subjects' authorizations.</i> <i>A "reasonable scope" concept for complaint handling is introduced, allowing the SDPI to choose the most appropriate and effective methods and measures for complaint handling based on specific circumstances and criteria set by the LLPPD, such as current operational priorities, systemic violations, or the need to provide an opinion on significant GDPR application issues.</i> <i>Suspension of deadlines for handling violations, e.g., when expert opinions or conclusions from other supervisory authorities are required.</i> <i>Consolidation of complaints, when two or more complaints are submitted by the same complainant regarding the same respondent or by different complainants about the same violations by the same respondent.</i> <i>The possibility of amicable resolution of complaints.</i> <i>Exemption from deadlines for handling international complaints.</i> <i>Extension of the statute of limitations for imposing administrative fines from two to three years.</i> <i>Publication of Supervisory Authorities' Decisions</i> <i>From January 1, 2025, the SDPI and the Inspector of Journalist Ethics will publicly disclose their decisions adopted during the handling of violations (except decisions to refuse or discontinue complaint investigations) on their websites within five business days from the decision date. The publication will comply with legal requirements for protecting information and will ensure anonymization, refraining from revealing trade secrets, professional secrets, or information related to security measures. In cases where the SDPI identifies no violations of the GDPR or other legal acts, the publication will not disclose the identities of data controllers or processors involved. Decisions will be available online for 10 years from the publication date.</i> Obligations for Data Controllers and Processors 1. Compliance with GDPR and National Requirements. Data controllers and processors must
--	--	--

		ensure that all data processing complies with the GDPR and the additional national requirements imposed by the Lithuanian law (Article 1). 2. Documentation and Assessments. Controllers must perform written assessments when processing employee or candidate data related to criminal convictions (Article 5). This assessment must consider the relevance of the criminal data to the job role, risks involved, and the proportionality of processing such data. 3. Transparency. Controllers must maintain a publicly accessible list of job roles requiring criminal record checks and publish it on their websites, if applicable (Article 5). 4. Engagement with Data Protection Officers (DPOs). Data controllers and processors are required to consult with their DPOs when performing certain high-risk processing activities, such as the use of sensitive data for employment purposes (Article 5). 5. Cooperation with Supervisory Authorities. Controllers and processors must provide all necessary information, documents, and access to facilitate supervisory authority investigations (Article 12). They are required to cooperate fully with inspections and inquiries initiated by supervisory bodies. 6. Retention of Personal Data. Personal data should only be retained as long as necessary for the specific purpose for which it was collected, ensuring compliance with both GDPR and Lithuanian law's guidelines (General Obligation). 7. Handling of Complaints. Controllers and processors must provide sufficient documentation and responses to supervisory authorities if complaints regarding GDPR violations are lodged (Articles 23-24). 8. Public Information. Controllers are responsible for ensuring that public information about the processing of personal data, including
--	--	---

		rights and obligations, is clear, accessible, and compliant with national guidelines (Article 141). 9. Security Measures. Controllers and processors must implement adequate technical and organizational measures to ensure the security of personal data and prevent breaches (Article 12 aligns with GDPR Article 32). 10. Sanctions for Non-Compliance. Controllers and processors are subject to administrative fines and other measures for violations of GDPR or related national provisions (Articles 32 and 321).
--	--	---

While CTI sharing carries an additional level of contextual urgency and responsibility due to the potential consequences if threat information is not shared, the data sharing use-case is often offline and the legitimate reason to share identifiers, which are considered PII, is less explicit, if any. Therefore, we recommend anonymizing all information in the shared data that could lead to revealing personal private data.

Confidentiality

There are two issues regarding confidentiality – the confidentiality of the source organization that should prevent leaking its sensitive information and confidentiality of recipients who ought to treat the received intelligence adequately. From the source organization's perspective, sharing threat intelligence involves the exchange of potentially sensitive information that could reveal crucial details about their security framework. This includes information about the infrastructure, its vulnerabilities, breach points and its internal processes. If this sensitive information is not kept confidential, it can help an adversary launch an attack on the organization.

Proper data sanitization methods should be incorporated to remove any sensitive information that the source organization wishes to keep confidential, for example, removing or replacing sensitive information is one of the options, breaking the trace back to the source organization is another one. Designing proper sanitization methods is a complex issue and the SOCCER project plans to elaborate the requirements for data sanitization in its future deliverables. Besides sanitization, additional measures should be considered to keep sensitive information about the organization confidential, such as access restriction, use of encryption in transit and encryption at rest as well as audits to oversee the operation. Standardizing the information shared in a way that it only communicates about the threat concerned and not about the internal infrastructure nor processes, can help to prevent information leaking. The question of trust in the recipient's confidentiality also presents a major challenge in relation to the sharing of CTI. Once the information has left the source organization and has been received by another, it is rather difficult to maintain control over its further dissemination.. It is necessary to ensure that recipients understand the confidential nature of the information and potential harm that could result from improper handling or unauthorized sharing. This requires a set of protocols, legal arrangements like Non-Disclosure Agreements (NDAs), and, possibly, technical restrictions to prevent further propagation of the shared data.

Traffic Light Protocol is a set of rules, grouped into 4 categories, used to better define the audience or recipients of sensitive information. For convenience, the categories are described by four colors (red, orange, green, and white). The classification into the appropriate category is the responsibility of the organization from which the information originates. The Traffic Light Protocol (TLP) is used to classify the shared information, basing on the fact that information sharing happens from the source towards the recipient. It was developed by the National Infrastructure Security Co-ordination Centre (NISCC). Four colors are used to represent the allowed levels of disclose for sensitive information [5].

Table 4 – Description of Traffic Light Protocol

TLP:RED	For the eyes and ears of individual recipients only, no further disclosure.
TLP:AMBER+STRICT	Limited disclosure, recipients can only spread this on a need-to-know basis within their organization.
TLP:AMBER	Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients.
TLP:GREEN	Limited disclosure, recipients can spread this within their community.
TLP:CLEAR	Recipients can spread this to the world, there is no limit on disclosure.

As an evolution of TLP the Information Exchange Policy (IEP) was introduced by Forum of Incident Response and Security Teams (FIRST). The goal of IEP is to support machine processing of the shared information as well as more precise understanding how to treat data during the whole sharing process. To this end, IEP includes existing sharing policies such as TLP and defines extensions to support future use cases.

The core of IEP is a policy framework which consists of five policy types: handling, sharing, action, licensing and metadata. The policies describe via policy statements how to treat the data in the respective situations. The policy statements are defined per each policy, e.g. the policy statement encrypt-at-rest is relevant for the storage of the shared information.

Trust

The source organization trusts the recipients to handle the received information responsibly and ethically, for example, that the recipient employs adequate data privacy measures, adhere to data protection laws, commits to use the data for agreed-upon purposes only (i.e. keeping the license agreement), prevents data leaks and keeps communication agreements if required by the source organization (e.g. citation of the dataset in publications or maintaining confidentiality as signaled or agreed upon).

Mutually, the recipient organization trusts in data received, i.e. how useful, credible, and effective data is in meeting its cybersecurity goals as its insights and decisions are made upon received data. If attackers manage to compromise a source of CTI, or data in general, they could manipulate the data to hide their activities, to waste organization's

resources or to cause a distrust in the results of the automated analysis using poisoned data.

Data quality

CTI quality can be measured in multiple dimensions. A study presented in [6] offers a prioritized list of quality metrics: accuracy, actionability, interoperability, provenance, relevance, reliability, and timeliness.

The same study also offers the explanation of each dimension captured in the following table (adapted from [6]).

Table 5 – Prioritized list of quality metrics

Accuracy	The degree to which threat data or intelligence is correct, objective, or without false positives.
Actionability	The degree to which threat data or intelligence allows a decision to be made or action to be taken without the need for further analyses.
Interoperability	The degree to which the formats of threat data or intelligence is compatible with consumers' internal systems allowing it to be accessed and integrated seamlessly.
Provenance	The degree to which a threat intelligence consumer is able to track the evolution of a piece of threat data or intelligence including its origins and the process through which it was produced.
Relevance	The degree to which threat data or intelligence meets the consumer's specific requirements and is useful for the purpose for which it was produced.
Reliability	The degree to which the source of threat data or intelligence is trustworthy, authentic, and competent.
Timeliness	The degree to which threat data or intelligence is available without delay in a specific context of use.

The organizations involved in sharing frequently ask questions related to these metrics:

- What is the level of false positives that is ok?
- Given the large volume and complexity of data, can I identify what data is relevant for others? Can I identify what data is relevant for me?
- Can I share data fast enough, so is it still valid? Do I receive data that is not already obsolete?

CTI and data quality metrics differ depending on the actual purpose. CTI is being shared to improve situational awareness while the datasets are shared to enable the research and development of analytical tools as well as their comparison. Therefore, the relevant metrics for sharing datasets are completeness, timeliness, consistency, and in case of data being used for ML the comprehensiveness, correctness and variety ought to be considered as well, as proposed in [7].

Table 6 – Metrics for sharing datasets

Completeness	The degree to which all required data is available in a dataset.
Timeliness	The degree data are up-to-date with reality.
Consistency	The degree the data are uniform and comparable even across datasets.
Comprehensiveness	The degree a dataset contains all representative samples from the population.
Correctness	The degree the records in a dataset are accurate and valid, and they are correctly labelled if these are labelled records.
Variety	The degree of the coverage of a dataset of all different cases on selected features.

Sharing agreements

The formal or informal sharing arrangements are commonly introduced to address the issues discussed in previous sections. In general, any type of arrangement should cover the nature of data being shared, the purpose of sharing, data protection methods, and obligations of the receiving party. On the other hand, sharing arrangements can differ significantly to account for the specificity of data being shared, the number of parties involved, and the method of data distribution.

When data is provided via download, typically to a large number of unknown potential researchers in the academic environment, it becomes impractical to have individual sharing agreements with each recipient. In such cases, a license can effectively define the terms of data usage. Nevertheless, the data must be free of confidential or private information since malicious actors will not respect the license. A similar style of sharing agreement is often employed in voluntary CTI sharing communities where even confidential data is being shared yet access is restricted to the defined set of trusted users with legitimate interest (e.g. Warden is a community of academic organizations CZ sharing cybersecurity events, see [warden.cesnet.cz](https://www.misp-project.org/communities) or MISP communities <https://www.misp-project.org/communities>).

On the other hand, when sharing sensitive data between small number of parties, NDAs (Non-Disclosure Agreement) are often the preferred approach. NDA binds the signing parties not to disclose any sensitive information they may obtain. Additionally, the agreement can include measures regarding access control, encryption, data usage, data removal, audit and penalties to balance the negative impacts on the source organization if data is misused. These NDAs often have a standardized form (used in many contracts by academic institutions) and can be used as a template to be customized to address the specific context of the sharing agreement.

3.5. Supporting requirements

Introduction

The document describes the environmental, organizational and technical conditions supporting the operation of the SOC. With regard to the environmental conditions, the

important requirements for the SOC premises are indicated. Issues of proper space organization, including the workspace, are also pointed out.

Solutions to ensure the proper physical security of the premises, technologies supporting the maintenance of work continuity and technologies supporting the maintenance of data security were indicated.

An important element affecting the proper functioning of the SOC is the preparation of communication channels, the internal one involving SOC employees and the external one - with SOC customers. In this regard, technical tools for effective communication are also indicated.

Accurate documentation of SOC activities is also a crucial matter. The role of the supporting systems (ticketing system, knowledge base, SOAR) is presented.

The effectiveness of SOC employees' work also depends to some extent on the technical equipment of the SOC and the work tools available to employees. Hence, the tools and workstation equipment for SOC employees are also discussed.

One of the aspects necessary to analyse at the planning stage of the SOC operations is the shift work organization. What the need to respond to cyber threats generally means for the SOC is working in a 24/7 mode. This implies the need for shift work organization. Thus, the processes of handing over shifts, keeping a shift log, scheduling replacements, and responding in case of absences are discussed.

Location requirements

Physical space considerations.

The physical location of the SOC should be selected to prevent any risk of information leakage. A leak might happen if content on monitors and video walls is visible through windows or if conversations in the SOC can be heard from outside. The SOC's rooms should not be located on the ground floor or close to a nearby building's window. If such a situation is inevitable, the windows should be equipped with curtains or blinds. The walls, doors, and windows should be soundproof enough to prevent any sounds from the SOC from being heard.

Various arrangements of the SOC space are possible. However, it seems that the frequent need for intensive information exchange between SOC employees favours open space arrangements. Such an arrangement also facilitates the organization of proper visualization of data relevant to the monitoring systems in the form of, for example, videowalls.

When designing the layout of the space of the SOC, which often provides services to external customers, it is important to keep in mind the desirability of separating a part to which such customers can be invited and can look at the work of the SOC without compromising the security of the SOC's operation.

For SOC's that function on a 24/7 shift basis, it is essential to reconsider the scheduling of the cleaning services and other health-related factors within the facility.

Conference room

Having dedicated conference rooms is essential for a Security Operations Center (SOC), particularly when it operates in an open space layout. These rooms offer a private setting

for discussions, meetings, and brainstorming sessions. Additionally, they serve as suitable venues for conducting job interviews with prospective SOC employees.

The room should be functional, aesthetic and practical. The size of the room should be adapted to the individual needs and technical capabilities.

Important equipment includes a conference table and chairs that provide comfort during extended meetings. Additionally, a key component for the conference room is a projector with a screen or a large format display for content presentation, along with a computer or laptop. Equally important is communication equipment, such as a conference phone and a videoconferencing system.

Common room

Employees need to take regular breaks between work, especially if it is the type of work that requires their full attention. A short time out and chatting with colleagues in the common room will always leave employees feeling refreshed and less stressed.

A perfect common room should be distinct from the primary workspace, creating a calming atmosphere with amenities like a coffee maker, refrigerator, and microwave. Additionally, it should feature comfortable seating to allow employees to unwind when necessary.

Locker room / Cloakroom / Place for personal storages

For the 24/7 model, it is important to provide a place where employees can change clothes and leave their personal belongings.

Shift work brings extra factors to consider, such as shared workstations among different employees. To lessen the discomfort of sharing items like keyboards or a mice, it is beneficial for each worker to have their own set of this equipment. Consequently, there would be a need for storage space where employees can keep these items, which could be provided in the form of lockable lockers in the locker room.

Desk layout, chairs

Ergonomics guidelines should always be considered when selecting desks for the SOC staff. Given that employees spend long hours at their workstations, ensuring their health is a critical responsibility for facility managers.

For shared workspaces, height adjustable desks are the most practical solutions.

Examples of desks layouts in the room:

- rows – great for teamwork within the same row, since everyone looks in one direction, but challenging for communicating with those in different rows
- facing each other – easy to talk to people but hard to collaborate and see someone's screen nearby
- facing away from each other – the easiest to collaborate, but not everyone faces the video wall

Lighting

The SOC personnel require natural light and a view to maintain their health.

Lighting of the workplace is one of the key elements affecting the comfort and the safety of the employee. It is strictly regulated by the safety standards and regulations specific to each country. Each workplace should, as far as possible, use natural lighting, in addition to cooperation with artificial light sources. The intensity of light should be adapted to the characteristics of the room and provide the possibility of its regulation. This applies to both natural lighting with the possibility of darkening and ensuring privacy, and artificial lighting, adapted to the number of people in the room, the time of day and the amount of natural light. In the night mode, lighting should be subdued and discreet, while providing the right level of light for optimal operation.

HVAC

Proper ventilation, humidity control, and temperature regulation are essential to avoid health issues.

The employer should ensure safe and hygienic working conditions for the employees by providing an adequate ventilation and air conditioning system in the premises. This is especially true in rooms where there is a large amount of electronic equipment that generates a lot of heat and where several people work. Labor codes in many countries contain provisions for adequate ventilation of the workplace. Employers are obliged to comply with these regulations.

Computer network

For security reasons, the LAN should be divided into separate networks for: production, test, guest access and VoIP telephony. Access to these networks should be possible both wirelessly and via cable. For security reasons, the 802.1X protocol or an equivalent solution should be implemented. If the organization has enough public IP addresses, a convenient solution would be to use a separate public IP address for the translation of outgoing traffic from every network listed above. The only exception should be a test environment - it should not have an exit to the global Internet network and should be strictly isolated (even physically) from other networks. If possible, it is worth considering the use of redundant links, such as 4G/5G technology, which will allow emergency Internet access and allow the testing of services from outside the organization's network.

If the operating room is physically separated from the SOC's server room or when there are more separate locations that are used by SOC's personnel, then there are two ways of interconnecting them. One is connection via dedicated fibres and the other is via encrypted connections. Encryption can be done by encrypting all traffic using firewall/UTM class devices that support IP-Sec, MACsec, etc., or by encrypting traffic from individual ends to the main VPN hub.

Number of LAN outlets: the number of outlets should consider the number of desktop computers, laptops, printers, scanners, Wi-Fi access points, VoIP telephones and other equipment like a videoconferencing system. As mentioned previously, all accessible LAN sockets (RJ-45) should be secured against unauthorized access using 802.1X or an equivalent technology.

In addition to network outlets, there should be a Wi-Fi network providing at least 3 separate SSIDs: for employees, for guests and for the test environment. It is recommended to enable client isolation and use enterprise-class authentication.

Due to the existing legal requirements regarding the ability to work remotely, the implementation of the Remote Access VPN solution should be considered.

Power supply and UPS

Due to the role that the SOC plays in every organization, it is necessary to ensure uninterrupted operation. One of the main elements of ensuring this is the continuous power supply and this applies to both the operating room and the entire technical infrastructure necessary for the operation. Therefore, it is worth considering power supply redundancy. This means using more than one power source and automatically switching to an alternate source in the event of a power failure. Batteries of UPS systems can sustain the operation of electronic devices in case of short outages. In particular, if the 24/7 operation model was chosen, it is worth considering either installing a large central UPS system covering selected power circuits or using small individual UPS systems for each key component, not forgetting network devices, Wi-Fi, AV, etc.

If at given location power outages occur frequently or are relatively long, consider installing a power generator as an additional system to ensure uninterrupted operation.

Physical Access Control

Ensuring appropriate control of physical access to the SOC premises is an obvious requirement due to the nature of the SOC's operations. Controlling access/entry on an ongoing basis prevents unauthorized access to sensitive/key data or devices, preventing their manipulation or theft.

Psychical access protection includes measures such as:

- electronic access control system, biometric sensors, access card
- physical barriers doors, fences, gates, locks

CCTV

Physical CCTV monitoring can provide professional oversight for staff, visitors and assets. CCTV will be sufficient if the infrastructure of a building is equipped with physical monitoring. It is advised that at least one camera faces the room's entrance, so that people entering the room can be recognized.

Technical requirements

Communication

Due to diverse needs and the necessity for rapid adaptation to current requirements, it is recommended that employees have a wide range of communication tools:

- cell phones with optional wired or wireless headsets for individual communication
- PSTN / VoIP desk phones with optional wired or wireless headsets for handling the general phone number; PBX serving the SOC's PSTN / VoIP numbers should provide all basic functions like IVR, redirections, hunt groups
- PSTN / VoIP conference phones for discussions in a larger group
- videoconferencing system with ability to share content
- team collaboration application (cloud based and self-hosted) with set of basic features like voice / video calls, presence, chats, file sharing, screen and content sharing, etc.
- remote assistance / Remote desktop software

- document writing and collaboration
- whiteboard-style collaboration
- backup of the updated contact list, including:
 - SOC employees
 - decision-makers for SOC operations
 - the organization's spokesperson
 - NOC employees
 - key systems administrators
 - support contacts for all key systems.

The backup file(s) should be available independently of the primary SOC systems' operations.

Video Walls

Video walls for a security operation centre offer a view of multiple TV screens in one picture. Their large high-resolution screens make it easy to monitor everything in time and make decisions. The equipment is advised for the unit's efficient operation. Properly positioned screens should be within sight for any employees working in the unit, providing situational awareness like ticket counts, spam waves or live information sources, just to name a few.

Videowalls allow you to observe events in real time. Thanks to such a view, the organization can respond to a given threat much faster. Depending on the needs of a given moment, video walls can be used as screens that display not only events but also important events in the world, and they can also be used to display training videos.

Whiteboards

Whiteboards can be standard white ones or interactive touch screens. A dedicated place for team members to collaborate and draw ideas enriches productivity. Whiteboard walls allow for practically endless amounts of analytical reasoning for employees through the use of flowcharts, outlines, word lists, pros and cons lists, and the like. They are targeted at training, the development of expertise and the transfer of knowledge.

In a situation when co-workers in a SOC are resolving an attack problem, the Team leader writes the specific type of attack in the middle of the drawing. The remaining employees brainstorm 3-5 main ideas in a circular formation around the main topic. Anyone close to the whiteboard and can draw a line from the mind map topic to each main idea and write on the whiteboard any idea on how to stop the attack.

Systems

Case management - Ticketing system

Every SOC needs a way to track incidents. Generally, the more mature the SOC, the more sophisticated and customized the incident tracking capability needs to be. Case and workflow management is deeply integral to SOC operations, more so than any other SOC tool. As a result, a universal solution does not exist.

A list of primary requirements that should be fulfilled by such a system to be helpful for a SOC is described in **Chapter 4 - SOC technical architectures "[AGH] Incident management - Solutions review.docx"**.

Some ticketing systems will overlap with related product segments, in particular Information collection, data enrichment, and response automation – SOAR.

Security Orchestration, Automation and Response (SOAR)

SOARs are sets of products and features that, as their name implies, enable the user to quickly and efficiently design and leverage repeatable processes common to a SOC.

More about SOAR can be found in **Chapter 4 - SOC technical architectures “[AGH] Tools required to build SOC.docx”**

Centralized password management system

A key factor in maintaining strong cybersecurity within an organization is enforcing secure password policies. Therefore, the implementation of a centralized password management system is crucial. Such a system should provide:

- centralized control, which offers a single dashboard for administrators to oversee and manage user passwords, improving both supervision and security;
- IT infrastructure integration, which effortlessly connects with systems like Active Directory and SSO, simplifying password management;
- audit logs monitor and record all password-related activities, helping with compliance and security audits by tracking password strength, reuse, and usage, including two-factor authentication;
- password sharing, which allows team members to securely share credentials without exposing real passwords; and
- automated password updates, which regularly refreshes passwords to enhance security and lower breach risks.

Shift log

Maintaining continuity in managing individual cases requires documenting all significant events during the shift. This is accomplished through the Shift Log, which enables event recording, management, and most importantly, clear and transparent communication to the next shift. Effective communication and task transfer are vital, especially in a SOC operating in the 24/7 mode.

Lab for Malware Analysis

SOCs often face suspicious files that require the assessment of their purpose, content, origin, and history. One of the most common methods is to use local anti-virus and cloud-based malware analysis tools. As a Security Operations Center (SOC) evolves and its requirements advance, the necessity for malware analysis becomes more frequent and critical. Malware analysis is the process of seeking understanding of the behaviour and purpose of a suspicious file to aid in detection and threat reduction. For SOC that are well-resourced, forming an advanced malware analysis capability can be not only rewarding but also necessary. Malware analysis may be used to achieve one or more of the following objectives for the SOC:

- breaking down a piece of malware and formulating a working understanding of its attack vector and likely purpose, e.g., qualities that may link it to known malware families or actors;
- evaluating malware behaviour so that its persistence, stealth, and C2 capabilities may be understood (and thus more easily detected), such as specific IOCs; and

- feeding both the above objectives back into not only the incident currently being worked on but also the long-term understanding and assessment of threats, campaigns, and actors, as well as in support of proactive hunt.

SOCs pursuing an investment in malware analysis should consider the following tips:

1. Fully assess the SOC's need for a malware capability.
Make sure that the conditions for implementing a malware analysis capability are met, and that there is work to keep the staff engaged. By contrast, SOC's that do not see a routine cadence of advanced malware or targeted attacks may not be good candidates.
2. Give malware analysts control over their own platform.
Analysts will frequently need random tools, utilities, updates, and dependencies; leveraging a static toolset and platform, they must seek external approval to update is a non-starter [NIEJASNE]. While there can and should be deliberate core common tooling, the analysts will also need to download tools and utilities to a) suit their own tastes and preferences and b) because they need them for a given incident right now. Do not fight this as it will alienate the staff and encumber timely analysis.
3. Isolate the malware analysis environment from all other constituency resources, including the SOC's analytic platforms.
It is important that the risk of "leaks" from the malware analysis lab is minimized. The countermeasure can include techniques such as network segmentation, trusted file transfer mechanisms, easy "pave"/refresh of the analysis environment, and various procedural controls.
4. Get the SOC's rules, authorities, and procedures related to malware written down on paper.

Data storage

With so much data to choose from, it is necessary to identify the most useful data for the job up front to avoid missing important events. This can occur either due to collecting too little data and not having the relevant information available to detect and handle incidents or to collecting so much that tools and analysts become overwhelmed. Additionally, designing, acquiring, deploying, and maintaining sensor and log collection capabilities can take tremendous resources depending on the scale and complexity of deployment. Trade-offs must be made regarding ingestion rate and storage versus cost. This strategy begins by broadly introducing considerations for data collection including planning for, tuning, maintaining, and retaining these collections. It then dives deep into host and network collection and monitoring as these are at the core of the SOC's data collection strategy. It finishes up by discussing considerations for cloud and OT environments, along with summarizing considerations for a data collection instrumentation approach. The goal of this strategy is to gather the right data in the right amounts from the right places in the enterprise, with an economy of effort and expense. Most importantly, the SOC needs to be deliberate in their planning, not just taking in any data they can, but selectively targeting the data that is most relevant and ensuring that appropriate policies are in place to allow them to collect this data. They also need to ensure they have the appropriate policies and budget approach in place to support data collection.

To get started on selecting the right data to collect, the SOC should pick a handful of business use cases which are important to the constituency and identify the top threats the SOC wishes to defend against. This will then drive which feeds are necessary to build out these use cases.

There are several drivers for the collection of security-relevant telemetry, many of which overlap between the SOC, other elements of the cybersecurity apparatus, and traditional IT operations. The most important are:

- defending networks, systems, cloud resources, and other digital assets
- insider threat monitoring and audit collection
- performance monitoring
- maintenance troubleshooting and root-cause analysis
- configuration management

Once the SOC understands the situations for which it wants to collect data, it next needs to consider the types of data available. Each SOC will choose data feeds to best illuminate the enterprise for preventing and detecting intrusions and other monitoring activities. The data the SOC needs will come from a variety of sensors and logs; understanding these potential sources is a key step in determining what data can support what use case and what data to prioritize collecting.

When considering what data to collect, it is mandatory to take into consideration what impact this process will have on the constituent systems. Collecting security and audit logs may degrade systems with limited CPU and memory amounts. There are several tips for minimizing the impact of collecting security telemetry:

1. Minimize the number of agents deployed, especially on end systems.
2. Carefully tune performance-related parameters of the agent.
3. Leverage existing collection points.
4. Leverage reliable delivery where this option exists.

In conjunction with identifying available data sources, the SOC needs to ensure it has the proper authorities and agreements in place for the data it is going to collect.

As the SOC is developing its data collection plan, it needs to consider how it will pay for the transport and storage of the data. The SOC needs to maintain awareness of how the collection volume may change over time. As applications move to the cloud, the volume of data flowing past perimeter taps and through firewalls increases, which also increases the amount of NetFlow or firewall events captured. These trends must be taken into account including some caveats:

1. Data volume estimates assume wide coverage and saturation of each technology.
2. This is not a strictly stack-ranked list of sources; for example, it is possible to make a single email gateway produce far more data than a given network firewall.
3. Even though a given data source may not be shown to cover a given function (such as analysis or forensics), it does not mean it will never support that goal.
4. Because estimating the overprovisioning of storage capacity is challenging, using a highly scalable option appears to be the most reasonable solution.
5. The general relationship between the volume of generated data and the types of data collected is shown in the chart below (Figure 1). The chart also highlights three areas of application for the collected data: preventative, detection, and analytical / forensics.

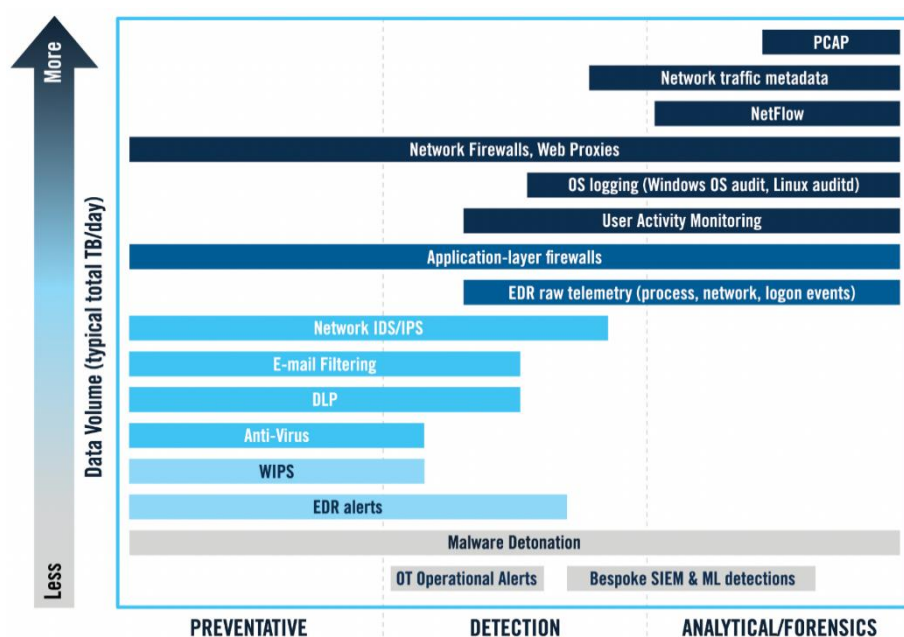


Figure 1 Data Source in the context of the SOC Usage and Volume.

Source: K. Knerler, I. Parker, C. Zimmerman "11 Strategies of a World-Class Cybersecurity Operations Center". MITRE, 2022. Page 186

Once the SOC has selected data feeds for collection, these feeds should be tuned. If the SOC over-tunes its data, it will miss important information that could help identifying malicious activity. If the SOC under-tunes its data, it can result in inefficient processes or missing the important activity due to all the noise and very high IT/cloud bills. One of the first things to do is to tune out any data that is known to have a low information value with respect to the SOC needs.

There are many options for determining which data is collected and processed locally, and which data is exported to a central SIEM for correlation. In general, when tuning data sources, larger, geographically distributed constituencies design collection as a combination of local and central techniques for processing and collection.

The amount of collected data is directly dependent on the required retention time. The duration for which the SOC must keep data is influenced by a mix of legal and regulatory obligations, the organization's risk profile, and financial limitations. The table below (Figure 2) shows the suggested values proposed by the authors of the study "11 Strategies of a World-Class Cybersecurity Operations Center".

Category	SOC triage	SOC forensics & investigations	External Support
EDR, network sensor alerts, and SIEM-correlated alerts	2 weeks	6 months	2+ years
NetFlow & traffic metadata logs	1 month	6 months	2+ years
Full-session PCAP	as needed	as needed	as needed
System, network & application audit logs	2 weeks	6 months	2+ years

Emails	2 weeks	2 years	As needed
--------	---------	---------	-----------

Figure 2 Suggested Minimum Data Retention Time Frames.

Source: K. Knerler, I. Parker, C. Zimmerman "11 Strategies of a World-Class Cybersecurity Operations Center". MITRE, 2022. Page 191.

Computer requirements

Dedicated workstations for the SOC personnel and separated workstations for incident responders and malware analysis are mandatory. Some advantages may be considered when laptops are to be used instead of the workstations. They allow easier relocation of workplaces in case of a disaster. When using laptops, it is important to implement additional organizational and technical measures to ensure information security.

Monitors

For comfort, we suggest using two large monitors, which improves the quality and efficiency of work. It also improves security, for example, in case of possible screen sharing or remote assistance, only one screen can be shared.

Keyboard/mice

Human interface devices are a highly personal choice, and people spend thousands of hours with them during a year, so spending some money on them is worth doing. The ideal way of doing it is providing some budget and letting people choose their own devices. Employees will keep their devices in personal storage and connect them to the computer at the beginning of their shift.

Headsets

An essential part of the team's work is communication. To facilitate it as much as possible and to enable independent conversations in an open space room, it is recommended to equip employees with individual headsets. If possible, allow employees to choose headsets according to their individual preferences so that they can use them comfortably throughout their shift.

Authentication

In a SOC, as in any organisation, the employees use systems that require authentication for access. A login-password pair is a commonly used method of authentication but is generally considered as insecure. Currently, the security standard is using Multi-Factor Authentication (MFA). Therefore, additional devices may be required to enable to deliver of an additional factor, such as:

- smart card readers
- fingerprint readers
- U2F Key

Vault

A basic, lockable locker should suffice for storing devices such as laptops, smartphones, USB drives, and portable or external hard drives provided to the SOC for examination. However, if there are specific legal or organizational requirements for storing items like

personal data, whether printed or digital, or physical evidence, then a vault might be necessary.

Processes and work organization

SOC structure

Before choosing the shifts coverage model in a SOC, a few decisions must be made based on factors that have fundamental impact on its organization and structure.

The SOC can have either tiered, tier-less or “SOC-everything” structure and choosing the one which best suits the organization is not an easy process.

If the organization prefers a SOC department which is under the same management, then all the core and auxiliary functions (detection, incident response, support, assessment and threat intel) are at the same level.

The core functions of a SOC include:

- continuous monitoring of systems and networks to detect potential threats
- identification, analysis, and classification of security incidents
- rapid response to detected threats, including isolation and removal of threats
- assessment and management of IT security risks.

Auxiliary functions of a SOC may include:

- providing training for employees on security best practices
- regularly conducting penetration tests to identify weak points
- conducting security audits and ensuring compliance with regulations and standards
- tracking and analysis of the latest trends in cybersecurity
- coordination with other departments of the organization to provide comprehensive protection

One of the alternatives introduces an additional reporting structure with the SOC managing the core functions while auxiliary functions are managed by a separate security director.

Very large SOC structures have dedicated directors for all its core and auxiliary functions.

An alternative approach involves deciding whether to establish a tiered or non-tiered SOC.

In the traditional tiered model, T1 analysts are the initial responders who receive and triage alerts from security appliances. Alerts that T1 analysts cannot resolve or those that require more advanced solutions are escalated to T2, and if specialized expertise is needed, further escalated to T3.

The job breakdown of such a T1-T3 structure is dependent on the model chosen a step before – the management structure and functions fragmentation.

If a SOC follows a tiered model, the central coordination in the SOC will likely need the following authorities in addition to those of the lower tier SOC:

1. Serve as an entity with a higher authority to the subordinate SOC.

2. Have access to security-relevant data from all subordinate SOC which may come in the form of aggregate metrics, summarized data, a view into the data, or situation specific content rather than all raw logs.
3. Coordinate response actions among the subordinate SOC.
4. Manage improvements of the subordinate SOC capabilities and operations, in accordance with fulfilling incident response requirements across the greater constituency.
5. Manage devices that aggregate security-relevant data from the subordinate SOC and sensors directly placed on hosts and networks, especially when the subordinate SOC do not have the engineering skills to do this on their own.
6. Act as the focal point for constituency-wide security information sharing and security awareness through common practices, SOC-provided and developed tools, and preferred technologies or standards.
7. Propose standards such as constituency-wide preferred standard network and security monitoring technologies and practice.
8. Negotiate constituency-wide licensing/pricing agreements of monitoring technologies that may provide benefits to the subordinate SOC, where possible.

To make a tiered SOC work well, the SOC must fulfil the following conditions:

1. **Ensure that service level objectives (SLOs) are not only defined, but also understood and agreed to by the analysts themselves, and updated as necessary:** Do not give an analyst a rigid 120 seconds to investigate every single alert. Give them the opportunity to dive a little deeper so that they have more ownership of the process while not ignoring the incoming queue for hours.
2. **Do not allow other staff to look down on Tier 1:** Most SOC professionals started as junior analysts. This is a growth position, not an underclass one. Tackling an alert queue is a transformative experience and will change the perspective of almost anyone engaged in this role. It is experience-building and a necessary position just like any other.
3. **Promote, advance, and automate, as appropriate:** It is important to prevent role stagnation. Once an analyst has mastered a role, a) evolve their job function and/or b) give them the ability to automate functions of their existing role, allowing them to move on to new tasks.
4. **Do not force an “up or out” culture:** If an analyst is doing well in their current position, and they do not want to move on, or should not, do not force them to. If advancement is overdriven, it can cause people to leave prematurely.
5. **Enable flexibility in role:** An analyst should not feel limited because of their role title. In a tiered scenario, allowances should be provided for analysts that show growth in skills or abilities, even if their title does not change. This might involve implementing job rotations for employees. It is a human resources strategy where employees are periodically moved between different roles, tasks or departments within an organization. This practice is commonly used as part of employee development programs, workforce flexibility strategies or succession planning. Job rotation involves planned shifts that allow employees to gain experience and skills in different functions, potentially over set intervals.

The tierless model is somewhat easier as there are no T1, T2 or T3, but all team members work in a flat structure, taking care of incidents from the first appearance in the SOAR system.

The choice of the model is made either at the initial step of building a SOC or later as a result of a reorganization process if requirements and conditions change.

We can compare these models as they both have pros and cons.

The tiered model limits analysts' growth, which causes potential retention issues. The tierless model is also not that perfect : it requires a more responsible team, it has a less defined process so management is more complex, and it can become riskier if expectations are not properly set by managers.

To make the tierless SOC structure work well:

1. **Nurture new staff in a way that does not jeopardize investigative quality.** If new staff are going to be asked to evaluate an event and determine if it is an incident, they will need assistance. This means they should be provided with all resources, such as playbooks, to aid in their decision making and they should have appropriate oversight, often by being paired with a senior analyst who can consult their work as needed. In this regard, even SOC's without tiering can still share qualities of those that are tiered.
2. **Help staff prioritize their work:** If staff members are responsible for both triaging incoming alerts and doing longer incident response, or other functions (like maintaining SOC tools or hunting), they may find it difficult to know what they should work on first. Depending on the analyst, certain responsibilities may get more or less attention. Try to balance staff feeling ownership for how they manage their time with clear written and verbally communicated expectations for what is a priority. Keep an eye out for analysts that always seem to focus on one aspect of the job over another; this may indicate a need to step in to better understand the situation.
3. **Manage separation of duties and reduce duplication of effort:** As the SOC gets larger, separation of duties becomes increasingly necessary. Without formal separation of duties, staff may become very fragmented in their time. This does not mean a tierless structure cannot work, it just means that perhaps the role descriptions are slightly narrowed and not everyone does everything.
4. **Create a culture where staff work together and help each other out:** Some incidents just take longer to work through than others. If one staff member gets involved in a significant response activity that takes them away from a more routine event triage, have other analysts jump in to fill the gap. They should then pay it back to their colleagues by supporting them in the same way.

Although there are no hard lines to be drawn, the table below (Figure 3) gives a general feel for the relationship between the constituency size and the different SOC structures. None of these structures are necessarily better than another. However, they do come with different challenges, opportunities, and expectations which will be discussed in the next few sections.

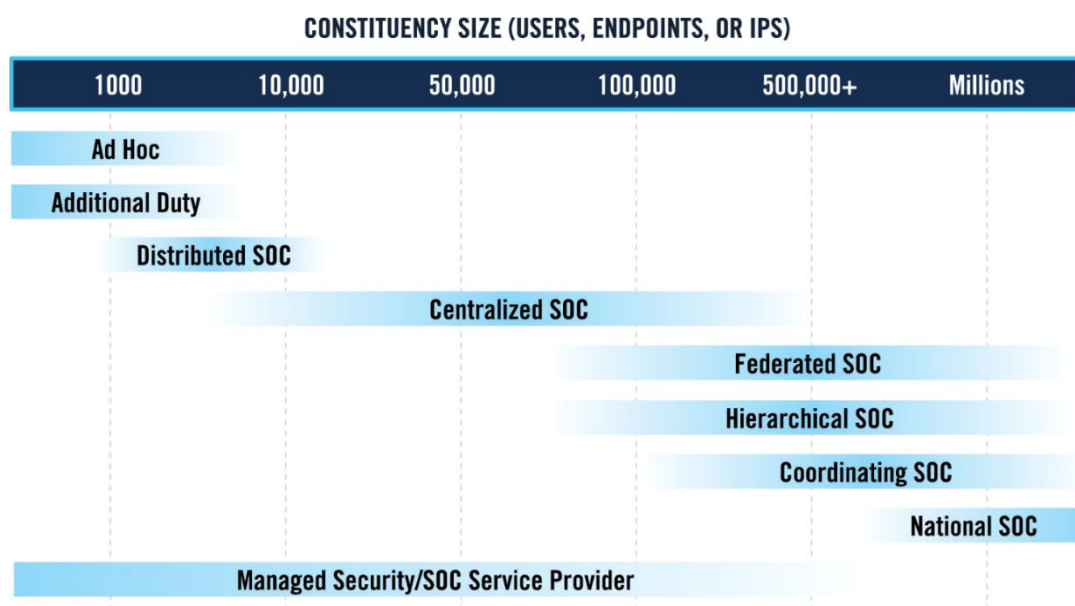


Figure 3 Constituency size (users, endpoints, or IPS).

Source: K. Knerler, I. Parker, C. Zimmerman "11 Strategies of a World-Class Cybersecurity Operations Center". MITRE, 2022. Page 55.

When considering if the SOC should be tiered or tierless, consider which model will best allow you to do the following:

1. **Respond to all alerts:** ensure that every alert purposefully curated and sent to the SOC for triage is, in fact, triaged.
2. **Respond to alerts in a timely manner:** no alert should sit untriaged beyond the triage SLO, which is usually less than an hour. However, be cautious about closing out alerts too quickly and sacrificing quality for quantity. Auditing or reviewing some alerts to ensure proper handling can help address any potential gaming of the metrics.
3. **Investigate every alert properly:** ensure each alert is given due attention by the analyst. Routine alerts are dispositioned with routine handling, and unusual alerts are given the hours of in-depth investigation they deserve, without unduly rushing the analyst to prematurely click alerts to closure.
4. **Give everyone the opportunity to work at their level:** people new to security operations do not usually have the practice and knowledge to perform in-depth analysis and incident closure. Those with years of SOC experience may feel this role is behind them. Without compensating controls, pooling a large group with varied experience can cause errors in analysis. In fact, some analysts may never progress past "front line" alert triage type functions.
5. **Give everyone the ability to advance:** in a tiered structure, that this may require more deliberate rotations or more formal promotions.
6. **Maximize operations quality and repeatability:** this can be done through standardization, automation, training, documentation, and continuous improvement. Each of these elements contributes to a SOC that can consistently handle incidents effectively, respond rapidly, and adapt to emerging threats, ultimately protecting the organization more effectively and efficiently.

Shifts

After choosing the SOC model that meets our organizations' expectations (both functional and business related), we can switch our attention to operations, staff, shifts and how they are organized and managed. Shifts are mostly relevant to security analysts,

or the first line of defence and the initial phase of incident response. Non-analysts jobs are mostly covered by 8x5 specialists with on-call readiness if needed.

First, it should be decided whether our SOC requires 24x7 operation or whether 8x5 or similar is a satisfactory solution. This may be a fundamental decision because 24x7 coverage is both expensive and has potential turnover implications, retention is more difficult, off-hours escalations should be created, and premium for off-hours is mandatory. However, an organization makes assumptions that attackers may be thinking about striking when nobody is watching, and this is not far from reality.

Considerations for moving to a 24x7 SOC include the following:

1. Is there a specific set of targeted or advanced threats against the constituency that suggests intrusion activity is likely to happen outside of normal business hours?
2. What is the size of the constituency and what are its normal business hours? Does its user population have after-hours access to the IT resources?
3. Does the constituency's mission encompass 24x7 operations that depend on IT, which, if interrupted, would significantly endanger revenue or life?
4. Have members of the SOC come in after hours to handle an incident, or have they discovered an incident outside SOC duty hours that could have been prevented if someone were there to catch it? Has this happened several times?
5. If an attack occurred during off-hours and there was an analyst there to notice it, are there resources outside the SOC that could stage a meaningful response before the following business day?
6. How big is the current SOC's staff pool? Are there only four people, or is it funded to support a team of 50 or more analysts? Is there the financial ability to increase the size of the team to meet a 24x7 staffing need?
7. Is the host facility open 24x7? If not, can the SOC be granted an exception?
8. Is there an organizational stigma associated with not being operational all the time? Some SOC's are considered a legitimate operations centre only if they function 24x7.
9. Is there a tolerance for a delay in identifying suspicious events? A SOC that is not 24x7 must catch up every morning on the previous night's event data; for those that do not staff on the weekends, this is especially challenging on Monday.

If a SOC does move to 24x7 operations, some additional things to consider are:

1. **24x7 SOC's will usually want to maintain a minimum staff of two analysts at all times:**
 - a. Two-person integrity is a best practice in monitoring since having only one person there with access to a lot of sensitive data and systems can present problems, no matter how well-vetted the employees.
 - b. There are logistical and safety concerns with keeping the floor staffed and secured when someone needs to leave the room.
 - c. With multiple analysts always on shift, they can cross-check each other's work.
 - d. Being the sole person on shift can be very lonely and monotonous.
2. **Each 24x7 seat requires roughly five full time equivalents (FTEs), including fill-in for vacation and sick leave:**
 - a. This is very expensive compared to 8 x5, 12x5, or even 12x7 staffing.

- b. Assuming a minimum of two filled analyst seats, that means roughly 10 FTEs, potentially 11, depending on leave and vacation policies within the organization.
- c. Therefore, taking a SOC from 8x5 to 24x7 requires an increase of at least eight FTEs.

3. Analysts on night shifts may feel underinformed, underutilized, and unrecognized:

- a. The night shift does not see the fruits of their labour as much because detailed analysis, response, and feedback usually occur during normal business hours. It is important to have regular deliverables/work output from those on night shift and regular feedback regarding what happened during the day. Because night-shift staff have far fewer interruptions, it may be effective to give them unique tasks that require several hours of focused work, such as in- depth trending or cyber threat intelligence analysis.
- b. Casual information sharing is less likely to occur when only a few positions are staffed, and a dedicated effort must be made to ensure collaboration across the entire team regardless of the shift time.
- c. One way to offset the issue of staff feeling disconnected is by rotating staff between days and nights every couple of months.
- d. Collocating the SOC ops floor with a NOC or IT Operations floor may help, especially with loneliness and management supervision.

Covering 24x7 requires at least 10-12 specialists and if we take into account possible sick-leaves and vacations , it is about 5 times more costly to have 24x7 than 8x5 SOC.

Possible shift configurations for 24x7:

- 12 hour shifts, 4 on 3 off (this model is least recommended as 12 hours of continuous work reaches lower efficiency past the 9th hour, which is a risk for operations)
- 10 hour shifts, 4 on 3 off
- 8 hour shifts, 7 on 3 off or 5 on 2 off (the most recommended model, efficiency does not diminishing significantly during shift)

Special treatment is needed for nights, weekend and holidays coverage and there are two options:

1. Permanent staff for each shift
 - better for team work and work-life balance
 - hierarchy and tensions may form between shifts
2. Rotation
 - no one is stuck on nights or at weekends
 - burnout is more common and work-life balance is in danger

Alternative approaches:

- extended hours: 7am to 7pm
- 8x5 with on-call after business hours: shift is aligned with business hours

The number of cybersecurity professionals needed by a SOC will be driven by factors such as the SOC mission and offered capabilities, size of the constituency, level of

automation, and funding available. Key factors that drive the number of staff needed for each capability area include:

1. **Real-time Alert Monitoring and Triage:** the number of alerts coming in and the level of automation that supports alert triage.
2. **Incident Analysis and Investigation:** Incident Coordination; Containment, Eradication and Recovery: the frequency of the number of cases that move from alert to an incident and the ability of each analyst to turn over cases, which is influenced by both their skills and the tools available to them.
3. **Cyber Threat Intelligence Collection, Processing and Fusion, Threat Hunting:** the most open ended of the SOC capabilities. Impacted by the risk posture of the constituency and the amount the constituency can afford to invest in these capabilities to help them reduce the risk.
4. **Vulnerability Scanning:** the number of systems being scanned or monitored; the complexity and efficiency of the tools being used; the complexity of the environment being scanned.
5. **Vulnerability Assessment, Attack Simulation and Assessments:** the risk posture of the constituency, which helps determine scope and frequency.
6. **Security Capability Engineering and Management:** Network, Endpoint, Cloud, Mobile, OT, and Analytic Platform: The number of sensors and covered nodes per the sensing technology; the number of different sensing technologies being used; the degree of automation and reliability of that platform; whether those different platforms can be managed centrally or are they on disparate networks or identity planes, requiring the administrator to “swivel chair” between them; and the engineering processes/life cycle requirements of its parent organization.
7. **SOC Enclave Engineering and Management:** the number and complexity of SOC systems in operation; how often new capabilities are rotated into operation; whether the SOC has any homegrown or custom capabilities to which it must devote development cycles; where (and if) a line is drawn between the system administration and engineering functions, and if any of these functions are performed outside of the SOC.
8. **SOC Leadership and Management:** size of the SOC; organizational standards and practices.

Shift handover and knowledge transfer must be done between shifts for summary and investigation continuation if it is ongoing. Every new type or class of incidents requires a knowledge base and use case updates for the other analysts. This is done in the last hour of the shift (when the situation permits and without a negative impact on ongoing investigations) and the new shift overlaps with the previous shift to share the ‘need to know’ and eliminate gaps.

Regardless of the staffing model, here is what can go in the pass-down log:

- names of the SOC operations staff on duty
- issues passed down from the previous shift, especially those mentioned verbally and not captured in the previous pass-down log
- case IDs opened and closed during the shift
- tips and referrals from other parties such as the help desk or user
- any issues escalated to parties outside the SOC
- sensor or equipment outages seen
- any sort of anomalous activity seen, especially if it has not yet spawned a case
- any anomalous activity that was seen that requires the incoming shift to continue analysis or escalation procedures
- a check-off of duties that the team was required to accomplish

- details on any tasks assigned to the shift that were not completed or need further attention
- anything else of significance that was encountered during the shift that is not covered in the SOC's SOPs

Special attention must be paid to this sharing if the customer (does not matter if internal or external) is in contact and it must be done in the way that does not require the customer to explain the already explained details to the SOC team.

Nowadays, SOC's rely on electronic ways of creating and delivering/sharing data and incident details and paperwork is not the preferred way of sharing. SOC teams work using SOC platforms and SOAR systems and all documentation should be made visible to the appointed and authorized team members with respect to security rules (confidentiality, integrity, availability (CIA), need to know, least privilege, etc.)

Last but not least is the management issue and coordination functions within the SOC and SOC management as a position. In smaller organizations, the team lead or manager may split their time between technical and managerial responsibilities. In medium and large SOC's, the SOC manager may focus almost entirely on day-to-day management, driving the SOC performance; communicating the value of the security operations to others; evolving the SOC through new technologies and processes; and recruiting, training, and assessing the staff. Consider the SOC's own organizational standards and practices to identify how many leads are needed given the number of individual contributors. If the SOC is 24/7 operation, it is often helpful to designate a lead per shift- either a manager, technical lead, or senior analyst.

A SOC greatly benefits from having leaders with a background in security operations as it takes strong technical understanding of the problem space to be able to make informed risk decisions. The most effective SOC leaders will have a mix of:

- qualities common to any leader such as people management skills
- technical and cyber literacy
- orientation toward high-ops tempo, high-stress positions requiring courage to make tough decisions and negotiate difficult decisions with leaders at all levels of the food chain

Just as the SOC operates within the context of a constituency, it also operates within a legal and regulatory environment. Much of this context will be specific to the country in which the SOC operates and will be driven by the type of legal system of the country and the types of laws in place. Things that the SOC will want to be aware of include:

- type of legal system the SOC operates under (e.g., civil or common law)
- role of the SOC in legal and regulatory compliance

Many regulations or standards only apply to certain countries. Some of these will impact how the SOC helps protect the systems and data of the constituency and some will define how the SOC executes in its own mission through actions such as reporting requirements. The SOC is not expected to be an expert in this area, rather they should build their operations with the support of legal counsel to ensure compliance.

Absences

The organization of the SOC's work should provide for the situations of an unplanned absence of an employee beforehand. The earlier the employee informs about the

absence, the more time the shift manager has to decide whether it is necessary to provide a replacement or whether the Centre will be able to operate with a reduced staff. Bearing in mind the 24/7 nature of the SOC's activities, it is worth introducing the rule of informing about an absence at least 8 hours in advance. It would also be desirable to develop a scheme for selecting a replacement person, as well as a method of gratification for such unplanned activity of the employee.

Students

Analysing the organization of a SOC in an academic environment, we cannot overlook the aspect of employing students. The cybersecurity industry faces a significant shortage of skilled workers. This issue is especially difficult in higher education, where salaries and benefits lag behind those in the corporate sector. A solution to this problem, particularly at technical universities, could be the employment of students. In every case, students should work under the supervision of experienced SOC employees. Moreover, professional activation of students, allowing them to gain invaluable practical knowledge during their studies, constitutes an additional, very valuable gain for the universities participating in the project, directly translating into the increase in the competencies of graduates.

SOC Setup and Environment (Physical and Technical) KPIs

These KPIs for the SOC setup and environment are designed to track and ensure the physical and technical robustness of the SOC infrastructure. They help maintain operational readiness, ensure employee well-being, and support continuous monitoring and response capabilities effectively. Each KPI targets specific aspects of the SOC's physical and technical setup to ensure smooth operation under all conditions.

Table 7 – KPIs for the SOC setup and environment

Physical Security of the SOC Premises

Percentage of Physical Access Controls Implemented. Measurement of the implementation rate of physical access control measures, such as electronic access systems, biometric access, security doors, and physical barriers. Aim for at least 95% implementation to mitigate unauthorized access risks.

Coverage of CCTV Monitoring. Measure the coverage of the CCTV systems in critical areas, such as entry points and server rooms. The KPI could be expressed as "Percentage of the SOC area under CCTV surveillance," aiming for 100% to ensure maximum coverage.

Soundproofing Efficiency. Evaluate the soundproofing of walls, doors, and windows to ensure sensitive discussions are not overheard. The KPI could be "Rate of soundproofing compliance as per standards," targeting full compliance to prevent information leakage.

Workplace Design and Comfort	Percentage of ergonomic solutions implemented in the SOC workstations aiming for 100% to reduce workplace-related health risks. Desk Layout Optimization. Evaluate how effective the current desk arrangement is for facilitating teamwork and efficient information exchange. The KPI could include "Percentage of staff satisfied with the desk layout for collaborative work." Ideally, target a satisfaction rate of 85% or higher based on internal surveys. Percentage of workstations with adequate natural and artificial lighting" and the number of HVAC inspections per year to ensure proper temperature and air quality control, targeting quarterly checks for optimal conditions.
Power Supply and Backup Systems	Uninterrupted Power Supply (UPS) Coverage. Measure the percentage of critical equipment connected to UPS systems. KPI: "Percentage of critical devices connected to UPS" aiming for 100% to ensure no downtime in operations during power interruptions. Power Generator Testing Frequency. Monitor the frequency of power generator testing to ensure readiness. The KPI could be "Number of successful generator tests per year," aiming for quarterly tests to guarantee reliability during prolonged outages.
Network and Communication Infrastructure	Network Segmentation Effectiveness. Measure the effectiveness of network segmentation between production, test, and guest networks. The KPI: "Percentage of critical network segments isolated per security standards" aiming for full segmentation to enhance security. Redundant Internet Links Availability. Assess the availability of redundant internet links (e.g., 4G/5G technology) to maintain connectivity during failures. The KPI: "Percentage of time redundant links were operational during outages," aiming for 100% availability as an emergency backup. Number of Active Secure Wi-Fi Networks. Measure the number of separate Wi-Fi networks (e.g., staff, guest, test environment). The KPI: "Number of distinct SSIDs provided for specific SOC operations" with a goal of maintaining separate networks for better security.

Workspace Utilities	Common Room Utilization Rate. Evaluate how frequently the common room is used by employees for breaks, indicating staff satisfaction with available facilities. The KPI: "Percentage of staff using the common room daily," aiming for high utilization as a sign of positive workspace culture and comfort. Conference Room Availability. Measure the availability and use of conference rooms for team meetings, job interviews, and planning sessions. The KPI could be "Percentage of time conference rooms are occupied versus available," ensuring rooms are efficiently used but not overly scarce.
Security Operations Tools and Equipment	Availability of Communication Tools. Measure the availability and reliability of communication tools (e.g., PSTN/VoIP phones, team collaboration apps). The KPI: "Percentage of fully functional communication tools during operations" with a target of maintaining 100% functionality to support internal and external communication. Video Wall Functionality. Assess the operational readiness and effectiveness of video walls used for monitoring security events. The KPI: "Percentage of uptime for video walls" aiming for 99% or higher, ensuring that crucial visual information is always accessible for monitoring.
Shift and 24/7 Operations Readiness	Shift Handover Quality Index. Monitor the effectiveness of shift handovers to ensure continuity. The KPI could be "Percentage of shift handovers completed without missed incidents or information gaps," targeting 100% as missed information could lead to security gaps. Frequency of Cleaning and Maintenance Activities. Measure how often cleaning and maintenance are carried out in the SOC space, especially during night shifts, to ensure cleanliness and hygiene in a 24/7 environment. The KPI: "Number of maintenance activities scheduled per week" ensuring minimal disturbance during critical operations.

Incident Monitoring and Response KPIs

These KPIs focus on the end-to-end process of incident management, from detection to resolution. The goal is to ensure that incidents are identified rapidly, escalated appropriately, analyzed effectively, and remediated thoroughly, while maintaining compliance and learning from each incident.

Table 8 – Incident Monitoring and Response KPIs

Incident Detection and Escalation	Time to Detect (TTD) Incidents: a maximum of 5-10 minutes for high-priority alerts to ensure minimal impact. faster detection helps reduce the time a threat actor can remain in the environment, thereby limiting potential damage. Incident Escalation Rate: around 20-30% of incidents, indicating that Level 1 analysts can resolve a significant portion, while complex threats are effectively escalated. efficient escalation helps prioritize resources for critical threats, reducing false positives and avoiding analyst burnout. False Positive Rate: a false positive rate of under 10%, indicating a well-tuned detection system a lower false positive rate allows SOC analysts to focus on real threats, improving productivity and reducing alert fatigue
Incident Response and Containment	Time to Respond (TTR) to Incidents: less than 15 minutes for critical incidents. a shorter response time limits the spread of a threat, minimizing impact and reducing recovery costs. Percentage of Incidents Contained Within SLA: 95% or above for critical incidents meeting containment SLAs helps ensure the organization remains within acceptable risk tolerance levels Incident Escalation Time: within 5-10 minutes for high-priority alerts. quick escalation ensures that higher-level engineers address complex threats promptly, reducing the risk of prolonged exposure.

Incident Analysis and Root Cause Identification	Incident Root Cause Analysis Completion Rate: 90% or higher. root cause analysis helps in learning from incidents and improving prevention measures for similar future incidents. Average Time to Complete Incident Analysis: within 24 hours for major incidents. quick and thorough analysis ensures the threat is understood and remediated effectively, while lessons are extracted for future security enhancement. Incident Severity Classification Accuracy: 95% or higher accuracy. proper classification is crucial to ensure that resources are allocated effectively, with priority given to the most serious threats.
Incident Resolution and Remediation	Incident Mean Time to Resolution (MTTR): MTTR of less than 48 hours for medium-severity incidents, and under 8 hours for high-severity incidents. a shorter MTTR means that incidents are being handled efficiently, minimizing disruption to operations. Percentage of Incidents Remediated Without Reoccurrence: 98% or above. this KPI measures the effectiveness of incident response and remediation steps, ensuring threats are fully addressed and do not reoccur. Patching and Remediation Compliance Rate: 95% compliance within SLA for critical vulnerabilities identified during incident response. ensuring vulnerabilities are patched in a timely manner helps prevent future exploitation.
Collaboration and Team Efficiency	Average Number of Incidents Handled per Analyst:

	number of incidents handled by each Level 1 and Level 2 analyst per shift. 10-20 incidents per analyst per shift, depending on severity. helps assess whether the workload is manageable and evenly distributed, preventing analyst burnout. Incident Collaboration Effectiveness: collaboration in at least 30% of major incidents. effective collaboration enhances response capabilities by pooling knowledge and resources, particularly for complex threats.
Reporting and Documentation	Incident Documentation Quality Score: 95% of incidents documented thoroughly with all details required (e.g., timeline, actions taken, lessons learned). comprehensive documentation ensures consistent record-keeping and supports future learning, audit requirements, and compliance. Post-Incident Review (PIR) Completion Rate: 100% for major incidents. PIRs help identify lessons learned, improve processes, and share findings across the SOC to enhance overall preparedness. Compliance with Reporting Requirements: 100% for all incidents that meet reporting thresholds. ensures regulatory compliance, avoiding fines, and maintaining organizational reputation.
Proactive Threat Management	Number of Threat Hunts Initiated Based on Incident Trends: at least one proactive hunt per month. helps identify potential threats before they materialize as incidents, boosting overall security posture. Threat Intelligence Integration Effectiveness:

	70% or above, showing effective utilization of CTI data in response workflows. Integrating threat intelligence provides valuable context and helps identify threat actors and tactics more effectively.
--	---

Compliance and Regulatory Requirements KPIs

Regulatory Compliance Rate	Adherence to GDPR Requirements: 100% compliance in all processes involving personal data collection, handling, and processing. GDPR compliance is crucial for SOC's dealing with user data. Adhering to the GDPR reduces the risk of legal penalties and ensures data subject rights are respected. NIS 2 Directive Compliance: Full compliance by the specified deadlines. The NIS 2 Directive establishes guidelines for a high level of network and information security across the EU. Compliance ensures the SOC adheres to the latest cybersecurity measures and standards.
Audit and Monitoring KPIs	Completion Rate of Internal and External Audits: 100% completion of scheduled audits, with no significant non-conformities reported. Audits ensure that the SOC adheres to compliance standards and that any identified issues are addressed promptly. Average Time to Address Audit Findings: Within 30 days of audit completion. A quick response to audit findings indicates proactive compliance management and commitment to improving security controls.
Incident Reporting Compliance	On-Time Incident Reporting to Authorities: 100% of incidents reported on time, particularly those involving personal data breaches as mandated by GDPR (within 72 hours).

	Ensures the organization remains compliant with legal requirements, avoiding penalties and preserving trust. Accuracy of Reports Submitted: All incident reports submitted must be complete and accurate to avoid regulatory scrutiny. Accurate and complete incident reports demonstrate thoroughness and compliance with regulatory standards, minimizing legal risks.
Compliance with Data Protection Policies	Data Processing Agreement (DPA) Adherence: 100% of agreements reviewed and updated to reflect compliance with the GDPR requirements. Ensures that third-party service providers adhere to similar data protection standards, reducing the risk of third-party-related breaches. Data Retention Policy Compliance: 100% compliance in retaining only data that is necessary and within the specified retention periods. Helps to reduce data storage costs while ensuring compliance with the GDPR's data minimization principle.
Employee Training and Awareness	Employee GDPR and Regulatory Compliance Training Rate: 100% of employees should complete regulatory compliance training sessions each year. Regular training ensures that staff are aware of their roles in maintaining compliance and helps avoid unintentional violations. Testing and Awareness Campaign Participation Rate: 90% participation rate for compliance-related activities. Awareness campaigns promote a culture of compliance within the SOC, reducing the risk of non-compliant behavior.
Third-Party Compliance Management	Third-Party Compliance Assessment Frequency:

	Quarterly compliance checks for all critical vendors. Regularly monitoring vendor compliance ensures that third-party providers adhere to agreed-upon standards, which is essential for maintaining the overall security of the SOC. Non-Compliance Rate of Vendors: Less than 5% non-compliance rate. Minimizing the number of non-compliant vendors ensures the overall security and compliance of the SOC are not compromised.
Policy and Procedure Updates	Frequency of Policy Review and Update: Review and update all key policies at least once per year or when major regulatory changes occur. Regular policy updates ensure the SOC adapts to new regulatory requirements and keeps up-to-date with best practices. Implementation of Regulatory Changes: 100% implementation of regulatory changes as per deadlines set by authorities. Timely implementation of changes prevents compliance gaps that could lead to fines or operational issues.
Data Subject Request (DSR) Management	Data Subject Request Response Time: Response within 30 days as mandated by the GDPR. Ensuring prompt response to DSRs reduces the risk of non-compliance with the GDPR and demonstrates respect for individual rights. Percentage of DSRs Successfully Handled Within SLA: 100% of requests to be completed within the SLA. Meeting SLAs ensures that the SOC respects individuals' rights and complies with the GDPR.

Collaboration and Information Sharing KPIs

Collaboration with External Partners	Number of Partnerships with External Entities: At least five active collaborations with significant partners. Formal partnerships enhance access to threat intelligence, share expertise, and support SOC operations by learning from others' experiences. Frequency of Collaborative Meetings: Minimum of one session per quarter. Regular interactions with partners help ensure ongoing exchange of information, addressing emergent threats through collaborative problem-solving. Information Exchange Volume: At least ten intelligence packages per month. Ensures that relevant and timely information is being exchanged, helping to stay ahead of emerging threats through collective knowledge.
Internal Collaboration within SOC	Inter-team Coordination Efficiency: 100% of major incidents should involve collaboration across relevant teams. Ensures that the knowledge and skills of all SOC members are being utilized to their full potential to handle complex security incidents. Internal Information Sharing Events: At least one internal knowledge-sharing event per month. Encourages a culture of learning and information exchange within the SOC, keeping everyone updated with new tools, techniques, and attack scenarios. Integration Between SOC and Research Teams: Participation in at least three research projects per year. Promotes collaboration between the SOC and academic research teams, leveraging real-world data to develop new detection methods or countermeasures.

Cyber Threat Intelligence (CTI) Sharing	Frequency of Threat Intelligence Updates: At least one major update per week, depending on the threat landscape. Sharing up-to-date threat intelligence ensures that both internal teams and external partners are aware of the latest threats, which helps in collectively enhancing cybersecurity defenses. Percentage of Shared Threat Intelligence Integrated by Partners: 70% or higher. This KPI shows the relevance and quality of the threat intelligence being shared. High integration rates indicate that the intelligence is useful and actionable. CTI Platform Utilization: Utilization rate of at least 80%. Indicates how effectively the SOC is leveraging its CTI platform to enhance collaboration and overall situational awareness.
Participation in Cybersecurity Communities	Engagement in Industry Forums and Networks: Participation in at least three forums or conferences annually. Engagement in broader cybersecurity communities helps the SOC stay updated with the latest threats, share best practices, and foster partnerships with peers. Number of Reports Contributed to Cybersecurity Community: At least two reports per quarter. Sharing detailed incident analyses enhances collective defense and supports the wider cybersecurity community in understanding and preparing for similar threats.
Effectiveness of Information Sharing Initiatives	Time to Share Threat Intelligence: Less than 24 hours from discovery.

	Quick dissemination of validated IoCs allows partners to react faster, improving the overall security posture of the collaborative network. Collaboration Satisfaction Rate: At least 85% satisfaction. A high satisfaction rate indicates that external partners find the SOC's collaborative activities valuable, fostering long-term relationships and continued information exchange. Quality of Shared Information: At least 90% of shared intelligence is rated as actionable by partners. Ensures that the intelligence shared is not only informative but can be acted upon to prevent incidents or mitigate threats.
Use of Shared Data in Defensive Improvements	Implementation Rate of Shared Threat Data: 80% or higher. This KPI measures how effectively shared intelligence is being used to enhance SOC capabilities and proactively strengthen defenses. Cross-Institutional Research Projects: Minimum of two per year. Leveraging shared threat data in research contributes to academic advancement and practical improvements in cybersecurity measures.

Capacity and Training of SOC Personnel KPIs

Training and Skill Development

Training Completion Rate:

100% of the SOC personnel should complete all required training annually.

	Ensures that all staff members are up-to-date with the latest security practices, compliance requirements, and operational procedures. It also helps in minimizing human error and enhancing the SOC's capability to respond to incidents effectively. Average Training Hours per Analyst: 20 hours per quarter per analyst. Continuous learning is crucial in the rapidly evolving field of cybersecurity. Adequate training hours help analysts stay current with emerging threats and the latest security technologies. Certification Acquisition Rate: 80% or higher. Certifications indicate a recognized level of knowledge and competency. This helps ensure that the personnel have the qualifications necessary to meet industry standards. Specialized Skill Training (e.g., Threat Hunting, Incident Analysis): 50% of personnel should be cross-trained in at least one specialized skill. Cross-training enhances the SOC's ability to cover specialized tasks, improves response capabilities, and provides operational flexibility in case of resource shortages or shifts.
Personnel Capacity and Workload Management	Analyst Capacity Utilization Rate: 70-80% utilization. Ensures a balance between maintaining productivity and preventing analyst burnout. Effective workload management allows SOC analysts to handle incidents efficiently without compromising quality. Average Number of Incidents Handled per Analyst: Between 20-30 incidents per analyst, depending on incident complexity and severity. Provides insight into workload distribution and operational efficiency. Ensures that analysts are neither overwhelmed nor underutilized. Analyst Shift Coverage Adequacy:

	100% of shifts covered by qualified personnel. Ensures continuous monitoring and response capabilities, particularly in a 24/7 SOC environment where shift work is critical to security operations.
Competency Assessment and Skill Gaps	Competency Assessment Score: An average score of 85% or higher across the SOC team. Competency assessments identify individual and collective strengths and weaknesses, allowing for targeted skill development initiatives. Skill Gap Identification and Closure Rate: 90% or higher. Addressing skill gaps promptly ensures that the team maintains high competency levels, especially in areas of rapid technological change.
Certification and Credential Management	Percentage of Personnel with Critical Certifications: 100% of personnel should hold certifications aligned with their job roles. Demonstrates that each staff member has achieved recognized standards of knowledge and capability needed for their role. Certification Renewal Compliance: 100% compliance for all personnel holding time-sensitive certifications. Ensures that SOC personnel retain their certified status and keep abreast of changes in the cybersecurity landscape.
Employee Satisfaction and Retention	Analyst Job Satisfaction Rate: 85% satisfaction rate. Job satisfaction is closely linked to performance and retention rates. High satisfaction indicates a supportive work environment conducive to productivity and professional growth. Analyst Retention Rate:

	90% or higher retention. High retention rates indicate a positive work environment, which is crucial for maintaining continuity and operational knowledge within the SOC. Employee retention also reduces the time and cost involved in hiring and training new analysts. Onboarding Duration for New Analysts: Less than three months. Short onboarding time ensures that new hires quickly become productive, minimizing the impact of staffing changes on SOC operations.
Incident Response and Decision-Making Competency	Number of Simulation Exercises Conducted Annually: At least four simulation exercises per year. Ensures analysts are well-prepared for real incidents. Hands-on practice with real-world scenarios is critical to improving decision-making under pressure. Simulation Success Rate: 85% or higher. Measures the effectiveness of training in practical situations. A high success rate indicates a strong understanding of response procedures and readiness for real-world incidents.
Cross-Training and Role Flexibility	Cross-Trained Personnel Rate: 60% or higher. Cross-training enhances flexibility in staffing, allowing personnel to step into different roles when required, thus improving the SOC's resilience during high workload periods or staff shortages. Percentage of Personnel Participating in Threat Hunting: At least 30% of Level 2 and above personnel should actively engage in threat hunting. This ensures that the SOC personnel are involved in proactive security measures, rather than only responding to incidents. Threat hunting skills also

develop analysts' understanding of sophisticated attack techniques.

Effectiveness of Organizational Structure and Processes KPIs

Efficiency of Incident Management Processes

Incident Response Time per Escalation Level:

Average response time for each escalation level (Level 1 to Level 3).

Level 1: Within 5 minutes.

Level 2: Within 15 minutes of escalation.

Level 3: Within 30 minutes of escalation.

Ensures the SOC's structured approach to incident management is working efficiently, with swift escalations to the appropriate personnel for more in-depth analysis and response.

Incident Workflow Completion Rate:

100% of incidents should adhere to the workflow.

Adhering to a structured workflow ensures incidents are managed systematically, minimizing chances for oversight and reducing response variability.

Percentage of Incidents Resolved Within SLA:

95% of high-severity incidents resolved within the agreed SLA.

SLA adherence demonstrates the SOC's effectiveness in managing and mitigating incidents promptly, thereby reducing the potential impact on the organization.

Shift and Handover Processes

Shift Handover Quality Index:

At least 95% of handovers rated as satisfactory or higher.

Effective handovers are crucial for 24/7 SOC operations. High-quality handovers reduce the likelihood of gaps in monitoring and help ensure continuity of response.

Percentage of Missed or Incomplete Handover Tasks:

	0% missed handovers. Ensuring all tasks and ongoing incidents are fully handed over prevents any lapse in incident response or monitoring, thereby maintaining continuous security coverage.
SOC Structure and Team Coordination	Team Communication Effectiveness: Collaboration on at least 50% of complex incidents. Complex threats often require the combined expertise of multiple roles. Effective communication and collaboration help ensure that incidents are resolved comprehensively. Percentage of Successful Cross-Functional Collaboration: 100% successful collaboration for incidents that need cross-functional input. Ensures the SOC can effectively coordinate with other departments when necessary, particularly for incidents involving multiple domains, such as data breaches or system outages.
SOC Process Optimization	Automation Implementation Rate: Automate 70% of routine low-risk tasks. Automating repetitive tasks helps free up analysts to focus on higher-priority incidents and complex threat analysis, thereby increasing the overall SOC's efficiency. Time Saved Through Process Improvements: 20% reduction in the time required for repetitive processes. Measuring the time saved through process improvements helps determine the impact of optimization efforts, making the SOC more agile and effective in handling complex incidents. Incident Backlog Reduction Rate: 30% reduction in incident backlog over six months.

	Reducing incident backlog indicates that the SOC is keeping up with incident volumes and addressing past issues more efficiently.
Compliance with Incident Management Procedures	Percentage of Incidents Documented Thoroughly: 100% thorough documentation. Ensures transparency and accountability in incident response, aiding in audits, reviews, and post-incident learning processes. Post-Incident Review (PIR) Completion Rate: 100% for all major incidents. Post-incident reviews are critical for understanding the root cause, lessons learned, and identifying potential process improvements that can prevent recurrence. Rate of Lessons Learned Incorporated into Processes: 90% of lessons learned incorporated within three months. Ensures continuous improvement in SOC processes based on real-world experience and enhances the ability to respond to similar incidents in the future.
Workforce Productivity and Utilization	Analyst Productivity Rate: 10-20 incidents per analyst per shift, depending on incident complexity. Productivity is essential for ensuring that analysts efficiently handle alerts and incidents, balancing quantity with quality. Percentage of Overtime Worked: Less than 10%. A low overtime rate indicates effective staffing and resource allocation. Excessive overtime could indicate insufficient staffing or inefficiencies in processes, leading to analyst burnout. Absence and Replacement Coverage: 100% coverage.

	Ensures that the SOC remains fully operational despite staff absences, maintaining continuous threat monitoring and incident response capabilities.
Tools and Resources Utilization	SOC Tool Utilization Rate: 90% utilization of key SOC tools. Ensures that analysts are using available tools effectively to enhance incident detection, response capabilities, and automation. Ticketing System Efficiency: Average closure within 24 hours for routine tickets, depending on severity. A well-functioning ticketing system indicates that analysts can track and resolve incidents efficiently, which is critical for maintaining overall process effectiveness.

Threat Detection and Response Optimization KPIs

Threat Detection Efficiency	Mean Time to Detect (MTTD): Less than 5 minutes for critical incidents. A shorter MTTD minimizes the time a threat remains undetected, thereby limiting potential damage. Effective detection relies on well-calibrated monitoring tools and trained analysts who can quickly identify malicious activity. Detection Accuracy Rate: 90% true positive rate. High detection accuracy is crucial to reduce false positives, allowing analysts to focus on real threats rather than wasting time on benign alerts. Ensuring accuracy helps prevent alert fatigue among analysts. False Positive Rate: Less than 10%. A low false positive rate indicates effective tuning of the SOC's detection systems, ensuring that analyst
-----------------------------	--

	resources are spent on actual threats rather than false alarms. Threat Intelligence Utilization Rate: 80% of threats should be detected using threat intelligence. Shows how well the SOC leverages external intelligence to enhance detection capabilities, ensuring up-to-date knowledge of threat actors and tactics.
Incident Response Optimization	Mean Time to Respond (MTTR): Less than 10 minutes for high-priority incidents. A shorter MTTR ensures that response actions, such as containment and mitigation, are initiated swiftly, reducing the potential impact of incidents. Threat Containment Time: Contain high-severity threats within 30 minutes. Effective containment prevents the spread of threats within the network, minimizing the damage they can cause. Percentage of Incidents Mitigated at First Response: 75% of incidents mitigated at Level 1 or Level 2. Indicates the effectiveness of initial response actions taken by analysts and the quality of response processes in place. Threat Escalation Rate: 20-30% escalation rate. An optimal escalation rate means that the majority of incidents are handled by the appropriate level of the SOC, while complex or persistent threats are escalated to senior experts for more in-depth analysis.
Automation and Orchestration in Response	Automation Coverage Rate: 70% of routine, repetitive response tasks automated.

	Automation reduces the response time and human effort required for basic response actions, freeing up analysts to focus on complex and strategic aspects of incident handling. Reduction in Manual Effort for Threat Response: 50% reduction in manual effort compared to the previous year. Reducing manual effort enhances efficiency and helps avoid errors, leading to faster and more reliable incident response. SOAR Playbook Utilization Rate: 90% of repeatable incidents should follow established playbooks. Ensures consistent and efficient response actions, helping analysts apply best practices during common threat scenarios.
Proactive Threat Management	Threat Hunt Frequency: At least four threat hunts per quarter. Proactive threat hunting identifies threats that may have evaded traditional detection methods, improving the SOC's ability to find sophisticated or persistent threats before they cause significant damage. Threat Hunt Success Rate: 50% or higher. A high success rate indicates that threat hunting activities are effectively identifying undetected threats and improving the overall security posture. Number of Incidents Prevented Through Proactive Measures: Minimum of five significant incidents prevented per quarter. Shows how proactive measures are reducing the number of successful attacks, demonstrating the importance of proactive threat management in the SOC.

Learning and Continuous Improvement	Root Cause Analysis Completion Rate: 90% or higher. Root cause analysis helps identify weaknesses in the SOC's detection and response mechanisms, allowing the organization to improve its security posture and reduce repeat incidents. Lessons Learned Implementation Rate: 85% of lessons learned implemented within three months. Ensures that the SOC continually evolves and adapts its detection and response capabilities based on real-world experiences. Percentage of Threat Intelligence Incorporated into Defense Mechanisms: 80% or higher. Demonstrates that the SOC effectively utilizes intelligence from various sources to enhance its detection capabilities and adapt to new threats.
Incident Analysis and Reporting	Time to Complete Incident Analysis: Within 48 hours of incident resolution for detailed analysis. Timely analysis helps in understanding the attack pattern, identifying the threat actor's behavior, and improving future defenses. Comprehensive Incident Report Completion Rate: 100% for high-severity incidents. Ensures that each incident is well-documented, providing valuable insights that can be used to prevent similar incidents in the future and assist in regulatory compliance.
Threat Visibility and Scope	Percentage of Network Visibility: 100% of critical network segments covered. Ensures that the SOC has comprehensive visibility across the organization's infrastructure, which is

essential for detecting and responding to threats in a timely manner.

Threat Scope Reduction Rate:

25% reduction in impacted scope per year.

Reducing the impact of incidents over time indicates that detection and response mechanisms are improving, effectively containing threats before they spread.

References

- [1] Narges Yousefnezhad, Avleen Malhi, Kary Främling, Security in product lifecycle of IoT devices: A survey, Journal of Network and Computer Applications, Volume 171, 2020, 102779, ISSN 1084-8045, <https://doi.org/10.1016/j.jnca.2020.102779>, <https://www.sciencedirect.com/science/article/pii/S1084804520302538>
- [2] <https://www.helsinki.fi/en/center-information-technology/it-security-university>
- European Cybersecurity Skills Framework, ENISA, September 2022.
- [3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
- [4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- [5] <https://www.first.org/tlp/>
- [6] Adam Zibak, Clemens Sauerwein, and Andrew C. Simpson. 2022. Threat Intelligence Quality Dimensions for Research and Practice. Digit. Threat. Res. Pract. 3, 4, Article 44 (December 2022), 22 pages. <https://doi.org/10.1145/3484202>
- [7] H. Chen, J. Chen and J. Ding, "Data Evaluation and Enhancement for Quality Improvement of Machine Learning," in IEEE Transactions on Reliability, vol. 70, no. 2, pp. 831-847, June 2021, doi: 10.1109/TR.2021.3070863
- [Fig. 1-3] K. Knerler, I. Parker, C. Zimmerman "11 Strategies of a World-Class Cybersecurity Operations Center". MITRE, 2022.

4. SOC technical architectures

For a Security Operations Center to function efficiently and effectively, certain technical capabilities must be in place – both within the security team and across the organization. When designing a SOC, several factors must be considered, including the selection of tools (which depends on the planned services), their placement within the organization, and their integration and data exchange mechanisms.

For example, most SOC teams require a SIEM system or a SIEM-like solution to perform routine analysis. Deploying a SIEM involves multiple considerations, such as defining its architecture, determining organizational coverage, ensuring availability, and selecting the appropriate tool.

This chapter outlines the requirements, architectures, and solutions necessary for the technical implementation of SOC services. Key topics include event logging, network configurations, scanning challenges, and the tools required to build technical capabilities for a SOC.

4.1. Architectural considerations for building a SOC

Building a SOC team within an organization is a complex task. One of the key questions to address is the availability of human and technical resources. The answer determines the choice of the operational model for the SOC. The two main models are Centralized SOC and Distributed SOC.

They differ not only in their organizational structure but also in the technical resources they require.

From a technical perspective, the key resources needed to build a SOC are the servers on which the SOC tools will run. From an organizational standpoint, personnel are required in both models, although the number of staff varies.

Organizational perspective of a Centralized SOC:

Advantages:

- Better collaboration
- Stronger SOC authority
- Opportunities for staff growth

Disadvantages:

- High cost of maintaining the team
- Frequent staff turnover, which requires continuous training

Staff:

- SOC manager
- SOC level 1 and level 2 / non-level SOC engineer (security analyst) – real-time alert monitoring, incident reporting, malware analysis

- SOC level 3 / SOC senior (security engineer / architect) – CTI, threat hunting, system administration (alternatively: SOC level 3 = threat hunting; SOC level 4 = CTI + system administration)
- Forensic engineer
- Awareness and training specialist

Resources needed:

- Dedicated office space (rooms)
- Servers
- TVs
- Office accessories (whiteboards, printers etc.)

Organizational perspective of a Distributed SOC:

A Distributed SOC can be understood in two ways – firstly, as a SOC team operating in each branch of the company, or secondly, as handing over SOC-related tasks to an external company. In the former case, human resources are duplicated per branch. In the latter case, human resources are reduced to a minimum.

Advantages:

- Reduced costs – no need to maintain or train an internal team
- Access to a highly qualified external team

Disadvantages:

- If using an external SOC, reduced agility

Staff:

- Security engineer – acts as a point of contact between the SOC and the organization

Technical perspective of a Centralized SOC:

Advantages:

- Dedicated resources – eliminates the risk that the server hosting SOC tools becomes inefficient due to the load from other tasks

Disadvantages:

- High cost of maintaining hardware resources

Technical perspective of a Distributed SOC:

Advantages:

- Resources are shareable – can be utilized for other tasks when the SOC has less work
- More flexibility
- Lower costs

Disadvantages:

- Risk of performance degradation if the infrastructure becomes overloaded

Multi-tenancy

When building your own SOC, especially if the goal is to provide services to multiple organizations, consider operating the SOC in a multi-tenancy mode.

In this mode, which is commonly implemented in systems that support SOC operations, work areas are separated. Essentially, a dedicated workspace is created for each organization, within which SOC analysts perform their tasks. Additionally, the model can be extended to teams, with a separate team assigned to each organization within the SOC. This approach helps ensure confidentiality, as data from one organization remains isolated from that of others. One of the key benefits of this model is reducing the risk of missing important events. If a single SOC team is responsible for multiple organizations and operates within a shared workspace, there is a chance that one organization's events could be overlooked in the noise generated by another organization. By creating separate work areas (and teams, if necessary), this risk is minimized. With dedicated teams focusing only on one organization, the likelihood of missing an event is nearly eliminated.

Separating workspaces is the lowest level of data separation in systems supporting SOC operations. Other options for data isolation include using dedicated disks for storing data from a specific organization, entire dedicated virtual environments, or dedicated physical servers. The choice of the appropriate level of separation largely depends on the confidence of the SOC team.

SOC availability

Availability is a critical aspect of a SOC, as it usually needs to operate 24/7 to effectively monitor, detect, and respond to threats in real time. Ensuring high availability (HA) in SOC operations involves addressing technical, process, and infrastructure requirements to minimize downtime and maintain continuous security coverage.

There are at least three key areas that influence considerations for high-availability operations in a SOC:

1. Threat monitoring in real time – Threats can occur at any time, and downtime in the SOC increases the risk of undetected breaches.
2. Incident response – Some incidents, such as data loss or reputational harm, require an immediate response.
3. Compliance and reporting – Various regulations require prompt reporting of detected incidents and threats.

When discussing the technical aspects of availability, the following topics must be considered:

1. Redundancy of infrastructure.

The SOC needs to rely on systems with appropriate failovers, both in terms of hardware and software. Depending on the scale and available funds, this can range from simple backups to a warm secondary system. This also involves communication redundancy, as the SOC team must maintain communication with each other and with third parties, even when normal channels are unavailable.

2. Network resilience.

The availability of the network is a critical focus. SIEM, XDR, and other systems depend on network availability in order to function properly.

3. Scalability.

Unpredictable data volume spikes, often related to incidents like DDoS attacks, will occur. The ability to dynamically scale resources and provide load balancing for services is essential.

4. Disaster recovery.

Given its critical nature, the SOC should have a well-tested disaster recovery plan and good backup implementation.

5. Uptime SLAs.

If the SOC relies on external vendors, appropriate SLAs should be negotiated, particularly for those services that are critical to operations.

4.2. Logging architecture

Logging architectures form the backbone of a Security Operations Center (SOC), enabling the collection, aggregation, analysis, and storage of data critical to threat detection, incident response, and forensic investigations. A robust logging architecture ensures that all relevant security events are captured, correlated, and retained in a way that supports both real-time operations and long-term compliance.

Cybersecurity logging in public universities differs from the commercial environment, making it difficult to directly adopt the processes and software used in that context. Universities usually have a looser structure, covering a range of operational and research environments with varying levels of autonomy. Their cybersecurity policies grant IT resource users more freedom, and policy enforcement tends to be less strict. Moreover, this environment only emphasizes the need for an efficient logging infrastructure to achieve an adequate level of cybersecurity.

Key components of logging

1. Log Sources

- Endpoints: Workstations, servers, and mobile devices.
- Network Devices: Routers, firewalls, intrusion detection/prevention systems (IDS/IPS), and switches.
- Applications: Web servers, databases, and custom applications.
- Cloud Environments: Logs from AWS, Azure, Google Cloud, and SaaS platforms.
- Threat Intelligence Feeds: External sources providing IoCs and other contextual data.
- Operating Systems: System-level logs from Windows Event Logs, Linux syslogs, etc.

2. Log Collection and Aggregation

- Agents: Lightweight agents installed on endpoints or servers to collect and forward logs (e.g. Fluentd, Logstash).

- Remote Logging Protocols: Syslog, SNMP, and proprietary APIs used to collect logs from devices and applications.
- Data Pipelines: Middleware that processes and normalizes logs before forwarding them to storage or analysis systems.

3. Centralized Logging Platform

- SIEM (Security Information and Event Management): Platforms such as Splunk, LogRhythm, or Elastic Security that aggregate and analyze logs in real time.
- Data Lakes: Centralized repositories for storing large volumes of raw and processed log data for long-term analysis (e.g. Amazon S3, Hadoop).
- Message Queues: Technologies like Kafka or RabbitMQ used to handle large-scale log ingestion without performance degradation.

4. Analysis and Correlation

- Pattern Matching: Detection rules used to identify known threats.
- Anomaly Detection: Behavioral analysis techniques that detect deviations from normal activity.
- Threat Intelligence Integration: Enrichment of logs with contextual data from external feeds.

5. Storage and Retention

- Hot Storage: High-performance storage for recent logs used in active monitoring and investigations.
- Cold Storage: Cost-efficient solutions for long-term archival storage (e.g. cloud-based object storage).
- Retention Policies: Guidelines that define log storage duration based on compliance requirements and organizational needs.

Logging use cases

The use cases for log collection and analysis define entire processing pipelines. These pipelines consist of a set of producers, event parsing and transformation rules, and a set of consumers. Producers determine the sources from which events are collected. Parsing rules extract important information from the events while filtering out irrelevant data, and transformation rules convert events into a standardized, machine-processable format. Finally, consumers determine the methods of accessing the logs and which tools are available for analysis.

The motivation for cybersecurity log analysis varies across organizations, making it difficult to generalize. The following is a brief overview of use cases relevant to any entity operating IT services; however, this list is by no means exhaustive.

- **Auditing** – validates that resources are configured in compliance with cybersecurity policies
- **Denial of Service (DoS)** – detects attacks that flood a target with excessive requests, leading to overload and denial of service for legitimate users
- **Intrusion Detection** – identifies unauthorized access to IT resources
- **Malicious Behavior** – detects user activities that violate cybersecurity policies
- **Phishing** – identifies social engineering attempts to trick users into revealing sensitive information or installing malware

- **Scanning** – detects information gathering attacks that may precede more targeted intrusion attempts

Sample logging architecture

The sample logging architecture described in this section is based on the system currently being developed at Masaryk University. Some components are already in production, others are under implementation, and some remain in the planning stage. Figure 1 illustrates the logging architecture, which consists of the following components:

1. **Log producers** – end stations where original log records are created. These are configured to send logs either to a relay or directly to the central point. Common log producers include:
 - a. User stations and servers
 - b. Services
 - c. Network infrastructure
2. **Log relays** – a potential multiple-tier hierarchy of relay servers that collect logs from producers and forward them further into the infrastructure.
3. **Central point** – the main server responsible event parsing, normalization, and forwarding logs to consumers.
4. **Log consumers** – tools used for short- or long-term storage and manual or automated analysis. Common log consumers include:
 - a. Analytical tools – allow users to quickly browse data and run queries.
 - b. Persistent storage – stores log records in large volumes for a defined period of time.
 - c. Security Operations Center (SOC) – provides continuous monitoring, running queries, and analyzing past incidents.
 - d. Correlation and detection tools – perform correlation and detection methods on predefined logs, generating complex security events (alerts).

In this document, Events Per Second (EPS) metrics measured in the network represent the average EPS recorded during working hours on a single day.

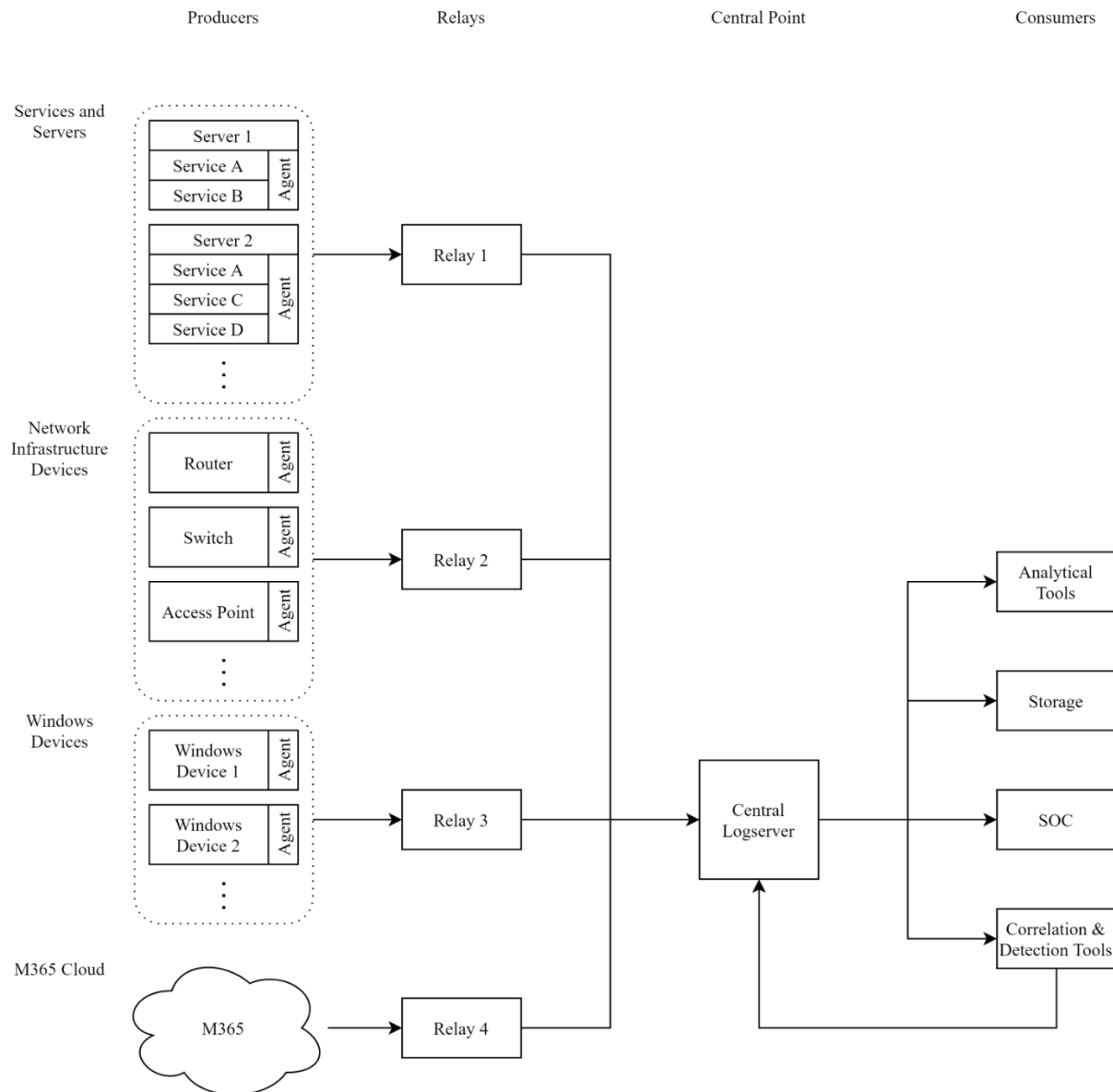


Figure 1 Architecture of the centralized logging infrastructure being developed at MUNI

Considering the use cases described earlier, log groups containing cybersecurity-related information that should be monitored have been identified:

- User station logs (Intrusion Detection, Auditing, Malicious Behaviour)
 - Windows
 - Linux
 - Mac OS X
- Server logs (Intrusion Detection, Auditing)
 - Linux operational logs (e.g. syslog, authlog)
 - MS Windows Server logs
- Service logs (Intrusion Detection, Phishing, Scanning, DoS)
 - Network - Radius, DHCP, VPN, DNS, email
 - Security - Firewall, IDS/IPS, EDR

- Domain - Active Directory
- WWW - Microsoft IIS
- Kubernetes
- Any other application providing a service
- External cloud logs (e.g. M365) (Intrusion Detection, Auditing)
 - Auth log
 - Audit log
 - E-mail log
- Network infrastructure logs (Intrusion Detection)
 - Access points
 - Switches
 - Routers

Producers

User stations

- A user station is any device directly managed by the organization and accessed by employees, students, or visitors.
- Logging options vary based on the OS; devices within the same OS group should use identical logging configurations:
 - Linux (Filebeat)
 - MS Windows (Winlogbeat)
 - MacOS
- In the MUNI infrastructure, there are currently around 2,500 Windows devices producing approximately 800 events per second (EPS).

Services and servers

- Key services and their threats are identified.
- Based on this, the scope of logging is set to cover all key services and features relevant to the identified threats.
- A service may be (and usually is, for redundancy) run by more than one server, and a server may run more than one service. Therefore, it is useful to abstract service logging from server logging and develop them separately (e.g. process mail service logs – sending and forwarding messages, separately from mail server logs – accesses, updates, etc.)
- In the MUNI infrastructure, OS logs are collected from the following server groups:
 - Windows: ~ 50 servers, ~ 700 EPS
 - Linux: ~ 30 servers, ~ 900 EPS
- And from the following services (only major services listed):
 - DNS: ~ 2 servers, ~ 2000 EPS
 - E-mail services: ~ 4 servers, ~ 16 EPS

- Web services: ~ 8 servers, ~ 10 EPS
- M365 cloud – logins, e-mail, SharePoint, etc.: ~ 20 EPS
- Fragmentation of services across different server groups/providers is an issue. For example, the e-mail service is provided by both local Linux servers and relays, as well as by the M365 cloud infrastructure.

Agents

- Agents are specialized SW deployed and configured on producers to collect logs and forward them further to the logging infrastructure.
- Agents are heterogeneous – different agents are suited for different purposes and use varying standards. Some are integrated within the OS, while others are installed separately.
- Configuration management is a challenge. In large, fragmented infrastructures, it is difficult to track the configuration of every device. A configuration database or **Git-based configuration repository** is recommended.
- In the MUNI infrastructure, the primary agents used are Winlogbeat, Filebeat, Syslog, Vector, and Rsyslog.

Relays

Relays are additional infrastructure components with the following functions:

- Aggregate connections – alleviate the load on the central log server
- Create groups with the same configuration – for example, grouping all Linux workstations or all Windows workstations. Relays should only forward logs and avoid fragmenting configurations (no parsing or normalization on relays)

Currently, the number of connected devices at MUNI does not require relays. However, they may be used in the future for large groups of similar devices, such as Windows workstations or network infrastructure devices. The proposed relay SW is Vector.dev¹.

Central log server

The central log server is a single point responsible for parsing, normalization, and forwarding logs to consumers. As a single point of failure in the infrastructure, it must have sufficient performance to handle the predicted load of events per second, and a backup should be available.

Monitoring of the server is essential, at least to answer the following questions:

- Is the server running?
- Are events being received at the expected rate?

At MUNI, Vector is used to handle ingestion, transformation, and forwarding. The server accepts connections from authorized log sources and processes them according to predefined pipelines (e.g. mail events -> mail parsing -> mail normalization -> consumer subset).

Grafana is used to monitor the health of the server, the number of events processed, and any instances of dropped events across separate pipelines. The following metrics are monitored:

- Lag time – the time delta between *event created* and *event reported* (~ seconds – hours)
- Errors – the number and type of errors generated on the log server, such as parsing and writing errors
- Drops – the event drop rate per pipeline
- Input/output rate – the number of events per source/sink

The total EPS input to the log server is approximately **10,000 EPS**.

Consumers

Analytical tools

- At MUNI, OpenSearch is used for general data analysis, though any ELK-like software would suffice.
- OpenSearch includes ELK Enterprise functions developed as open source, but as a side effect, it contains bugs that can take time to fix. One current issue is a faulty OIDC integration (which has already been resolved).
- The Discovery function and CLI enable search, filtering, and aggregation.
- Visualizations, grouped in dashboards, are used for common day-to-day tasks by cybersecurity incident handlers, service providers, and OpenSearch administrators. An example dashboard is shown in Figure 2.

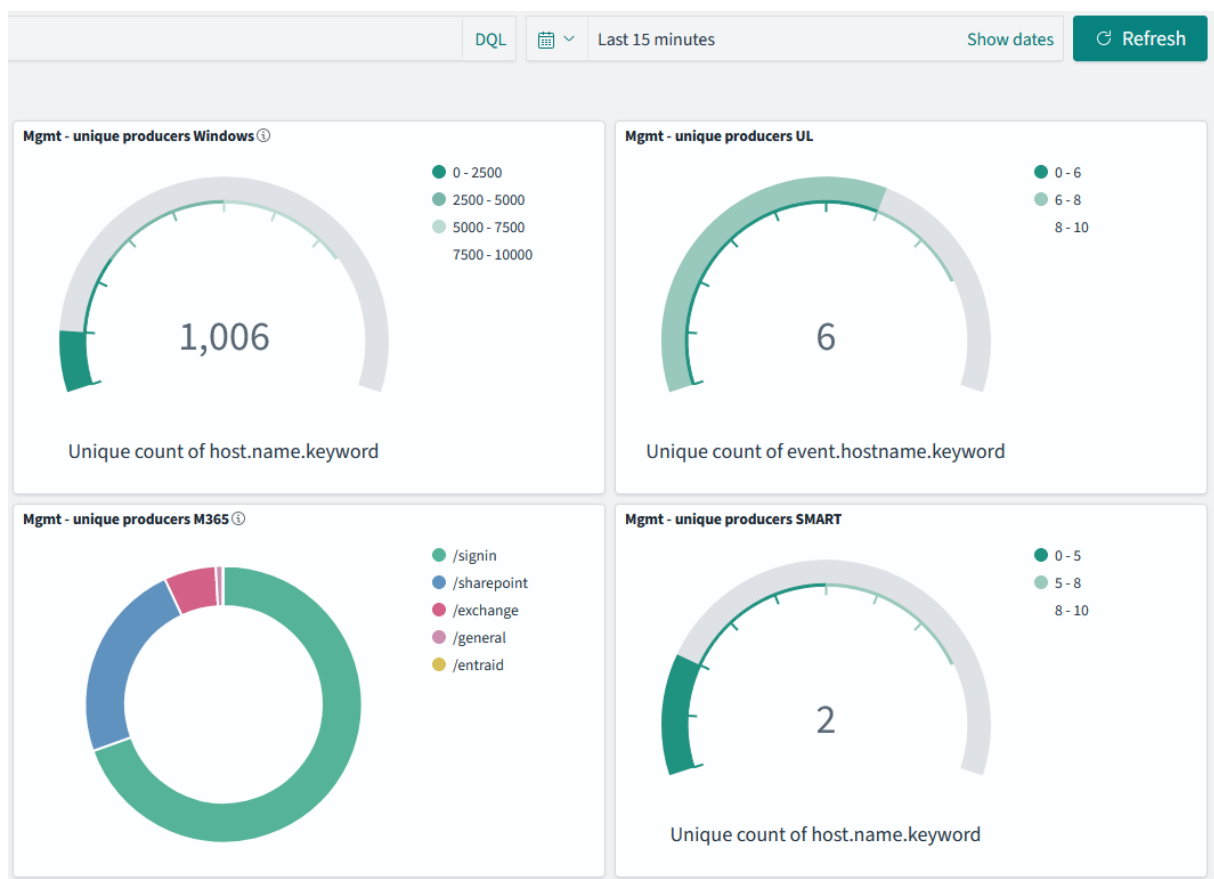


Figure 2 An OpenSearch dashboard displaying the number of unique event producers across four separate pipelines (Windows devices, Unified login, M365 cloud, and SMART proxy service) within the selected time frame.

Storage

Storage is logically and physically divided into two tiers. The basic level is Tier 0 (Raw), which stores data in its original form, e.g. data sent by syslog. It is advisable to retain data in Tier 0 throughout the retention period, due to the potential need for recalculations in subsequent dashes (for example, due to an error). Tier 1 (Curated), stores data that has undergone parsing at the Vector level. This process involves dividing event messages into new fields, which vary for each collected service. Additional levels will be created as needed in the future, which can be an archive tier for storing aggregated statistics, an experimental tier for testing purposes, etc.

Data retention

Since service and asset logs contain personal data, such as IP addresses, data management and processing must comply with applicable legislation. The data retention period is limited and should be kept to a minimum; however, this is often against the preference of service administrators, who seek longer retention periods for greater convenience in handling potential incidents. For each use case, it is necessary to discuss the retention period with the data manager (source) and remain within the legislative framework. Data is deleted once the retention period has expired.

For selected categories of log records, the retention period is set at up to six months.

The data lake was built in compliance with applicable legal and internal regulations, with particular consideration for GDPR requirements. Compliance analysis is an ongoing process – an area that requires active management even after the project's completion.

- Long-retention data storage (Tier 0):
 - S3 (MinIO) serves as a separate log storage containing raw events that have not been processed by Vector.dev. The events remain in the format in which they were sent by the agents.
 - The separate storage serves as an archive with a long data retention period (180 days).
 - Raw data is stored in the “logs-raw” bucket, following a predefined layout. For object segmentation within the bucket, the object prefix includes user group and date information. The full address of an object may look like this:


```
s3://logs-raw/year=2023/month=05/day=25/hour=12/ics.diti.css.windows-xxxxxxxxx.zst
```
 - ~500GB of compressed JSON-encoded data is stored per month (compressed using Zstandard)
- Short-retention data storage (Tier 1):
 - Implemented using the OpenSearch system, which stores data in a processed format (indexes) with a short retention period (~1-2 weeks).

SOC

A basic SOC role can be provided by OpenSearch, as it can be configured to support SOC functions, such as data visualization and querying. At MUNI, OpenSearch has been configured with specialized dashboards to display relevant data to incident handlers and service administrators, with details available on demand via querying.

Incident handlers have access to all cybersecurity-relevant logs and can define and implement their own visualizations. This enables near real-time visualization of anomalies as well as an ex-post forensic analysis for incident investigations. Service administrators can access logs relevant to their services for security and performance monitoring. Additionally, management can review any dashboards used by teams they oversee.

The advantages of using OpenSearch as a SOC solution include its open-source nature and the lack of a need for a dedicated SOC system. The main disadvantages identified are that OpenSearch is not designed for a SOC, so it lacks automation for common tasks like generating management overview functions. Furthermore, any specialized function, visualization, and query must be implemented and managed manually.

Correlation and detection tools

A correlation and detection engine using both logs and network flows is currently being developed. The prototype is based on Wazuh, configured to utilize the OpenSearch indexed data. The alerts generated by this engine are re-entered into the logging infrastructure and are further processed in separate pipelines.

Log architecture monitoring

- Grafana for Vector and the underlying infrastructure (Kubernetes cluster)

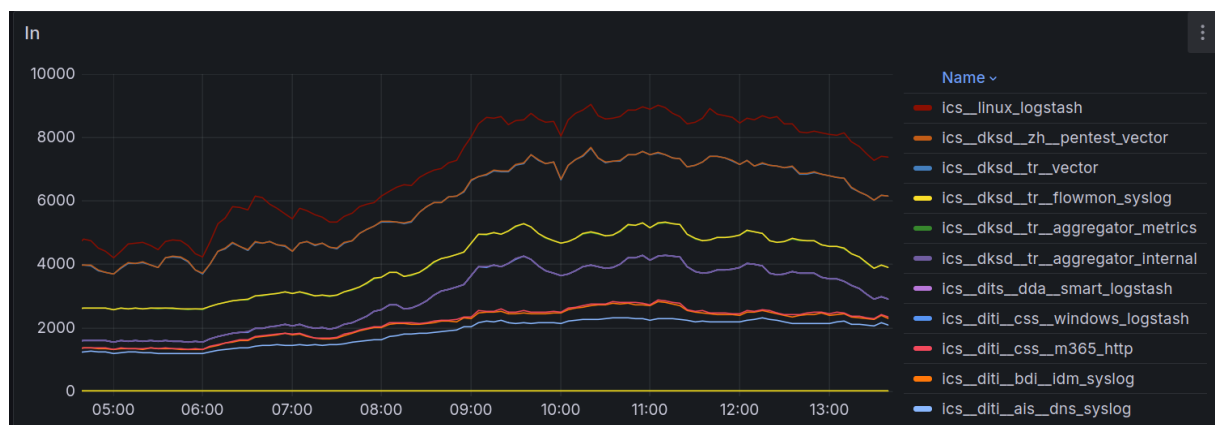


Figure 3 A Grafana dashboard visualizing the input rate of received events per aggregator source

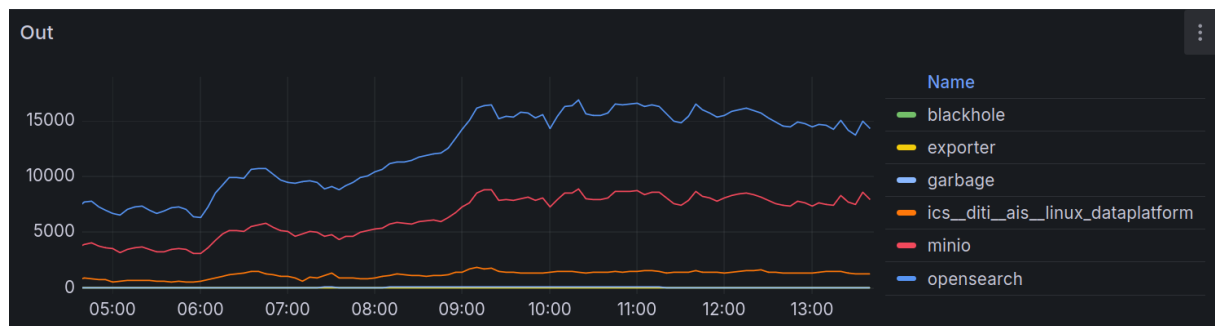


Figure 4 A Grafana dashboard visualizing the output rate of processed events per Vector sink

OpenSearch reference configuration

This section outlines the technical aspects of a reference OpenSearch configuration. The configuration can be significantly scaled down and will still fulfil its role for smaller data loads.

- The OpenSearch cluster consists of 8 instances, evenly distributed across a Kubernetes cluster with 4 physical nodes. Each instance is configured with a resource limit of 16 CPU cores and 64 GB of memory. The CPUs used on the nodes are Intel Xeon Silver 4310.
- Storage is dynamically allocated using a StorageClass provided by the local-path-provisioner. The underlying storage consists of two 14TB Samsung PM9A3 NVMe drives, which are joined using LVM in stripe mode.
- The four Kubernetes cluster nodes are connected via a 100GBE L2 switch. External clients, such as the log aggregator, can connect via a separate 10G interface.
- Rack hints ensure that index replicas are spread across at least three of the four physical nodes. Additionally, Kubernetes podAntiAffinity is used to schedule exactly two instances on each node.
- The OpenSearch API is published through a Kubernetes service with the ExternalIPs attribute configured to the IP addresses of the four Kubernetes nodes. A round-robin DNS record is used to evenly distribute client requests across all nodes.
- Users can access OpenSearch either via the aforementioned API or through the OpenSearch dashboard. End-user authentication is performed using OIDC, with each client department assigned a separate role that grants access only to its own log data.

4.3. Networking configuration and placement of sensors

The effective operation of a Security Operation Center (SOC) depends largely on proper network configuration and the strategic placement of sensors. Correct sensor placement ensures effective monitoring and rapid response to threats. This enables the detection of suspicious activity both in traffic leaving and entering the organization. Proper network configuration facilitates the isolation of critical resources, minimizing the risk of lateral movement by threats. Adequate tuning of these elements reduces informational noise and allows for a faster detection of anomalies. Best practices and key aspects in this regard are outlined below. A detailed analysis of the selected tools listed can be found in Chapter 6: Software/Hardware Solutions Review.

Networking configuration

Proper network configuration should ensure adequate segmentation, access control, and visibility of network traffic. This enables SOC teams to monitor and detect threats in real time. A properly-designed network, including redundancy and encryption, minimizes the risk of failure and ensures secure data transmission. Below are the most important principles:

- Segmentation and zoning

Networks should be logically divided into different zones based on function and the level of data sensitivity. For example, public zones can support websites, internal zones can support business applications, and restricted zones can support critical systems such as university databases. VLANs should be implemented to separate traffic between

different zones and, if logical, within the zones themselves. For instance, it is advisable to place VoIP devices in a separate VLAN, as they only communicate with the local call server and printers. Boundaries between zones should be further secured with firewalls that can monitor and control data flow. Limiting the number of contact points between zones reduces the risk of unauthorized access or threat propagation.

- Redundancy and reliability

Networks should be designed with redundancy, involving the duplication of components such as servers, routers, and switches. Redundant links should provide alternate routes for data transfer. Failover mechanisms should be regularly tested to ensure seamless switching to alternative components in the event of a failure, thus ensuring business continuity. Testing redundancy mechanisms is essential for detecting potential weaknesses and preparing the network for emergencies. Load balancing should be an integral part of the network design, enabling network traffic to be distributed among multiple components. This solution not only improves reliability but also enhances infrastructure performance. The SOC should have a backup, dedicated internet connectivity using alternative technologies (such as 5G). In the event of a DoS attack or power outage, redundant links of regular connectivity may be down, but the SOC must still be able to interact with peers and authorities to manage the incident.

- Access control

Firewalls and ACLs control access by determining which devices or users have access to specific resources. Restrictions should be configured based on the principle of least privilege. Every connection to sensitive segments should be authenticated using appropriate mechanisms, such as digital certificates, two-factor authentication (2FA), or tokens. All access attempts should be logged to monitor potential incidents and unauthorized access attempts. Logs should include information such as source IP address, time, user, and the type of access requested to facilitate later analysis.

- Visibility and monitoring

Implementing Intrusion Detection and Prevention Systems (IDP/IPS) enables real-time monitoring of network traffic. IDS/IPS systems analyse traffic and can proactively block identified threats. Tools such as SIEM, acting as traffic flow analysers, integrate data from various devices and systems, enabling the detection of anomalies and potential attacks across the organization. Regular monitoring of ports and endpoint devices includes systematic scanning of open ports and observation of activity associated with their use. These activities help detect unauthorized access and attempts to exploit potential security vulnerabilities. The implementation of Endpoint Detection and Response (EDR) tools allows for the identification of unusual activities on workstations and servers, such as the installation of malware or attempts to escalate privileges.

- Regular updates and patching

All network devices (such as routers and switches) should be updated regularly to eliminate known vulnerabilities. Updates should be deployed in a controlled manner, starting with a test environment, to minimize the risk of network disruption. Monitoring systems should be configured to automatically notify when security updates are available. In the event that deployment of updates is not possible, countermeasures such as additional firewall rules should be applied to reduce the risk of vulnerability exploitation.

- Encryption and secure communication

Connections used to transfer data between systems should be encrypted using protocols like TLS (Transport Layer Security) or VPN (Virtual Private Network). This is especially important in public or untrusted environments. All keys used to establish encrypted connections should be properly stored and managed to prevent unauthorized access and ensure protection against loss. Only proven and up-to-date encryption algorithms should be used to ensure resistance to modern methods of attack.

- Scalability and modularity

The network should be designed with future expandability and the implementation of new technologies in mind. Compatibility with the latest standards will allow it to adapt to future needs. Dividing the network into modules enables partial upgrades or repairs without interrupting the operation of the entire system. When designing the network, it is worth considering spare capacity in terms of connections, ports, or transmission bandwidth to meet future needs without having to rebuild the infrastructure.

- Logging and audit trails

Network devices should be configured to generate comprehensive logs, which should then be collected and stored in a central system. This approach enables easy analysis, event correlation, and long-term data storage, facilitating anomaly detection and supporting security management. The log data should capture the full path of events, which is crucial for incident analysis. With detailed logs, it is possible to determine when, where, and how a particular network incident occurred. Logs must be protected against tampering. Systems storing logs should ensure compliance with legal requirements for data storage.

Types of sensors

A Security Operations Center (SOC) should utilize a wide range of sensors to monitor, detect, and respond to threats in IT systems. These sensors can be physical devices, software, or a combination of both, providing comprehensive protection for IT infrastructure. The key types of sensors used in a SOC include:

- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are systems focused on monitoring network traffic to detect potential threats. IDS operates in passive mode, analyzing traffic and generating alerts when suspicious activity is detected. In contrast, IPS operates in active mode, blocking identified threats in real time. Both IDS and IPS rely on signature databases of known attacks, as well as heuristic techniques, to identify new types of threats.
- Security Information and Event Management (SIEM) is a key component of a SOC, aggregating logs and telemetry data from multiple sources, such as firewalls, servers, applications, and network devices. SIEM sensors enable real-time analysis of collected data to detect anomalies, irregularities, and potential threats. By applying correlation rules, they can identify complex attacks, such as lateral movement or privilege escalation across the network. SIEM systems often integrate with complementary tools like IDS/IPS and EDR to provide more comprehensive threat detection, enhancing their effectiveness.
- NetFlow/IPFIX sensors analyze network flows by collecting metadata about network traffic, such as source and destination IP addresses, ports, protocols, and the amount of data transmitted. While they do not capture packet content, they

enable efficient monitoring of traffic patterns. NetFlow analysis enables the detection of anomalies such as unexpected data transfers or network scanning, making these sensors useful for managing network performance and identifying potential threats. The data stored at the collector serves as a source of truth about the state of network traffic during an attack.

- Endpoint Detection and Response (EDR) are advanced sensors that monitor activity on workstations, servers, and other endpoints. By capturing data on processes, files, network connections, and user interactions, EDR enables the detection of abnormal behavior. These sensors provide threat-hunting and response functions, such as isolating infected devices and removing malware. Advanced EDR systems often integrate with XDR platforms, enabling comprehensive threat management across the entire IT environment.
- Network Detection and Response (NDR) specializes in analyzing network traffic for threats, focusing on detecting anomalies and suspicious activity in network communications. NDR can detect attackers' activities at various stages, such as network exploration or data exfiltration. These sensors are crucial in environments where many devices, such as IoT or OT, do not support traditional EDR agents. When used alongside SIEM and EDR, NDR enhances the organization's ability to respond to threats, and provides a more comprehensive view of its security standing.
- Data Loss Prevention (DLP) systems are data leak protection solutions that monitor and control the flow of information within an organization. DLP sensors analyze data at different levels – within network traffic, on end devices, and in the cloud. They detect attempts to transmit sensitive information externally, such as personal data, financial documents, or trade secrets. They can operate in passive (monitoring) or active (blocking transfers) mode. An important element of DLP is integration with security policies and the classification of sensitive data.
- Honeypots are specially designed systems or servers that simulate attractive targets for potential attackers. Their primary purpose is to lure cybercriminals, enabling the analysis of their activities and the detection of new attack techniques. Honeypot sensors provide valuable insights into the tools and methods used by attackers, helping to develop more effective defence mechanisms. They typically operate in an isolated environment to minimize the risk of threats spreading across an organization's network.

Placement of sensors

The deployment of sensors within a network is crucial for effective monitoring and protection of IT infrastructure. Proper placement ensures the detection of suspicious activity both at network boundaries and within internal segments, allowing for a swift response to threats. Well-configured and strategically positioned sensors minimize the risk of data loss while providing full visibility into network traffic – an essential foundation for effective SOC operations. Below are the key principles:

- Strategic placement

Sensors should be positioned at critical points within the network infrastructure. For instance, placing sensors at network boundaries, such as firewalls, ensures the monitoring of both incoming and outgoing traffic for abnormal behavior. It is equally important to place sensors within internal network segments that support critical systems and data, such as application servers or databases. This approach enables

comprehensive monitoring and early threat detection in the most sensitive areas of the infrastructure. Sensor placement should be balanced to avoid creating “dead zones”, where monitoring might be ineffective. Regular reviews of sensor placement are recommended as part of ongoing threat assessments and infrastructure changes.

- Monitoring inter-segment traffic

Sensors should capture traffic between different network segments to detect suspicious activity, such as abnormal connections or unusually large data transfers. Placing sensors at points of contact between segments enables detailed tracking of data flow and the identification of potential attack vectors.

- Comprehensive traffic visibility

Achieving full visibility of network traffic requires proper configuration of monitoring ports, such as SPAN (Switched Port Analyzer) or TAP (Test Access Points). It is equally important to prevent overloads that could lead to data loss. Sensors should capture traffic in real time, enabling in-depth analysis of events, trend monitoring, and identifying threats that may not trigger immediate alarms or be visible in real time.

- Flexibility and scalability

Sensor deployment strategies must be designed with future network infrastructure needs in mind. Sensors should be easily expandable as the number of devices increases or new technologies emerge. This approach enables the organization to adapt to evolving threats and requirements. It is advisable to choose sensors that support open standards and can integrate with a variety of network management platforms.

- Avoiding single points of failure

To ensure uninterrupted monitoring, sensors should not become a single point of failure in the monitoring system. Redundancy, both in hardware and logic, must be implemented, along with backup monitoring routes to guarantee system continuity. This will ensure continuous operations, even during maintenance or unexpected outages. Additionally, consider implementing a distributed architecture to minimize the risk of failure at any single point.

- Securing sensors

Securing the sensors themselves is just as important as securing the data they monitor. Physical and logical protection of sensors is crucial to maintaining their integrity and reliability. They should be placed in restricted access locations, and the data transmitted by sensors must be encrypted using robust algorithms to protect against tampering and unauthorized access. Regular security testing is necessary to ensure the sensors remain resilient to emerging threats.

4.4. Scanning, asset management, vulnerability management

This section outlines key considerations that should be integrated into the design of scanning, asset management, and vulnerability management architecture. These considerations should be further evaluated and refined to form a comprehensive guide for the SOC Toolbox technical architecture.

The examples presented in the following sections are based on the experiences from the Masaryk University environment. The foundation of asset discovery and vulnerability scanning is built upon a physical server with a strong network connection, complemented by several small, purpose-built cloud scanners.

Scanning

Scanning involves using automated tools to identify vulnerabilities, misconfigurations, and other weaknesses in systems, applications, and networks. It enables SOC teams to maintain visibility into the organization's security posture and identify potential attack vectors before they can be exploited.

Periodic network scans serve two key objectives:

1. **Vulnerability Management:** By identifying and addressing weaknesses in the network, the risk of breaches and attacks is reduced. Scans uncover outdated software, misconfigurations, and potential entry points, providing crucial input for performing vulnerability management.
2. **Asset Discovery:** Knowing all devices, systems, and applications connected to the network helps maintain an accurate inventory, ensuring that unauthorized devices or potential rogue connections are identified. Maintaining an accurate inventory enables proper prioritization for vulnerability management and other security areas.

There are several types of scans: network, web application, endpoint, and cloud security scanning. All of these help discover assets and identify vulnerabilities.

Asset management

Asset management is the process of identifying, cataloguing, and maintaining an inventory of all hardware, software, and digital assets within an organization. It ensures that the SOC has a clear understanding of the environment it is tasked with protecting. Asset management is also commonly required for organizations to establish a functional information security management system.

The importance of asset management lies in the benefits it provides – enhanced visibility of assets, easier prioritization, and attack surface reduction. Identifying unauthorized or unmanaged assets helps reduce potential entry points for attackers, while knowing which assets are critical (e.g. those containing sensitive data) aids in prioritizing protection efforts.

Within the asset management domain, we can differentiate three key components: asset discovery, asset classification, and asset lifecycle management.

Asset discovery – comments from real use cases

The main purpose of this component is to perform asset discovery through port scanning. The tools are discussed in more detail in other documents, but for asset discovery, tools like masscan, nmap, rustscan, and other port scanners are typically suitable. Alternatively, higher-level solutions extending the capabilities of port scanners, such as IVRE or snor4, can also be used.

Due to performance requirements, particularly the capabilities of the network connection, a physical server was chosen. Based on benchmarks comparing the cloud

platform and the physical machine, it was found out that, due to differing network link capacities and the overhead of the cloud platform (in our case, OpenStack), the physical server can achieve a scanning rate up to 10 times better than the cloud. However, this may vary depending on the infrastructure and can be easily adjusted to fit the organization's needs and capabilities.

Based on the experience at the University of Tartu in Estonia, one way to mitigate scanning performance issues when using Virtual Machines is to reconfigure the hypervisor or cloud software and the servers to enable lower-level access to the networking stack. The University of Tartu uses an OpenStack-based private cloud. When running large-scale network scanning software in OpenStack virtual machines, it is recommended to disable the local firewall on the OpenStack nodes (where the scanning VM is deployed) to allow direct connection to the network. It is also suggested to disable the OpenStack virtual network VLAN module for the VM, providing direct access to the node's network interface. This should mitigate most of the performance issues while still allowing the benefits of virtualization.

To ensure easy recovery in case of server failure or other unpredictable events, it is essential to perform configuration management using a suitable tool, such as Ansible, Puppet, or Chef.

Regarding asset discovery, it is generally recommended to conduct it across all network subnets of the organization, except for selected subnets that are unsuitable for scanning, such as those with IoT devices. An important consideration is setting the correct rate limit to prevent the scan from placing an unreasonable load on both network elements and the end machines being scanned. This setting should account for the size of the network and the robustness of individual network elements. Additionally, necessary adjustments to the network elements should be made, such as adding exceptions to firewall logging.

It is also good practice to inform administrators of local networks and services about upcoming scans before they begin or when significant setting changes occur. Although properly configured scans should be completely harmless, occasional issues may still arise.

These basic scans are typically performed in an opt-out regime, meaning the entire network is scanned unless there is a reason to exclude certain areas. This reason may be identified by the SOC team in advance or requested by a local administrator (with justification). Information about the scans is available to the SOC and includes details on the tools, schedule, and contact information for the responsible person.

There is often a possibility to perform more detailed vulnerability scans, which may pose risks. These should always be explicitly confirmed with the administrators of the scanned services in advance, and are typically conducted on a non-production instance of the service intended for testing.

Another important aspect to consider is the network placement of the scanning server, ensuring that private/internal networks receive adequate attention. Private addresses often house critical data and services accessible only to internal users, yet they can still face security risks. At Masaryk University, publicly available and university-wide accessible systems are currently being dealt with. The scanning capabilities are planned to be expanded to segmented internal networks, likely through VPN connections or firewall configurations.

Regarding scalability – at Masaryk University, the physical scanning server is set up with 24 CPUs and 32GB of RAM, and has three network interfaces (10Gbit) attached to provide perspectives from both external (internet) and internal networks (university subnet + 10.0.0.0/8). Each scan of an entire /16 subnet takes up to 80 hours. This is accomplished by using a scanning rate of 80,000 pkt/s with Masscan. Please note that this approach focuses solely on IPv4.

Vulnerability management

Vulnerability management is the process of identifying, assessing, prioritizing, and remediating security vulnerabilities in an organization's environment. It is a continuous process that helps reduce risk and improve overall security.

The usual steps of the vulnerability management process include identification, assessment, prioritization, remediation, reporting, and monitoring.

For identification, vulnerability scanners are used to detect weaknesses in systems, applications, and configurations, typically integrated with asset management for a comprehensive view. In the assessment phase, vulnerabilities are evaluated based on their severity (for example, CVSS) and impact. Based on this assessment and other factors (such as asset criticality and existing exploits), vulnerabilities are prioritized for remediation (patched or mitigated by means of additional security controls). Finally, remediation efforts are tracked, progress is reported, and retests are conducted to ensure that vulnerabilities are no longer exploitable.

Vulnerability scanning – comments from real use cases

To facilitate parallel development of vulnerability scanner orchestration and integration, multiple cloud machines have been chosen to run individual scanners and their orchestration. However, this may vary depending on the infrastructure and can be adjusted to fit the organization's needs and capabilities.

Similar to the server used for asset discovery, emphasis must be on easy deployment and management of these servers. This can be achieved by applying the Infrastructure as a Code (IaC) approach and using a configuration orchestration tool (e.g. Terraform or AWS CloudFormation for building cloud VMs) in combination with a configuration management tool (e.g. Ansible, Puppet, or Chef for configuring the machines).

As with asset discovery, correctly setting the rate limit and adjusting the scan target list is crucial to prevent excessive load on scanned systems and related infrastructure components, such as network devices. Certain vulnerability scanning actions can have a negative impact on the availability and integrity of the systems being tested. Therefore, it is necessary to consider which parts of the infrastructure, and under what settings, can be subjected to vulnerability scanning.

4.5. Tools required to build a SOC

Building an effective Security Operations Center (SOC) requires selecting and integrating a well-defined set of tools. These tools enable monitoring, threat detection, exchange of information, incident response, and continuous improvement, forming the foundation of the SOC's technical capabilities. Below is an overview of essential technical tools categorized by function. Various available solutions on the market will be discussed in detail in Chapter 6. It is important to note that there is a wide range of tools available, and their selection, customization, and integration depend on the organization's

financial capacity and the chosen SOC model.

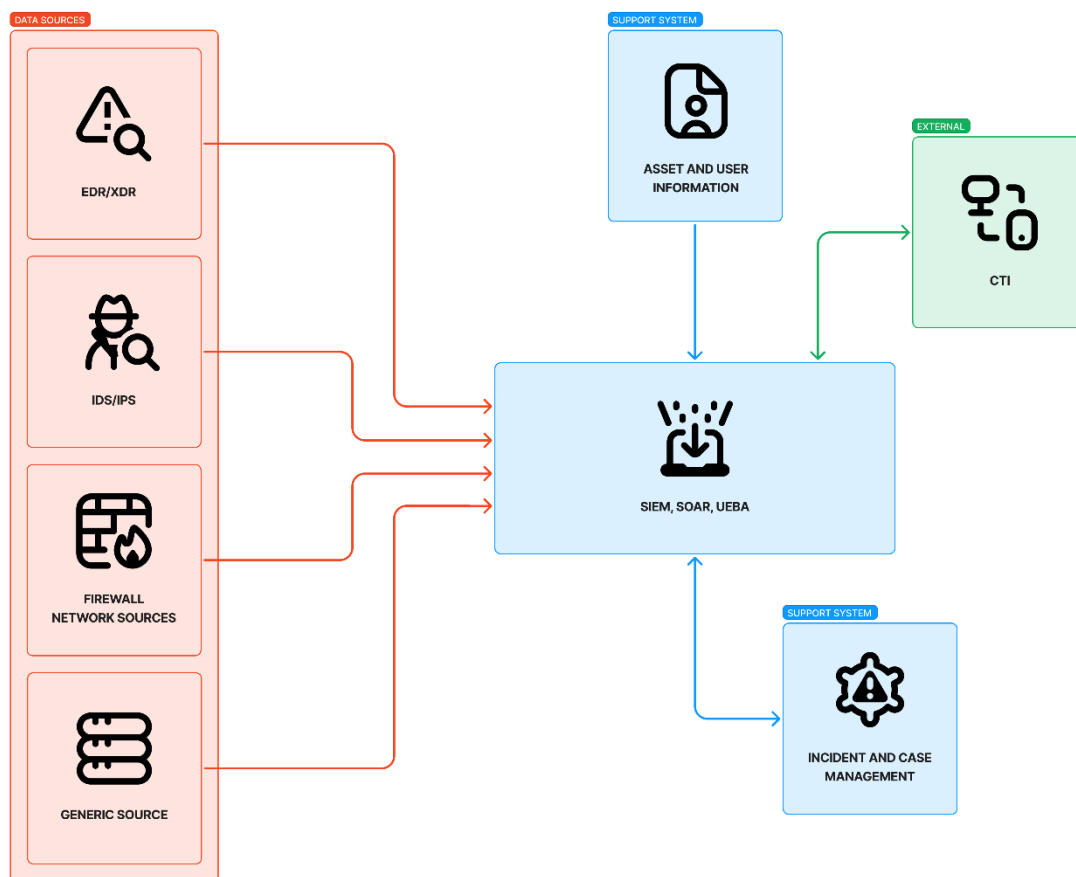


Figure 5 A diagram illustrating an example of tool integration (image source: Flaticon.com)

Security Information and Event Management (SIEM)

A SIEM system is the backbone of any SOC, aggregating and normalizing log data from diverse sources – such as firewalls, servers, IDS, applications, and network devices – to enable centralized monitoring. By applying correlation rules, SIEMs can detect anomalies and potential threats in real time, supporting incident response with alerts and forensic data. Advanced analytics helps identify complex threat patterns, which is crucial for both detection and compliance. SIEM systems must be scalable and capable of integrating with other tools to handle high data volumes and support custom organizational rules.

User and Entity Behavior Analytics (UEBA)

User and Entity Behavior Analytics (UEBA) is a cybersecurity solution designed to detect and respond to anomalous activities by analyzing the behavior of users and entities within an organization's network. By leveraging machine learning, advanced analytics,

and behavioral modelling, UEBA identifies deviations from established patterns, such as unusual login times, irregular file access, or unexpected network usage. Unlike traditional security tools that rely on predefined rules, UEBA dynamically adapts to evolving threats, making it highly effective at detecting insider threats, compromised accounts, and advanced persistent threats (APTs). By contextualizing actions within their behavioral baselines, UEBA enhances threat detection accuracy, reduces false positives, and complements existing security frameworks.

Endpoint Detection and Response (EDR)

EDR solutions monitor endpoint activity to detect and investigate threats on devices such as computers, mobile phones, and servers. By continuously logging endpoint data, EDR tools identify both known and unknown threats, as well as suspicious behaviors that may indicate malware or unauthorized access. These tools provide SOC teams with real-time analytics and automated responses, such as isolating compromised devices, to contain threats at the endpoint level. EDR systems are crucial for managing endpoint security and provide forensic data for incident response, enhancing visibility and control across IT environments.

Extended Detection and Response (XDR)

XDR solutions extend beyond EDR by consolidating and analyzing data from multiple security layers – such as endpoints, networks, email, and cloud environments – to provide a comprehensive view of threats. This integration enhances SOC capabilities by correlating events from various sources, enabling the detection of complex attack chains that might evade traditional point solutions. By centralizing threat detection, response, and investigation within a single platform, XDR reduces response times, improves SOC efficiency, and minimizes alert fatigue by prioritizing significant incidents. Through machine learning and behavioral analytics, XDR further enhances proactive and adaptive threat detection, fostering a more resilient security posture across all layers of the IT environment.

Security Orchestration, Automation and Response (SOAR) tools

SOAR platforms streamline SOC workflows by automating repetitive tasks such as alert triage, investigation, and incident response. By using playbooks, SOAR tools standardize responses across various incident types, automatically triggering actions such as threat containment, data enrichment, and alert prioritization. This automation not only improves incident response speed and consistency, but also reduces analyst fatigue and the likelihood of human error. Integrated with SIEM and other SOC tools, SOAR enables a cohesive and efficient incident management process, allowing analysts to focus on more complex threats that require human insight.

Network monitoring tools

Network monitoring tools provide visibility into network traffic, identifying anomalous activities and potential intrusions in real time. These tools often include Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), which can detect and, in some cases, block malicious traffic. Effective network monitoring tools support SOC teams by ensuring that all network segments are monitored, providing insights into lateral movement of threats within the infrastructure. These tools play a vital role in identifying suspicious activity that may not be captured directly by SIEM and endpoint tools.

Asset inventory and asset inventory software

An accurate and up-to-date asset inventory is crucial for SOC operations. This tool provides a comprehensive view of all assets within an organization, including devices, applications, and users. Asset inventory solutions help SOC teams maintain visibility over organizational resources, identifying unprotected devices and unauthorized access points. When integrated with SIEM or EDR tools, asset inventory assists in prioritizing critical assets during incident response, enabling the SOC to make data-driven decisions that protect high-value resources.

Incident and case management solutions

Incident management systems are essential for organizing and tracking all security incidents within the SOC. These tools enable analysts to document incident details, assign tasks, and manage workflows throughout the incident lifecycle. By maintaining a structured incident register, SOC teams can generate reports, analyze historical data, and gain insights into recurring patterns and threats. Incident management solutions also help SOC teams meet compliance requirements by providing a complete record of incident responses and their outcomes. Integration with SIEM and SOAR further enhances the incident management process by enabling faster responses and coordinated actions across the SOC infrastructure.

Cyber Threat Intelligence (CTI) sources

Threat Intelligence Platforms (TIPs) collect and organize threat data from both internal and external sources. They help SOC analysts identify emerging threats by providing insights into Indicators of Compromise (IOCs) and Tactics, Techniques, and Procedures (TTPs) used by threat actors. CTI sources, which include feeds from commercial providers, open-source intelligence, and sector-specific sharing communities, help SOC teams stay ahead of evolving threats. Integrating CTI with SIEM and other detection tools enriches the data available for analysis, enabling the SOC to proactively adapt defenses and tailor responses based on specific threat profiles.

References

[1] DCAF, 2023. Guidebook for New CSIRT Employees. Available at [Guidebook_for_new_CSIRT_employees_EN_09032023.pdf](#) [Accessed Oct. 27th, 2024]

[2] "How to set up CSIRT and SOC," ENISA, <https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc> [Accessed Nov. 3, 2024].

5. Introduction to digital forensic and incident response (DFIR)

Handling and response to security incidents is a fundamental reactive activity for organizations in regard to information security and cybersecurity. Its primary goal is to contain the security incident, identify its source, understand the attacker's methodology, analyze the impacts, and propose the appropriate security measures. The security incident needs to be resolved quickly and in the correct manner. Digital forensic analysis plays a key role in this respect. The analysts aim to confirm or disprove the forensic hypothesis in a digital forensic analysis, particularly when resolving a security incident.

This chapter summarises the fundamental aspects of security incident resolution and digital forensic analysis.

5.1. Security incident handling and response

This guide offers a framework for security teams in academic organisations demonstrating how to handle security incidents, supporting the development of internal procedures. Aligned with NIST SP 800-61 Rev. 2 [1] and European regulations such as the NIS Directive [2], NIS2 Directive [3], and the General Data Protection Regulation (hereinafter referred to as "GDPR") [4], it outlines general incident response phases. Specific procedures for handling various types of incidents, such as malware attacks or social engineering, should be independently developed by the institution.

Security incident handling phases

According to Article 6 of the NIS2 Directive, incident handling means any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident. Security incident response is a complex process that must be divided into several partial phases. Each phase may involve several activities, depending mainly on the type, scope, and severity of the security incident.

The incident handling lifecycle outlined in NIST SP 800-61r2 typically consists of four main phases:

1. preparation,
2. detection and analysis,
3. containment, eradication, and recovery, and
4. post-incident activity.

ISO/IEC 27035 [5] is an international standard providing guidelines for managing information security incidents. According to ISO/IEC 27035 incident handling lifecycle offers a more structured approach to managing security incidents, covering six phases::

1. preparation,
2. detection and reporting,

3. assessment and decision,
4. response,
5. lessons learned, and
6. coordination and communication.

The approach provided in the NIST is more focused on computer security incidents, while ISO/IEC 27035 addresses a broader range of security incidents, including those related to information breaches and cyber-attacks. Despite the differences, both frameworks emphasize the importance of preparation, detection, containment, eradication, and recovery in effectively managing security incidents and improving overall cybersecurity resilience.

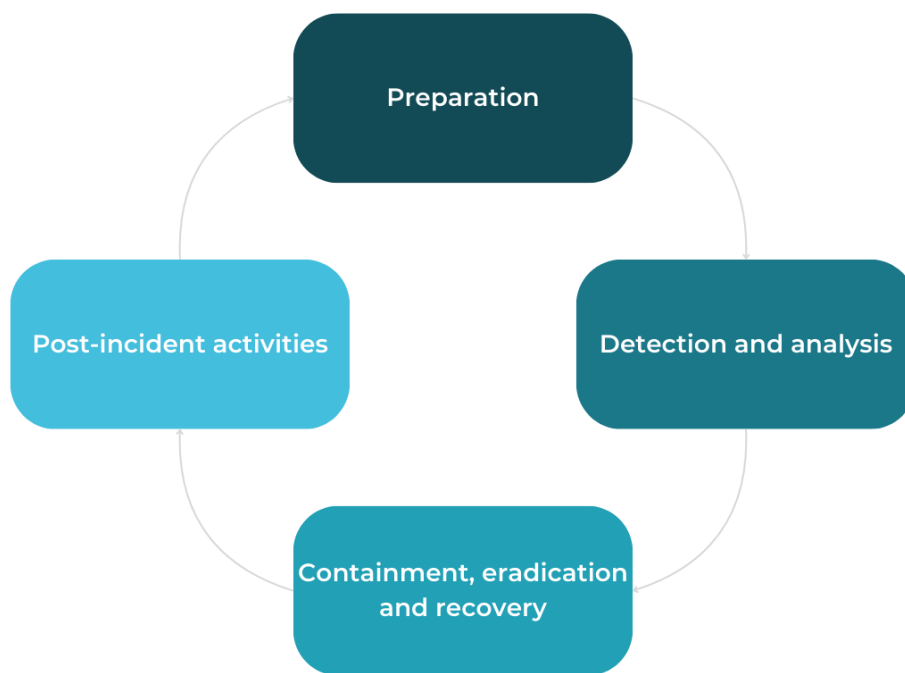


Figure 1 Phases of security incident resolution according to NIST 800-61 r2.

To better answer the needs of academic organizations, we have slightly modified and adjusted the solution phases according to NIST 800-61 r2. A flowchart of the security incident resolution process is given in Fig. 2.

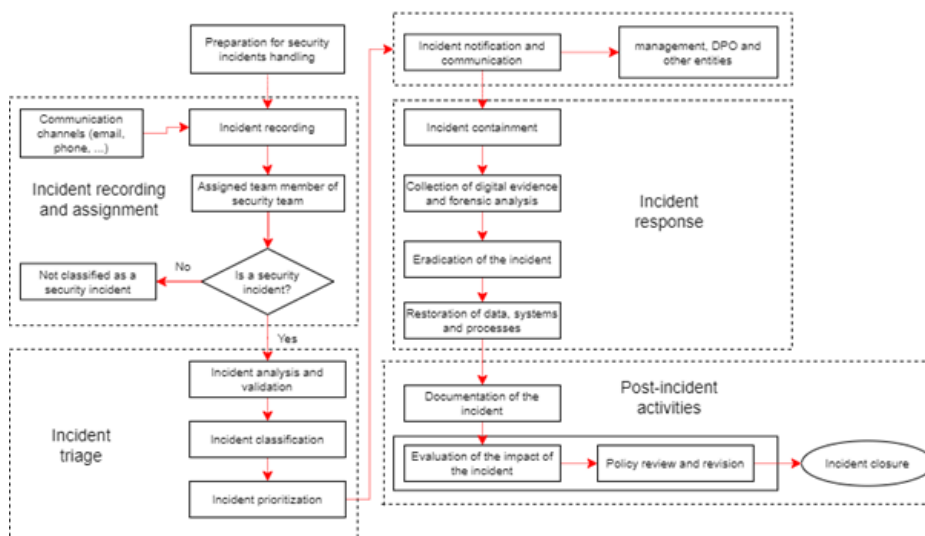


Figure 2 Proposed phases of security incident resolution - Appoint security team members - Impact evaluation

Draft provisions for an academic organization's internal regulations:

Handling of security incidents typically involves the following phases:

- a. preparing for security incidents,
- b. recording and assignment of a security incident,
- c. triage of a security incident,
- d. notification of a security incident,
- e. response to a security incident:
 - o Malware attack [6],
 - o Social engineering [7],
 - o Ransomware [8],
 - o Data breach [9],
 - o Linux server compromise [10],
 - o Other.
- f. post- incident activities and the closure of the security incident,
- g. review of working practices and suggestions for improvement.

Each phase may involve several activities, depending on the type, scope, and severity of the security incident.

Preparing for security incidents

Preparing for security incidents is crucial for an effective response, involving establishing procedures, acquiring resources, and training the security staff. This phase consists of setting up workflows, verifying procedures, training staff, and maintaining technical security, readiness and preparedness to act. Additionally, this phase may also involve the development and implementation of a DRP (Disaster Recovery Plan) and BCP (Business Continuity Plan), closely associated with incident handling and response. Examples of developed playbooks include:

- IRM playbooks [11],
- Gov.scot [12],
- Taksati [13].
- IRC playbooks [14].

1. Initiation of resolution and recording of security incidents

This phase initiates security incident resolution after the security team have collected incident information, either through monitoring activities or reports. Incidents can be reported via emails, reporting forms, or phone calls, with CSIRT teams requiring at least an email report and possibly a phone call for emergencies. It is recommended that the reporting procedures should be simplified in the context of limited technical expertise of those reporting incidents. Upon receipt of a report, a ticket is created and assigned to a security team member for investigation. If the issue qualifies as a security incident, it is pursued accordingly; otherwise, it's closed or escalated to the technical support to deal with if it's only a technical issue. Internal regulations should mandate the users to report incidents and ensure that the users understand the reporting process.

An example of questions to consider when reporting is given on the Slovak Government CSIRT.SK website [15].

Security incident triage

The triage of a security incident means that the security incident in question is further analysed and validated. At this stage, the category and priority status of the security incident is determined. Those handling the incident in this phase analyse the security incident to find out the details, such as the type of attack, the severity of the security incident, the intended target of the attack, the impacts to the organization, the method of dissemination, and potential vulnerabilities that have been or could have been exploited. These details will then assist the organization's security team in the next stages of resolving the security incident.

Draft provisions for an academic organization's internal regulations aim to streamline the security incident triage, involving steps such as adding incident details, assessing severity, classifying by type, and determining whether the existing workflows are applicable

2. General and specific procedure for dealing with security incidents

This guide is intended to assist in the development of a generic procedure for dealing with security incidents within academic organisations. Specific procedures for each type of security incident that the security team encounters on a relatively routine basis will be a part of the material. When a specific resolution workflow is developed for the category of security incident being addressed, those handling the incident shall follow that procedure.

3. Security incident notification

During the incident notification phase, incident details are conveyed to stakeholders such as the academic organization's management, third-party vendors, and government entities such as law enforcement and cybersecurity agencies. Once the incident is confirmed, those handling the incident notify the management for necessary approvals as outlined in the organization's internal regulations, facilitating urgent activities such as the analysis of accounts and devices. Example of an organization's internal regulation notification:

- a) Security incidents of medium severity are reported to the Security Team Director.
- b) High severity incidents are reported to the academic organization's management.

- c) High severity incidents, if crisis management is in place, are also reported to them.
- d) The PR department is notified if the general public or media communication should be required.

In the case of personal data breach incidents, prompt notification to the DPO is essential, with assistance provided by those handling the incident and other person involved. Should the need arise to notify the general public and media, which will involve numerous users or give rise to legal implications, the PR department or legal department should be notified accordingly. Major incidents are dealt with by the crisis management team, ensuring communication alignment and adherence to guidelines across all organizational components. The notification phase is performed based on the findings collected during the incident to that moment (either via communication with management or externally). Therefore, it is not possible to determine exactly where notification should be effected in every incident (given the differentiation between internal and external notification procedures, see below).

At this stage it is necessary to distinguish between internal and external communication channels. If PR is included, some information needs to be verified internally (BCP is closely linked). Should it prove necessary to inform the general public, or a large number of users (especially employees and students) of the organisation about the security incident and its resolution, or when the media are interested in the incident, the spokesperson of the PR department in the organisation shall also be informed about the incident to the necessary extent. In that case, certain recommendations ought to be added (e.g. verification of internal procedures, IR is not carried out independently but in synergy with a larger running process within BCM).

4. Security incident response

Security incident response is a time-consuming phase in the security incident response process. In terms of procedures, it follows the notification about a security incident, and it usually marks the closure of the security incident. Given the scope of this phase, we have decided to devote a separate chapter to it.

The specificity of this phase is that it will differ depending on the type of security incident. It seems recommendable to provide a general framework for the different phases within the general procedure and to specify the activities and features of each phase for each particular type of security incident in line with the established procedures. It can be seen in the security incident handling flowchart shown in Fig. 2 that before starting the general procedure, security team members are required to prioritise the specific procedure, provided that such a procedure has been adopted in the organisation.

Generally, the response to a security incident involves the following activities:

- a. containment of a security incident,
- b. Digital trace collection and digital forensics,
- c. eradication of a security incident,
- d. recovery from a security incident.

It is important that the activities should be run in parallel. In some cases, the resolution of a security incident may be split into several parts and recovery may already be underway on one part of the IT infrastructure, while digital traces are still being collected on another.

5. Post-incident activities and security incident closure

After completing the security incident response, the organization's security team will document the incident, updating the ticketing system with resolution details, impact assessment (if discernible), and providing a brief description of the resolution along with the identified attack vectors. If communication is effected with other units or institutions, relevant information will be thus shared. For major incidents, producing a Security Incident Report is advisable, serving as a foundation for investigations or addressing data breaches.

Draft provisions for an organization's internal regulations specify the closure process for security incidents. Those with established resolution workflows follow those procedures, while others are closed within the recording system. An effective closure requires details on resolution, impacts, and incident handling, high and critical severity incidents necessitating a security incident report. Those handling the incident have to manage closure operations and inform those reporting the incident, and, upon request, provide post-incident conclusions.

After a security incident is resolved, a comprehensive evaluation of procedures, tools, and actions must follow to highlight the areas for improvement. This analysis will enable incident response procedures to be updated in the context of subsequent preparation phases specified in the organization's internal regulations. This includes the creation of a Security Incident Report for incidents of high and critical severity that pose a threat to a part or the whole organisation, the Report ought to provide a complete history and resolution of the incident (low and medium severity or frequently recurring incidents do not warrant such analysis or evaluation). Regular (e.g., every 3 months) meetings of (CSIRT) team members are recommended to evaluate the procedures, tools, and staff readiness even when no incidents have occurred.

IHaR Guides

The above text summarises the incident handling and response process. It is supplemented by several methodological documents that offer basic guidelines for those responding to the incident, highlighting each step of incident response and handling procedure, including descriptions of tools and templates. These guidelines are divided into several sections.

The first section provides guidelines for the security incident management including policies, taxonomy, and reporting. The second part is focused on the specific procedures according to type of incidents:

1. Data Breach
2. Malware
3. Ransomware
4. Social Engineering
5. Server Compromise

5.2. Digital Forensics

Digital forensics is a multi-step process identifying the involved digital media as potential evidence, the final step being their presentation as evidence to expert witnesses in court during civil or criminal proceedings [16]. Digital forensics can be used in civil or criminal proceedings and on resolving security incidents. In this case, digital

forensic analysis can be defined as the incident response process, from the identification and analysis of digital evidence to presentation of the findings to senior management or in a court of law, in civil or criminal proceedings. The main objectives of digital forensic analysis include:

- Assisting in recovering, analysing, and safeguarding computers and related materials so as to help investigating bodies use them as evidence in a court of law.
- Deciding on procedures at the crime scene to ensure that the collected digital evidence should not be damaged or corrupted.
- Data collection and duplication – recovery of deleted files and partitions from digital media to extract and validate digital evidence.
- Assisting in the quick identification of digital evidence and estimating the impact of the attacker's actions on the individual or organisation.
- Creating a computer forensic report that provides a complete overview of the investigation process and its results.

Digital Evidence

The central concept of digital forensic science is **digital evidence**. No unified definition of this term is available, although numerous attempts have been made in this respect. Digital evidence can be defined as:

- any information with probative value stored or transmitted in a digital form [17].
- Any information stored or transmitted in the binary form that can be presented in court as material evidence (International Organization of Computer Evidence) [18].
- Any information with probative value stored or transmitted in the binary digital form that can be presented in court as material evidence with probative value (Scientific Working Group on Digital Evidence) [19].

When analysing the above definition, it becomes apparent that digital evidence is a reasonably broad term. Its essence lies in data storage in digital form, which helps clarify facts or verify certain hypotheses. The main shortcoming of some of the definitions is that they tend to focus on evidence while neglecting data that may, even indirectly, aid in the investigation. Storing data in binary form is also considered outdated as it is only one way of displaying computer data. The key features of digital evidence are [20]:

- **Intangibility** – Data and information are intangible but can be materialised, for example, by storing them on a physical medium or printing them on paper.
- **Latency** — Digital evidence is invisible. We can see photographs, videos, and documents, but not the actual data or information; it is the results only that are perceptible.
- **Temporal Traceability** — Digital evidence contains timestamps. Every activity (e.g., file creation) is recorded alongside the exact time it was executed.
- **High Information Value** — Digital evidence can have high informational value about activities of the given device and about the users or adversaries.
- **Large Data Volume** – Modern computer systems process large amounts of data. A growing demand for memory and storage media increases the volume of user data and the data necessary for the operating system, metadata, and others. This

directly relates to the capacity and financial aspects of securing and storing digital evidence for use in criminal or other legal proceedings.

- **Extreme Dynamism** — This affects the lifespan of digital evidence. The lifespan of digital evidence depends on the medium on which it is stored. Certain parts of memory (e.g., registers) are prone to changes, resulting in the digital evidence having the lifespan of the order of milliseconds
- **Heterogeneity and Complexity** — Computer systems are heterogeneous, comprising a variety of hardware components, operating systems, software, etc., which results in a wide variety of digital evidence sources.
- **Originality** – Digital media and files can be easily copied without data loss or damage.

Given the specific characteristics of digital evidence, it is essential that explicit rules should be followed when collecting, storing, analysing, or handling digital evidence. A valuable resource in this regard is the RFC 3227 standard [21] providing the requirements and regulations relevant to collecting and handling digital evidence:

- **Admissibility** – digital evidence must meet specific legal requirements in order for the evidence to be admissible in a court of law.
- **Authenticity** – the integrity of digital evidence must be maintained, and the chain of custody must be preserved.
- **Completeness** – digital evidence must describe the entire event, not just a specific perspective.
- **Reliability** – the procedures and tools for collecting, examining, analysing, storing, and evaluating digital evidence must be capable of reproducing the same results over time. The procedures should not cast doubt on the authenticity of the evidence and the conclusions drawn after the analysis.
- **Credibility** – digital evidence should be clear, understandable, and credible. The version of digital evidence presented in court must be traceable back to the original binary digital evidence. Otherwise, it is not possible to determine whether the digital evidence was fabricated.

6. Principles of Digital Forensics

Resolving security incidents and dealing with specific cases in civil or criminal proceedings requires the proper handling of digital evidence according to predefined conditions that ensure its immutability. For this reason, it is advisable that several principles should be observed that underpin digital forensic analysis [22]:

- evidence Exchange,
- evidence Characteristics,
- forensic Soundness,
- authentication,
- chain of Custody,
- evidence Integrity,
- objectivity, and
- repeatability,

One of the principles often recalled in forensic science is the Locard's **exchange principle**. This fundamental principle in forensics states that the contact between two objects leaves traces on both objects. This means that material will be transferred from one to the other when two objects come into contact (interact) in the physical world and vice versa. We often see very similar traces in the digital world when two systems interact. For example, when a person sends an email, information about the email, including metadata, is stored by all email servers along the way to the recipient. At the same time, these emails pass through multiple network devices, leaving temporary data necessary for data transfer on each device.

Each type of trace has its **specific properties**, which are essential from the perspective of forensic investigation, as they determine the specific steps of the investigation, particularly in terms of evidence securing, preservation, and analysis. Selected properties of digital evidence are explored in the previous sections.

Forensic investigation is considered **correct** as long as the established principles, standards, and processes of digital forensic analysis are followed [22]. The scientific method refers to the use of "a method or procedure consisting of systematic observation, measurement, and experiment, as well as the formulation, testing, and modification of hypotheses" [23]. Digital evidence must be stored and analysed in a forensically sound manner in order that it could be used. A group of experts in digital forensic analysis consider an investigation correct if the original source of the digital evidence is not altered in any way and is fully reproducible by a third party. However, the ability to ideally capture digital evidence is far from flawless in practice. A good example is the collection and analysis of the device memory. In practice, it is sometimes necessary to interact directly with memory to secure its image.

A key principle in digital forensics is **authenticity**, that is, verifying the genuineness of digital evidence. Verification of authenticity is essentially a two-step process: first, it is examined whether the presented digital evidence is the same as that obtained initially and in the second step its value as evidence is assessed. In the initial stage of the proceedings, it may be sufficient for an individual familiar with the digital evidence to testify about its authenticity. For example, those who collected the digital evidence can confirm that the evidence presented in court is the same evidence that was actually collected. Similarly, a system administrator can verify that the data retrieved from their system is the same data that was originally stored in the system. There are two methods of authenticating the evidence.

1. **Physical authentication** - documentation of the process of finding/retrieving the physical carrier of the trace. e.g., a hard drive and securing it at the scene, for example, storing it in a container that prevents media substitution and protects the materials against unauthorized alteration. This will prove that it is the same data medium that has been originally secured.
2. **Data authentication** - authentication of the contents of the secured media, usually by creating an image and recording the hash fingerprint of the image, e.g. using SHA256/SHA512. This procedure proves the authenticity of the media contents during further processing. It is closely associated with another essential principle of digital forensic analysis - integrity. These aspects will be addressed in more detail in subsequent sections.

The **chain of custody** is documentation that records the entire process of collecting, transferring, handling, and storing physical or digital evidence. This lifecycle begins when forensic investigators (analysts) secure the digital evidence and ends when the security incident is resolved, or the investigation results are handed over to the appropriate

authorities. Afterwards, the digital evidence may either be returned or destroyed. It is critical that the chain of custody should be maintained. If digital evidence needs to be presented as evidence in a court of law, any break in the chain of custody may result in the evidence being excluded from civil or criminal proceedings. It is, therefore, essential to ensure that the entire lifecycle of the digital evidence should be fully documented.

This document records the sequence of control over the given piece of evidence from the moment it was identified, collected, or obtained by a forensic analyst to its current state and location. The purpose of the chain of custody is to enable the identification of access and movement of digital evidence at any given time. The chain of custody report may consist of more than one document, e.g., for digital traces, alongside a document recording the acquisition of digital data from a specific device, the movement of that device, and documentation recording subsequent extracts or copies of potential digital traces for further analysis or other applications. The chain of custody record should contain at least the following information [24]:

- a unique identifier for the digital evidence,
- the case to which the digital evidence relates,
- a list of individuals who had access to the digital evidence, including the time and place of access,
- a list of individuals who checked the digital evidence and the time of the check,
- reasons for checking the digital evidence (case identification and purpose statement) and, if applicable, the relevant authority,
- any necessary changes to the digital evidence, the name of the responsible person, and justification for the change.

The chain of custody record should be maintained throughout the entire life of digital evidence and preserved for a specified period of time even after the case in which the digital traces were obtained and analyzed is concluded (e.g., in criminal proceedings). Maintaining an appropriate chain of custody requires several essential steps [25]:

- 1) Collection: Recording the retrieval of initial evidence, including the date, time, and collection method.
- 2) Documentation: Keeping precise records of those who interacted with the evidence, the reasons for their involvement, and of any alterations made.
- 3) Storage: Ensuring that evidence is securely stored in tamper-proof containers or digital formats with restricted access to prevent unauthorized handling.
- 4) Transfer: Documenting evidence movement between different locations or individuals, with a clear log of the transfer process and those involved.
- 5) Analysis: Keeping a detailed record of the forensic analysis process, including the tools and methods used, to ensure transparency and the ability to replicate the results.

Another essential principle of digital forensic analysis is **integrity**, i.e., preserving digital evidence in its original form. The purpose of integrity checks is to demonstrate that the digital evidence has stayed the same since the time it was first secured. In practice, verifying the integrity of digital evidence involves comparing the digital fingerprint (hash) at the time of Collection with the digital fingerprint at the time of comparison. While ensuring integrity is an important principle, it cannot always be achieved in practice, as data on live systems and networks is subject to constant changes.

Objectivity is a crucial factor in digital forensic analysis. The interpretation and presentation of digital evidence should not be biased. This is not an easy task for a forensic analyst, as people form the first impression of the situation, especially if they are familiar with the broader context. They may also encounter different people and hear

their opinions when collecting digital evidence. Forensic analyst must resist preconceived notions and pressure to reach specific conclusions. The most effective way to ensure objectivity is to let the digital evidence speak for itself as much as possible. Every conclusion should be the result of precise argumentation supported by the analysis of the digital evidence. Another effective approach to ensuring objectivity is to involve several independent forensic analysts and compare their findings.

A key aspect of any scientific method is that experiments or observations must be repeatable to be independently verified (there are exceptions, e.g. securing RAM). This also applies to digital forensic examinations. It is essential that the findings in a forensic investigation could be independently verified, as the investigation may affect individual rights (e.g., personal liberty). Therefore, a forensic analyst must repeat some or all of the analyses conducted by another forensic specialist. To enable such verification, it is essential that each step should be fully documented when working with digital evidence and throughout the forensic examination process. Other investigators can verify the results by using this documentation and the same digital evidence.

Phases of digital forensic analysis

Similar to other processes, digital forensic analysis involves several steps or phases. Standardising these phases helps to streamline digital forensic analysis and accelerate the forensic examination process by clearly defining procedures and specific steps. This prevents various errors, preserves the integrity of digital evidence, and enhances the credibility of the final conclusions.

Currently, there are few universally accepted models available. Over time, several process models have been defined and refined. Each iteration has attempted to integrate new technologies and methods into the previous model. Recent research on process models has focused mostly on incorporating new methods and tools into existing models to improve processing efficiency or to address new investigation problems [26]. The models utilised in this study include the generally accepted DFRWS 2001 model, the process model mentioned in earlier sections [22] and the ISO/IEC 27037:2012 standard [24]. The resulting model covers six phases of the analysis:

1. Identification
2. Acquisition and Collection
3. Preservation
4. Examination
5. Analysis
6. Presentation

The following table provides a brief description of each phase of digital forensic examination, including the outputs from each phase.

Table 1 – Digital forensics phases

Phase	Description of Activities	Phase Output
Identification	Identification of the purpose of the investigation and necessary resources Identification and description of the environment Searching, recognizing, and	Identified devices

	documenting potential digital evidence	
Acquisition and Collection	Gathering data from digital devices Gathering devices that contain potential digital evidence	Forensic image Other digital evidence
Preservation	Storing digital evidence on suitable media Ensuring the integrity of secured digital evidence	Cryptographic hash
Examination	Extracting data (artifacts) from digital evidence Reducing and filtering data (artifacts) File recovery and data carving	Selection of relevant digital evidence (artifacts)
Analysis	Identification of tools and techniques to be used Prioritization, filtering, and correlation of digital evidence Interpretation of analysis results and confirming/refuting of hypotheses	Confirmation/refuting of hypotheses
Presentation	Summarization and explanation of results Submission of results to the client	Forensic report Presentation

DFIR Guides

The above text summarises the digital forensic analysis, digital evidence, and the forensic examination process. It is supplemented by several methodological documents that offer forensic analysts basic guidelines on performing each step of digital forensic analysis, including descriptions of tools, forensic artefacts, and templates. These guidelines are divided into sections.

The first section includes guidelines applicable to the initial phases of digital forensic analysis, from identification and acquisition to creating forensic triage. These guidelines are included in the following documents:

1. **Identification of digital evidence sources and their preservation** – a document focused on identification and preservation of digital evidence sources
2. **Digital evidence acquisition, mounting, and tools** – a document focused on acquiring digital evidence, working with disk images, and securing digital evidence, including tool descriptions.
3. **Digital forensic triage and tools** – a document focused on digital forensic triage and tools required for this part of digital forensic analysis.

The second part is focused on examination of digital evidence . Two situations can arise when securing and analysing digital evidence: the digital device is either powered on (live acquisition and analysis), or off (post-mortem acquisition and analysis). The following issues are addressed in this section :

1. **Live Forensic Analysis - OS Windows** – steps involved in digital forensic analysis on a powered-on device with the Windows OS installed.
2. **Live Forensic Analysis - OS Linux** – steps involved in digital forensic analysis on a powered-on device with the Linux OS installed.
3. **Live Forensic Analysis - OS MacOS** – steps involved in digital forensic analysis on a powered-on device with the MacOS.
4. **OS Windows Artifact Analysis** – a guide to the most analysed forensic artefacts in the Windows operating system.
5. **OS Linux Artifact Analysis** – a guide to the most analysed forensic artefacts in the Linux operating system.
6. **OS MacOS Artifact Analysis** – a guide to the most analysed forensic artefacts in the MacOS.
7. **Memory Artifact Analysis** – step-by-step instruction on how to analyse memory artefacts from various devices.
8. **Network Forensic Artifact Analysis** – step-by-step instruction on how to analyse digital evidence obtained from the network traffic.
9. **Analysis of Virtual Machines and Cloud Services** – step-by-step instruction on how to examine virtual machines and cloud services from the perspective of digital forensics.

The third group of the guidelines are focused on supplementary activities aimed at adding context or collaborating with other entities and preparing a final report:

1. **Collaboration with Law Enforcement Agencies** – an overview of procedures for collaborating with law enforcement agencies
2. **DFIR report** – detailing steps to create a report from digital forensic analysis and incident resolution

References

[1] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide," CSRC, <https://csrc.nist.gov/pubs/sp/800/61/r2/final> (accessed May 15, 2024).

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

[4] "Legal text," General Data Protection Regulation (GDPR), <https://gdpr-info.eu/> (accessed May 15, 2024).

[5] ISO/IEC 27035-1:2023 Information technology — Information security incident management Part 1: Principles and process, Published (Edition 2, 2023)

[6] [UPJS] Malware guideline.docx

[7] [UPJS] guide_social_engineering_v2.docx

[8] [UPJS] Ransomware guideline.docx

- [9] [UPJS] Data breach guideline.docx
- [10] [UPJS] Linux server compromise guideline.docx
- [11] "IR playbooks - Mathieu Saulnier," Scribd, <https://www.scribd.com/document/632061669/IR-Playbooks-Mathieu-Saulnier> (accessed May 16, 2024).
- [12] The Scottish Government, "Cyber resilience: Incident management," Scottish Government, <https://www.gov.scot/publications/cyber-resilience-incident-management/> (accessed May 16, 2024).
- [13] "Incident response playbook creation. Chris Taylor Taksati Consulting - PDF free download," DocPlayer, <https://docplayer.net/137693778-Incident-response-playbook-creation-chris-taylor-taksati-consulting.html> (accessed May 16, 2024).
- [14] Got a plan? [online]. INCIDENT RESPONSE CONSORTIUM. 2022 [cit. 2024-12-02]. Dostupné z: <https://incidentresponse.com/mini-sites/playbooks>
- [15] "Nahlásiť incident," Nahlásiť incident | CSIRT.SK, <https://www.csirt.gov.sk/nahlasit-incident.html?csrc=2677669608893138056> (accessed May 15, 2024).
- [16] Raghavan, Sriram, and S. V. Raghavan. "A study of forensic & analysis tools." 2013 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE). IEEE, 2013.
- [17] Whitcomb, Carrie Morgan. A historical perspective of digital evidence: A forensic scientist's view. International Journal of Digital Evidence 1.1 (2002): 7-15.
- [18] Pollitt, Mark. A history of digital forensics. IFIP International Conference on Digital Forensics. Springer Berlin Heidelberg, 2010.
- [19] Angus M., and Richard Paige. Requirements in digital forensics method definition: Observations from a UK study. Digital Investigation 27 (2018): 23-29.
- [20] Rak, Roman, and Viktor Porada. Digitální stopy v kriminalistice a forenzních vědách. Soudní inženýrství 17.1 (2006): 3-23.
- [21] Brezinski, D., and T. Killalea. RFC 3227: Guidelines for Evidence Collection and Archiving, 2002. Available at: <https://www.ietf.org/rfc/rfc3227.txt>
- [22] Arnes, André, ed. Digital forensics. John Wiley & Sons, 2017.
- [23] Turvey, Brent E. Case linkage: Offender modus operandi and signature, 2008.
- [24] ISO/IEC 27037:2012, Information technology - Security techniques - Guidelines for identification, Collection, acquisition, and preservation of digital evidence, 2012.
- [25] Redactor. "Best Practices for Chain of Custody in Digital Evidence." Redactor Blog, June 26, 2024. Available at: <https://www.redactor.com/blog/best-practices-chain-of-custody-digital-evidence>. Accessed 2 Jan. 2025.
- [26] Du, Xiaoyu, Nhien-An Le-Khac, and Mark Scanlon. Evaluation of digital forensic process models with respect to digital forensics as a service. arXiv preprint arXiv:1708.01730, 2017.

6. Review of software and hardware solutions

6.1. Review methodology

The selection of tools to be used will depend on the scope of tasks for which the SOC is responsible. The tools must be carefully chosen to ensure these tasks are performed effectively and efficiently. An important factor is the size of the SOC team, as well as the model in which security functions are carried out (e.g. a small in-house SOC, service model, or intermediate solutions). A centralized SOC requires a different set of tools compared to a SOC operating in a distributed model.

The methodology for selecting tools used in SOC includes a number of procedures, techniques and tools for monitoring, detecting, analysing and responding to IT security threats. This includes both incident response procedures and the monitoring of IT infrastructure in order to detect irregularities. These include:

- Event monitoring. Using tools to monitor events and logs from various systems and networks to detect irregularities, attacks or unauthorized access.
- Threat detection. Using advanced tools to detect unusual behaviour, phishing attacks, malware, and other security threats.
- Analysis and response. Developing incident analysis and response procedures, including the use of specialized tools for package analysis, data recovery, and response to current threats.
- Process automation. Using tools to automate incident response processes to reduce response times and minimize the impact of incidents on infrastructure.
- Data visualization. Using data visualization tools such as network maps, bandwidth graphs or network activity reports, which facilitates the analysis and understanding of the occurring phenomena.

Selecting the right tools for SOC is crucial for its proper operation. The methodology of tools used in SOC is continuously evolving to counter increasingly advanced threats in cyberspace, and to ensure effective protection of IT infrastructure against attacks.

Methodology of selecting tools for SOC

SOC utilizes a range of advanced tools to support the team's operations and to automate various security tasks. For optimal operation, it is crucial to efficiently deliver the necessary data and conduct effective analysis. The tools supporting SOC operations are designed to deliver analytical data, enable effective data analysis, and facilitate incident response if a threat is identified. Such tools include advanced systems such as SIEM, SOAR, EDR or XDR, as well as additional sets of tools supporting the team's activities, which include software such as network scanners, vulnerability scanning tools, network monitoring tools, CTI sharing platforms, and many others.

The methodology of selecting tools used in SOC includes criteria that facilitate the selection of appropriate hardware and software that ensures reliable operation and effective support for activities related to monitoring, detecting, and responding to IT security threats.

Selection of SOC hardware

When selecting hardware for a SOC, the following aspects should be taken into account:

- **Requirements analysis.** The first step is to analyse the specific requirements of a given IT environment and expectations related to monitoring, detection, and response to incidents. These requirements may result from regulations, industry-specific needs, the size of infrastructure, the type of data stored, etc.
- **Efficiency.** Your hardware should provide enough performance to handle large amounts of data, analyse network traffic in real time, and detect unusual patterns and behaviours.
- **Flexibility.** Hardware should be flexible, allowing for easy expansion and adaptation to the changing needs and requirements of the IT infrastructure.
- **Ensuring business continuity.** The choice of equipment should consider redundancy and the ability to maintain business continuity in the event of a failure.
- **Safety.** The equipment should meet rigorous security standards, both physical and cybersecurity-related.
- **Compliance with regulations.** The hardware should comply with applicable data storage and security regulations, as well as other industry-specific regulations.
- **Network monitoring.** In the case of network monitoring equipment, it is important to take into account parameters related to bandwidth, support for various protocols, packet parsing capability, etc.
- **Costs.** Evaluation of purchase costs, implementation, maintenance, and possible expansion of equipment.
- **Tech support.** Technical support and software updates are essential.
- **Issues specific to the academic community,** such as funding methods, the Public Procurement Act, and challenges related to the interface between science and teaching.

The proper selection of hardware for a SOC is aimed at ensuring that the chosen hardware will be able to meet the demands of monitoring, detecting and responding to IT security threats, while meeting the requirements for performance, security, and compliance with relevant regulations.

Selection of software for SOC

When choosing software for a SOC, the following aspects should be taken into account:

- **Requirements analysis.** The first step is a comprehensive analysis of the SOC's requirements and needs, considering the organization's operational specifics and IT infrastructure.
- **Functionality.** The software should offer a wide range of functionalities, such as event monitoring, network behaviour analysis, incident detection, incident management, reporting, integration with other systems, etc.
- **Scalability and flexibility.** The software should be scalable, allowing it to adapt to changing needs and infrastructure developments, as well as flexible in configuration.
- **Integration with existing tools.** It is essential that the SOC software is compatible and easily integrated with existing IT tools, such as network monitoring systems, logging systems, incident management systems, etc.
- **Regulatory compliance.** The software should comply with applicable IT security standards and data protection regulations, such as GDPR, ISO 27001, PCI DSS, etc.

- Software licensing method, commercial or open source. The open-source model offers significant cost savings but typically demands greater teamwork and higher skill levels from employees. In many cases, commercial software offers additional functions that are not available in the open-source version or require the installation of additional plugins or modules. For more on this topic, refer to the "Solutions – Open-source vs COTS" chapter.
- Technical support and updates. The availability of technical support, regular software updates and the development of functionalities in accordance with new trends and threats are essential.
- Safety. The software should meet rigorous security standards, both regarding the software itself as well as the data stored within the system.
- Costs. Evaluation of purchase costs, implementation, training, maintenance, and licensing software.
- Issues specific to the academic community, such as funding methods, the Public Procurement Act, and challenges related to the interface between science and teaching.

The proper selection of software for a SOC is aimed at ensuring that the selected tools will be able to meet the demands of preventing, detecting and responding to security threats, while meeting the needs of a specific organization and the relevant regulations in a given industry.

Documentation and sources of knowledge

When selecting hardware and software for a SOC, it is crucial to rely on knowledge from various sources, such as legal acts and standards, device and software documentation, manuals and documentation published by cybersecurity organizations, device and software manufacturers, information provided by companies and cyber specialists, etc.

However, when evaluating a specific solution, demos and POCs are the most important factors to consider. In this way, you can effectively familiarize yourself with the capabilities of the offered tool and test its key functions. Product demonstrations can be conducted either in person or online, and they can be carried out for both entirely new programs or improved versions. POC usually offers a comprehensive overview and summary of key functions of the offered product. Additionally, these features are presented in relation to the customer's needs. As a result, these solutions allow for relatively quick and quite effective familiarization with the capabilities of a given tool. Specific concerns can be addressed through answers to the questions raised.

6.2. Open-source vs commercially available off-the-shelf (COTS) SOC tools

Introduction

While deciding whether to adopt open-source or commercially available off-the-shelf (COTS) tools as the foundation for the SOC platform, SOC components should be analyzed from several viewpoints, such as licensing conditions, cost, frequency of

security updates, customization, etc. The goal of this section is to discuss the most important characteristics that should be taken into consideration.

The adoption of open-source software typically incurs low or no licensing costs and often allows for code customization. If an open-source tool does not support required integrations (e.g. APIs, protocols, database connections), it could be modified as required either by the organization that adopts the tool or by a partner IT company. However, with COTS tools, requesting additional features from the provider may be necessary, and these requests can either be denied or take a considerable amount of time to fulfil.

On the other hand, COTS tools are often more actively developed than open-source projects, so users may be able to expect consistent updates. They also typically require less effort for setup and maintenance in comparison to using open-source tools. With open-source tools there is also a risk that they may be abandoned by the community or taken over and changed into a COTS model after being adopted by a large number of users.

COTS tools can be further classified as:

1. **On-premises COTS** - can be deployed inside the organization's environment.
2. **Managed COTS** - are accessed over the internet (as a service) and are deployed and managed by the tool provider, typically in the cloud.

Using **managed COTS** limits deployment options, typically requiring data migration between local infrastructure and the cloud. However, it eliminates the need for setup efforts. Using **managed COTS** often makes more sense when the organization is already working with data stored off-premises, particularly when the data or systems being investigated are hosted in the cloud. Choosing managed COTS is also a practical option when an organization lacks sufficient skilled engineers to maintain the infrastructure required to run the solution on-premises.

On-premises COTS software typically requires more effort for deployment, maintenance, and updates from the infrastructure operators compared to **managed COTS**. Its main advantage is providing control over data location (especially when data locality is required by law or organizational policies), and allows avoiding the need to stream data over the internet. Compared to open-source solutions, **on-premises COTS** are usually restricted to officially supported functionalities and integrations, and do not require customization efforts. On-premises solutions also require a designated space for physical placement, such as a well-organized and secure server room.

Software licenses and terms

Software (both open-source and COTS) can be made available by means of various types of licenses. Some of them differ in specific details, while others are entirely distinct from one another. For example, licenses may differ in software linking, distribution, modification, private use, and sublicensing. Choosing the most appropriate licensing model has a significant impact on the subsequent use. [1,2]

Licenses can grant various types of permissions to the software or tool license holder, dictating how the software can be used or extended. The main considerations are:

- Linking - using the software/tool as a linked or plugged-in component within another licensed software, typically without modifying it.
- Distribution - distributing software to third parties, e.g. clients.
- Modification - extending the software.

- Private use - whether modified software must be made public.
- Sublicensing - whether modified software must be distributed under the same license.

There are many unique open-source licenses. The following Table 1 [4] gives an overview of open-source licenses and specifies whether they are approved by the open-source community, and whether using the license could raise legal risks.

Table 1 - Types of open-source licenses

License	OSI Approval	Potential legal risk
MIT License	Yes	Low
Apache License 2.0	Yes	Low
BSD 3-Clause New or Revised License	Yes	Low
BSD 2-Clause Simplified License	Yes	Low
Generic Public Domain	Yes	Varies
ISC License	No	Low
Creative Commons Zero v1.0 Universal	No	Varies
GNU Lesser General Public License v2.1+	Yes	High
Mozilla Public License 2.0	Yes	Medium
The Unlicense	Yes	Low
Zlib/libpng License	Yes	Low
SIL Open Font License 1.1	Yes	Low
BSD Zero Clause License	Yes	Low
Creative Commons Attribution-ShareAlike 3.0	No	Varies
Creative Commons Attribution ShareAlike 4.0	No	Varies
GNU General Public License v2.0+	Yes	High
GNU Lesser General Public License v3.0+	Yes	High
Python Software Foundation License 2.0	Yes	Low

The **OSI Approved** column indicates how well the license complies with open-source community standards and conforms to Open Source Initiative¹ (OSI) requirements. OSI has a license review process that can be requested for new open-source licenses to obtain approval from the Open Source Initiative.

The **Potential legal risk** column is based on the “Open Source Security and Risk Analysis” (OSSRA)² report [4] summarizing a set of commercial software audits performed by the Black Duck Audit team. The four risk tiers are:

- **Low risk:** Permissive licenses – generally have no or very few limiting conditions.
- **Medium risk:** Semi-permissive licenses – Typically allow modifications but may require modified software to be published under the same conditions or license.

- **High risk:** Restrictive licenses – Typically allow modifications and integration into other software but may require changing the license of the larger software or even publishing the modified version as open source.
- **Varies** – The risk varies depending on the type of usage.

The risks associated with using open-source software primarily arise when the software is modified, repackaged, or used in ways that violate the terms of the license. Open-source software may be free to use for a limited time or with a limited feature set, but a paid license may be required for commercial use. For example, the OpenFaaS community edition is free for personal use or for commercial use with a 60-day limit, but requires a subscription otherwise. On the other hand, some tools offer exceptions for academic organizations that teach students, and might be completely free to use as long as the organization is not using them for profit.

To manage potential risks, it is important for an organization to keep track of the licenses used by adopted tools and services, or by the in-house developed or extended software, along with their specific conditions. For software that is developed or extended in-house or by external partners, there are tools available that can scan all libraries and included tools for individual licenses, ensuring that they are compliant with the main license of the created software. Some asset or vulnerability scanning tools (e.g. Snyk3) also include features for license compliance and Intellectual Property (IP) rights management. Academic organizations should review their internal policies and consult legal experts when determining which license types are acceptable.

Pricing models of COTS tools

This section outlines the typical pricing models of COTS tools and examines the advantages and disadvantages of choosing between them.

Pricing models can vary significantly between different COTS tools, depending on whether they are managed cloud services, licensed software to be deployed on-premises, or re-packaged open-source tools with added support, extensions, and automation. The most common pricing models for COTS tools are:

- **Freemium** – The software is free to use when the number of users or volume of usage is low. The free tier typically comes with set quotas or usage limits.
 - Example: Jira is free for teams of 10 or fewer members, and allows up to 2GB of data storage.
- **Subscription-based** – The software has monthly or annual subscription costs. Subscription fees can either be based on a fixed monthly amount or dynamically calculated. For example, subscription fees may depend on the number of employees using the tool or the number of devices in the fleet.
 - Example: The Malwarebytes ThreatDown corporate subscription plan has a varying annual fee per managed device, depending on the selected set of features and the level of support.
- **Single payment** – The software requires a single one-time payment for the usage license. This model has become relatively uncommon.
- **Usage-based pricing** – The cost depends on the amount of resources used by the team. This is typically used in Public Cloud environments, where the actual cost of using a cloud service depends on the consumption of underlying cloud resources (e.g. Virtual Machines, storage space, network bandwidth).

- Example: The Amazon AWS Inspector price depends on number of EC2 instance hours, assessments, container images scanned, etc.
- **Dynamic pricing** – When the pricing depends on factors that are not known ahead of time to the client. It typically varies based on the size of the organization, but may be largely up to negotiation.
 - Example: Sprinto – recurring annual fee depends on the size of the client organization, number of regions, and the complexity of infrastructure.

Pricing models can often be hybrid, combining the characteristics of other basic models:

- **Bundle pricing** – Combining multiple tools and services into a single package with a single price or subscription for the whole bundle. This makes it more difficult to estimate the comparative cost of a specific COTS tool.
- **Tiered pricing models** – A tool may offer different pricing options based on such criteria as the number of users, the set of required features, or data volume.
 - Example: Jira has four tiers: a free tier for small teams, user-based monthly standard and premium tiers, and a dynamically priced annual subscription enterprise tier for very large companies.

Selection criteria

In addition to licenses and cost models, there are many other features and characteristics to consider when deciding whether to adopt open-source or COTS tools. The aim of this section is to highlight the most important characteristics that should be considered when choosing between open-source and COTS tools, as well as infrastructure components, for building SOC platforms.

A study performed by Guilherme Avelino et al. [3] revealed that, among all open-source projects, only a small percentage receive consistent and timely updates, and there is always a risk of project abandonment. While this is less likely with widely used open-source tools, the frequency and duration of updates are especially important for security-critical software to keep pace with vulnerabilities and threats that are constantly being identified by the security community.

The study by Xiaozhou Li et al. [5] identified 8 main factors and 74 sub-factors that developers can consider when selecting between open-source software. The main factors and their corresponding sub-factors were:

- **Community support and adoption**
 - Popularity, Community reputation, Community size, Communication, Involvement, Sustainability, Product Team, Responsiveness
- **Documentation**
 - Usage documentation, Software requirements, Hardware requirements, Software Quality Documentation
- **License**
- **Operational SW characteristics**
 - Trialability, Independence from other SW, Development language, Portability, Standard compliance, Testability
- **Maturity**

- **Quality**
 - Reliability, Performance, Security, Modularity, Portability, Flexibility/Exploitability, Code Quality, Coding conventions, Maintainability, Testability, Existence of benchmark/test, Changeability, Update/Upgrade/Add-ons/Plugin, Architectural quality
- **Perceived risks**
 - Perceived lack of confidentiality, Perceived lack of integrity, Perceived high availability, Perceived high structural assurance, Strategic risks, Operational risks, Financial risks, Hazard risks
- **Trustworthiness**
 - Component, Architecture, System, OSS provider reputation, Collaboration with other products, Assessment results from 3rd parties

In addition to the factors, they also documented a set of KPIs that can be used to measure the level of each factor. For example, the maturity of an open-source project can be assessed by considering factors such as the number of software repository forks, release frequency, number of releases, project age, number of commits, development versions, and integration of new features. For the security factor, KPIs included the number of security vulnerabilities, the time taken to resolve vulnerabilities, community concern regarding security, and the impact of vulnerabilities. However, not all factors are directly applicable when selecting SOC tools, as new software is not typically developed from scratch.

When selecting SOC components, it is recommended to consider at least the following criteria in addition to the pricing model and license types:

- **On-premises deployment support** – Can the software be used on organization servers? Can data be stored on-premises?
- **Availability as SaaS** – Can the software be used as an existing cloud service without the need for deployment efforts?
- **Release frequency** – Indicates how often the software receives updates.
- **Documentation quality** – How detailed and well-written is the documentation? Does the documentation include all necessary details, such as hardware requirements, deployment templates, manifests, etc.?
- **Number of vulnerabilities reported** – How many critical issues and vulnerabilities have been reported in recent periods? How quickly are these critical issues and vulnerabilities fixed?
- **Age of the tool** – indicates whether it is mature and how long it has been available for the users to test.
- **Size of the community** – indicates the extent to which the user community has adopted the software and how extensively the solution has been tested by the users.
- **High Availability (HA)** – whether and how well the software is designed to handle failures without disruption.

- **Audit log availability** – Does the software generate a security-relevant chronological log of events, such as the creation of new users, changes to permissions, policies, etc.?

Conclusions

This section has provided an overview of the key characteristics that should be analyzed when choosing between open-source or commercially available off-the-shelf (COTS) tools for designing the SoC platform. The selection criteria, including licensing conditions, cost models, frequency of security updates, customization, and other factors have been discussed. The available COTS tools and their open-source counterparts are further outlined and analyzed in other sections of this chapter.

References

- [1] Open-source licenses, <https://opensource.org/licenses/> [Last visited: 16th January 2025]
- [2] GNU Operating System, “Various Licenses and Comments about Them”, <https://www.gnu.org/licenses/license-list.html> [Last visited: 16th January 2025]
- [3] Avelino, G., Constantinou, E., Valente, M. T., & Serebrenik, A. (2019, September). On the abandonment and survival of open source projects: An empirical investigation. In 2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM) (pp. 1-12). IEEE
- [4] Fred Bals, “Top open source licenses and legal risk for developers”
<https://www.synopsys.com/blogs/software-security/top-open-source-licenses.html> (26.04.2024)
- [5] Li, X., Moreschini, S., Zhang, Z., & Taibi, D. (2022). Exploring factors and metrics to select open source software components for integration: An empirical study. *Journal of Systems and Software*, 188, 111255

6.3. SIEM, SOAR, EDR, XDR

The SOC team uses a variety of tools to support its operations. Crucial to the operation of the SOC are systems designed to collect, analyse, and correlate information. These systems include, among others, the following classes: SIEM, SOAR, EDR, XDR.

SIEM

Security Incident and Event Management - systems responsible for collecting, analyzing and storing a large amount of data from the entire organization's environment. The analysis process involves managing the data, matching it to predefined patterns, or enriching it with additional information (e.g. IOC indicators). The task of SIEM systems, unlike the others on this list, is not to take automatic actions. They only serve as analytical tools. SOC teams, using SIEM systems, gain enhanced visibility into the activities within the infrastructure of the institutions they protect. In some cases, SOC teams can prevent more advanced attacks by detecting them during the reconnaissance stage.

There are many SIEM-class systems available on the market. Some of them are paid,

while others are offered free of charge. Examples of SIEM-class systems include Splunk, ElasticStack, and OpenSearch.

Splunk

Splunk is one of the leaders in SIEM solutions. It is software developed by Splunk Inc., a company headquartered in the United States. Recently, this company has been acquired by another American company: Cisco Systems, Inc. This software contains all the functionality expected from a SIEM-class system: it serves as a log aggregator, enables the viewing of logs both historically and in real time, allows for correlation queries and alert generation, features a module for recording and handling incidents, supports log enrichment with information from external sources, and offers a comprehensive list of ready-to-use SIEM views provided by solution vendors. Splunk offers granularity of user privileges by means of restricting access to system functionality, but also restricting users from accessing logs from specific systems. The system also supports the use of Machine Learning. Splunk enables the generation of charts, data aggregation tables, dashboards, and reports. This SIEM system offers licensing based on the amount of data written per day, the number of queries, or the number of log sources.

Elastic Stack

Elastic Stack is a solution developed in 2010 by Elastic NV. The main components of the solution are the search engine Elasticsearch, the data visualization interface Kibana, and the log collection interface Logstash. Initially, the solution was known as the ELK Stack (Elasticsearch Logstash Kibana Stack). Elastic Stack is available in a free version (which lacks many functionalities typically associated with a full SIEM system, but can be extended with additional free plugins to overcome some of these limitations), and a paid version (having all functionalities of a SIEM-class system). It offers a number of ready-to-use, official parsers, allowing you to extract specific information from logs and save it in a key-value form. In the absence of official support for a solution, a large community of Elastic Stack users often share their parsers. The free version of the solution does not include such functionalities as auditing user operations, integration with SSO systems for system logging, report generation, event alerting, and Machine Learning capabilities. Currently, the solution is developed by a company headquartered in the United States. In 2021 (starting with version 7.11), the solution changed its licensing rules, which required many existing implementations to switch from the free to the paid version. Today, Elastic Stack is licensed based on the resources used, with the licensing model applying to both cloud and on-premises deployments. Due to its open-source nature, many other SIEM-class solutions are built upon Elastic Stack's code.

OpenSearch

Open Search is a solution that was developed by cloning (forking) Elasticsearch and Kibana in 2021 (a clone of the last version of Elasticsearch licensed under the previous open-source model – 7.10.2) by Amazon. Since then, OpenSearch has been developed as a standalone product, consisting of OpenSearch – a search engine, and OpenSearch Dashboards – a data visualization interface. The solution is maintained as free, open-source code. During its development, most of the functionality that was previously only available in the paid version of Elastic Stack was added to OpenSearch. Thus, by using OpenSearch, users gain access to such features as generating and sending alerts for detected events, Machine Learning capabilities, and audit logs. The solution is a good alternative for SOC teams looking for a free SIEM solution. OpenSearch also has many forks and solutions that are built upon it. One of them is Log2Logic, created by a Polish company. It offers all the functionalities provided by OpenSearch. However, due to its

parallel development with OpenSearch and dedicated support, Log2Logic is a paid product. This solution is a good balance between the benefits of free and paid solution.

SOAR

Security Orchestration & Automated Response - systems designed to create and execute playbooks that automate activities. SOAR systems usually use APIs to communicate with other systems. Many security professionals consider SOAR systems as the perfect complement to SIEM systems. SIEM systems focus on collecting and analyzing events, generating incidents to which SOAR systems automatically respond. For this reason, some SIEM solutions introduce SOAR functionalities into their offerings. Examples of SOAR solutions include Cortex SOAR, Sentinel SOAR, and Shuffle.

Cortex SOAR

Cortex SOAR is an advanced solution from Palo Alto Networks that enables automation of security processes, integration of different tools, and faster incident response. Its architecture is cloud-based, but on-premises deployment is also possible, allowing greater flexibility depending on the needs of the organization. Cortex SOAR stands out for its extensive integration with other security systems, so that even complex processes can be automated. The main advantage of the solution is its high scalability and support for multiple teams (SOC) in different locations. The platform provides extensive capabilities for creating and managing 'playbooks' that define automated responses to security threats. With advanced reporting and analytics capabilities, Cortex SOAR enables better monitoring and optimization of security operations. Integration with other Palo Alto products, such as firewalls and Threat Intelligence solutions, further enhances its effectiveness. Cortex SOAR is primarily targeted at large enterprises and organizations with developed security management needs.

Sentinel SOAR

Sentinel SOAR is an embedded product within Microsoft Sentinel, a comprehensive SIEM (Security Information and Event Management) platform running in the Azure cloud. This paid solution enables the orchestration of security processes and automated response to threats. Sentinel SOAR integrates with the Microsoft ecosystem, as well as with a range of external solutions, providing extensive customization options for organizations. A distinctive feature of Sentinel SOAR is its deep integration with Azure cloud services, meaning that all operations are performed in the cloud. It offers pre-built automation templates as well as the ability to create custom ones, enabling users to respond quickly to security threats. Microsoft also relies on artificial intelligence and machine learning in Sentinel SOAR for predictive threat detection. The use of cloud resources allows the solution to scale quickly, making it an ideal solution for large organizations with distributed IT resources. Sentinel SOAR is a solution that will primarily be appreciated by organizations already using the Microsoft ecosystem, but will also work well in more complex environments thanks to its extensive integration.

Shuffle

Shuffle is an open-source solution offered by Shuffle Automation, Inc., designed to automate security operations and incident response. The product can be run both in the cloud and locally, offering flexibility to suit various types of environments. Shuffle stands out for its ease of use and lack of advanced coding, making it affordable even for smaller security teams with limited technology resources. The core part of the system is available for free under an open-source model, which is a huge advantage, but paid versions with

additional functionalities, such as advanced integration features and technical support, are also offered. Shuffle allows users to easily create automation 'playbooks' that integrate with popular security tools as well as IT systems. The system features a high degree of flexibility and openness, providing users with full control over their automation processes. Thanks to its open-source nature, combined with its wide integration support, Shuffle can be an attractive alternative to the more expensive SOAR solutions available on the market, especially for small and medium-sized companies.

EDR

Endpoint Detection and Response - systems designed to monitor endpoints for suspicious behaviour. These systems operate directly on the endpoint device, record every event and user activity, analyze the data, and if a threat is detected, automatically take action to stop any detected threats.

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint (formerly Microsoft Defender Advanced Threat Protection or ATP) is an advanced EDR solution designed to help enterprises detect, investigate, and respond to sophisticated cyber threats. It leverages a combination of behavioral sensors, cloud security analytics, and threat intelligence to provide real-time monitoring and response capabilities across endpoints. The strengths of Microsoft Defender lie in seamless integration with other Microsoft security tools, offering automated investigation and remediation features, comprehensive threat detection, and detailed incident response guidance. It empowers security teams to proactively hunt for threats, respond swiftly to incidents, and fortify their overall security posture. On the other hand, Microsoft support for older systems or non-Windows systems is limited.

Broadcom's Endpoint Detection and Response solutions

Broadcom's Endpoint Detection and Response solutions are the result of its enterprise acquisitions and are represented by Symantec Endpoint Security and VMware Carbon Black Cloud. The solution's main benefit is the support for a wide range of devices and operating systems, including mobile devices, virtual machines, and containers. It offers a comprehensive approach to endpoint security by continuously monitoring endpoint activity, and combining advanced threat detection, investigation, and response capabilities. It leverages machine learning, behaviour analysis, and integrated threat intelligence to identify and respond to sophisticated cyber threats, including advanced persistent threats (APTs) and zero-day attacks. The platform offers robust features for threat hunting, real-time incident response, and automated remediation, enabling security teams to quickly detect and neutralize threats before they can cause significant harm. Broadcom EDR integrates with other security tools within the Broadcom cybersecurity portfolio, enhancing overall threat visibility and optimizing security operations. Carbon Black Cloud also integrates threat intelligence to predict and prevent future attacks, helping organizations strengthen their overall security posture. Additionally, it offers seamless integration with VMware's broader security and IT management ecosystem.

ESET Enterprise Inspector

ESET Enterprise Inspector is a product from the EU CEE region, specifically Slovakia, from a company with over 30 years of experience in cybersecurity. It offers advanced threat detection, investigation, and response capabilities, making it suitable for businesses of all sizes. It provides real-time visibility into endpoint activities, using behaviour-based

detection and machine learning to identify and mitigate sophisticated threats, including zero-day exploits and APTs. The solution enables security teams to perform in-depth threat hunting, analyze incidents with detailed context, and automate response actions to minimize potential damage. ESET's EDR integrates seamlessly with the broader ESET security ecosystem, offering a lightweight, efficient, and highly customizable platform that empowers organizations to maintain a robust security posture against evolving cyber threats.

XDR

Extended Detection and Response - These systems build upon the functionality of EDR solutions. XDR systems extend EDR functionality by detecting and analyzing information from networks, servers, the cloud, and other security layers. XDR systems automatically collect and correlate data from multiple vectors, which enables them to detect threats faster and more accurately. Some examples of XDR systems include CrowdStrike Falcon, SentinelOne Singularity, and Wazuh.

SentinelOne Singularity

SentinelOne Singularity is a managed, commercial XDR cloud platform that aims to provide end-to-end visibility across enterprise system endpoints, real-time data analytics, security event detection, and automated security responses throughout the entire technology stack. The main features that elevate SentinelOne Singularity into an XDR solution include integrated threat intelligence, where it utilizes both its own intelligence and third-party security event and incident feeds. This enhances endpoint incidents by providing real-time threat intelligence and up-to-date indicators of compromise (IoCs). Security actions and responses can be automated using Singularity API and Customizable Workflow, which can be triggered by alerts to auto-enrich data, add context to events, quarantine compromised endpoints, or perform other remediation actions. Singularity Marketplace contains a set of integrations to provide access to third-party applications and services, and to design more complex analytics and orchestrated response pipelines. The marketplace is deployed as a Function-as-a-Service (FaaS) cloud platform, and integrations can be quickly deployed as cloud-native serverless functions. SentinelOne Singularity's relatively high price is often raised as a disadvantage. While relatively few false positives are often highlighted as a significant advantage, SentinelOne Singularity tends to block some legitimate processes. As a result, it requires fine-tuning and the setup of custom exclusion rules after deploying agents.

CrowdStrike Falcon

CrowdStrike Falcon is a popular commercial XDR cloud platform that is known for its ease of deployment and configuration, and wide platform availability. Its protection is built upon monitoring the system and processes, detecting anomalous processes through machine learning, Indicators of Attack (IOA), and 24×7 managed hunting. CrowdStrike endpoint agent will actively terminate or pause processes that are classified as malicious based on their activity. The agent is also protected against uninstallation and requires a cloud-backed security code before it can be removed from the system. Falcon supports a wide range of endpoint types, including Windows, Linux, and Mac workstations, as well as cloud instances and containers. Falcon features a marketplace where partner companies can offer services that integrate with third-party tools and solutions, for example, offerings for additional analytics, threat intelligence, identity security, as well as risk management and insurance. One of its unique features is the

ability to simulate policies in order to estimate and visualize the effect of security scenarios. Policies configured as 'simulated' will generate logs and alerts based on the live system, but will not actually trigger any defense actions, which allows security analysts to quickly evaluate the impact of new security policies and test "what if" situations before fully enabling the rules. As a disadvantage, Falcon is considered to be more expensive than other commercial XDR platforms. There have also been complaints of low transparency of pricing. In the summer of 2024, CrowdStrike faced significant criticism following the CrowdStrike Windows Glitch of July 19, 2024, when a large number of Windows machines failed to boot after a CrowdStrike software update, which caused major service disruptions in critical systems, such as those in hospitals and airports. While this was primarily a software development, validation, and deployment issue rather than a security incident, it highlights the fact that relying entirely on a closed commercial solution can make it challenging for an organization to self-validate deployments and resolve time-critical issues independently.

Wazuh

Wazuh is an open-source XDR platform that supports both self-hosted and cloud-managed deployments. Wazuh provides a set of classical EDR endpoint security features, such as malware detection, log analysis, threat hunting, configuration assessment, and file integrity monitoring. However, by running a managed Endpoint Detection and Response service, Wazuh can leverage globally detected security events and knowledge to offer extended features and services to all Wazuh users, providing protection against ever-evolving security threats and transforming it into an XDR platform. Wazuh supports major cloud providers (e.g. Google, Azure, AWS), and is capable of detecting and monitoring virtual machines, cloud instances, as well as Docker and Kubernetes containers. One of the key advantages of Wazuh is its ability to collect logs and telemetry from a wide spectrum of sources. For example, it includes native support for analyzing cloud logs and data from Pub/Sub messaging services. It also supports analyzing GitHub and Office 365 logs for the purpose of detecting security events and threats. Another key feature is the ability to automate responses to security incidents. The organization's security team can define Wazuh's custom active response actions and configure their triggers accordingly. Such actions can be written in any programming language. In the case of self-hosting, an organization can manage the whole deployment or pay for professional support, in which case the provider maintains the system and provides 24/7 assistance. In the case of cloud-managed deployments, the organization is required to install Wazuh agents, while the rest of the components are managed by the provider. As an open-source platform, Wazuh offers excellent transparency and extendibility compared to fully commercial XDR platforms, and it also benefits greatly from community support.

Table 1 SIEM solutions: comparison table

Feature	Splunk	Elastic Stack	OpenSearch
Implementation model	On-premises/Cloud	On-premises/Cloud	On-premises/Cloud
Licensing	Subscription	Free and Subscription	Free and Subscription
Open-Source	No	Yes	Yes
Release frequency	Quarterly	Regular (approximately every few months)	Regular (approximately every few months)
Vulnerabilities reported	Approximately 1-2 per year	Approximately 1 per year	No data
Age	>20 years	13 years	2 years
Community size (in thousands)	20+	100+	Data not available
Roles and permissions	Yes	Yes (with X-Pack)	Yes
Integrations with other security solutions	Yes	Yes	Yes
Integrations with CTI sources	Various, including STIX/TAXII	Various, including STIX/TAXII	Various, including STIX/TAXII
API	Yes	Yes	Yes
High Availability (HA)	Yes	Yes	Yes
Notifications	Alerts via email, SMS, webhooks	Alerts via email, webhooks (with X-Pack)	Alerts via email, webhooks
Reports	Yes	Yes	Yes
Event management	Yes	Yes	Yes

Audit logs	Yes	Yes (with X-Pack)	Yes
Machine learning	Yes	Yes (with X-Pack)	Yes
Unified meta key names	Yes	Yes	Yes
Work areas	Yes	Yes	Yes

Please note that the availability and extent of features may vary based on specific configurations, versions, and licensing tier.

Table 2 SOAR solutions: comparison table

Feature	Cortex SOAR	Microsoft Sentinel	Shuffle
Implementation model	On-premises/Cloud	Cloud	On-premises/Cloud
Licensing	Subscription	Subscription	Free
Open-Source	No	No	Yes
Release frequency	Quarterly	Continuous	Continuous
Vulnerabilities reported	Approximately 1-2 per year	No data	No data
Age	4 years	4 years	3 years
Community size (in thousands)	Data not available	Data not available	Data not available
Roles and permissions	Yes	Yes	Yes
Integrations with security solutions	Yes	Yes	Yes
API	Yes	Yes	Yes
High Availability (HA)	Yes	Yes	Yes
Notifications	Email, SMS, Webhooks	Email, SMS, Webhooks	Email, Webhooks
Reports	Yes	Yes	Yes
Incident management	Yes	Yes	Yes
Audit logs	Yes	Yes	Yes
Machine learning	Yes	Yes	No
Automated responses	Yes	Yes	Yes

Please note that the availability and extent of features may vary based on specific configurations, versions, and licensing tiers.

Table 3 - EDR solutions: comparison table

Feature	Microsoft Defender for Endpoint	Broadcom's Endpoint Detection and Response (Symantec)	ESET Enterprise Inspector
Implementation model	On-premises/Cloud	On-premises/Cloud	On-premises/Cloud
Licensing	Subscription	Subscription	Subscription
Open-Source	No	No	No
Release frequency	Continuous updates	Approximately quarterly	Approximately quarterly
Vulnerabilities reported	No data	Approximately 1-2	No data
Age	12	8	5
Community size (in thousands)	Data not available	Data not available	Data not available
Roles and permissions	Yes	Yes	Yes
Integrations with security solutions	Yes	Yes	Yes
API	Yes	Yes	Yes
High Availability (HA)	Yes	Yes	Yes
Notifications	Email, SMS, Webhooks	Email, SMS, Webhooks	Email, SMS, Webhooks
Reports	Yes	Yes	Yes
Audit logs	Yes	Yes	Yes
Machine learning	Yes	Yes	Yes
Integrations with CTI Sources	Yes	Yes	Yes

Please note that the availability and extent of features may vary based on specific configurations, versions, and licensing tiers.

Table 4 XDR solutions: comparison table

Feature	SentinelOne Singularity	CrowdStrike Falcon	Wazuh
Implementation model	On-premises/Cloud	Cloud	On-premises/Cloud
Licensing	Subscription	Subscription	Free
Open-Source	No	No	Yes
Release frequency	Continuous updates	Continuous updates	Continuous updates
Vulnerabilities reported	No data	No data	No data
Age	10	12	7
Community size (in thousands)	Data not available	Data not available	Data not available
Roles and permissions	Yes	Yes	Yes
Integrations with other security solutions	Yes	Yes	Yes
API	Yes	Yes	Yes
High Availability (HA)	Yes	Yes	Yes
Notifications	Email, SMS, Webhooks	Email, SMS, Webhooks	Email, SMS, Webhooks
Reports	Yes	Yes	Yes
Audit logs	Yes	Yes	Yes
Machine learning	Yes	Yes	Yes
Integrations with CTI Sources	Yes	Yes	Yes

Please note that the availability and extent of features may vary based on specific configurations, versions, and licensing tiers.

6.4. Asset Inventory Management

Introduction

A detailed, correct, and up-to-date description of the IT environment is necessary for situational awareness in cybersecurity. Asset (Inventory) Management Systems enable storing, updating, and reviewing environmental information and thus constitute an important database for cybersecurity. With a properly configured and maintained system, it is possible to visualize the layout of the environment (both virtual and physical), the configuration of its individual elements and the persons responsible for, or otherwise connected to them, at any time.

Challenges

The Asset Management System needs to cope with the following challenges:

- **Building and maintaining the inventory** – During deployment, all relevant elements and parts of the infrastructure must be entered into the system. Furthermore, the data within the system must constantly correspond to reality, so every change in the infrastructure necessitates a relevant system update. Manual maintenance and operation of the system are, therefore, difficult and prone to errors. Most state-of-the-art systems offer at least partial automation and error detection.
- **Coping with obsolete or inaccurate information** – Errors made during creation or maintenance may result in obsolete or inaccurate information appearing in the system. This could be more harmful than lack of any information as it may, for instance, create a false sense of security when running a vulnerable service not documented in the asset inventory.
- **Providing human and machine-readable data** – Asset inventory often serves as a data source for other organizational security systems and processes. The system should therefore provide content in both structured and human-readable formats.

University environments add their own specific challenges to the common ones listed above.

- **Large and open environment** - Universities bring together a large number of different categories of people, such as students, lecturers, researchers, together with non-teaching staff and management. Setting up an environment that would meet the requirements of all distinct groups of users and at the same time offer sufficient performance and security level is a complex issue.
- **Lax policies** - The university IT environment is diverse and at the same time strives to support the free exchange of ideas. A configuration optimal for security might therefore not be as highly prioritized as it is in the commercial setting. University policies tend to be lax.
- **Lower internal coherence** - In the academic environment, some entities, e.g., successful research groups, enjoy a higher level of autonomy than other units.

They may require specific functionalities as well as direct administration of specific university assets, and they often execute rapid and unannounced changes with limited documentation. In the absence of documentation, changes to security-related asset configuration, performed as part of routine maintenance, may impact their operations in unexpected ways.

Requirements

When choosing an Asset Management System to be deployed, the university should consider in the first place:

- **Modularity** – The proposed system should be conceived as a set of interconnected tools (subsystems) with an integration layer that ensures data consistency across all involved tools and provides user comfort and options for modular expansion of functions with further advanced functions and/or subsystems.
- **Interfacing** – The integration layer serves as a single entry point for system users, while user interfaces for managing and registering the IT infrastructure will be provided directly through the interface of integrated specialized tools (subsystems). Specialized management functions that are not available in integrated tools or require the cooperation of multiple integrated tools will be called up and presented directly from the unified one-user interface of the integration layer, which minimizes the necessary modifications directly in the integrated tools. Interface integration has been outlined in Figure 1.
- **Open access** – The integration interface will be an open platform that will allow the addition of more tools according to stakeholder requirements for specific outputs as well as reports on asset management data and interconnected systems. The stakeholders for asset management include a wide range of university roles, like local (e.g., faculty) IT administrators, cybersecurity operators, and management.

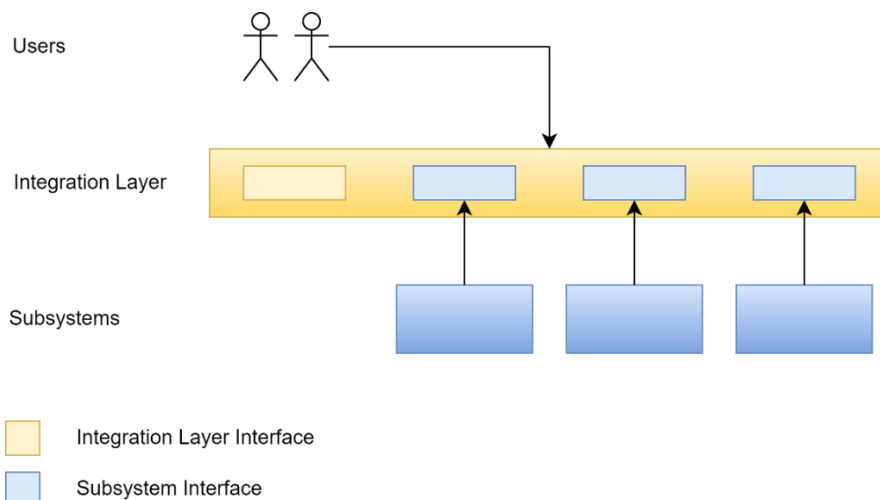


Figure1 Layout of the interfacing requirements; Asset Management System at MUNI

Subsystem for management and registration of IT infrastructure components

The responsibilities of the system deployed in a university environment focus primarily on the infrastructure, which is more prone to change in this environment than in a commercial setting. There are other devices like user stations, mobile devices, and

computer accessories. Here, the academic environment also differs from a commercial setting, where the central management of user devices is frequently enforced. Universities often promote a Bring-Your-Own-Device policy, and they rarely enforce central management even with regard to employee devices. However, user devices fall out of the scope of asset inventory, which generally focuses on static assets. The subsystem for management and registration of IT infrastructure components should include the following key elements:

- Management and registration of the internal components of the organization's IT infrastructure, including physical records of devices and how they are arranged in racks located in halls, connections between devices, the personnel in charge, and inventory numbers. This also includes passive elements such as racks, cabling, telephone networks, building management systems (BMS), cameras, and access security systems as key assets within property management.
- Registration and management of IP address ranges and individual IP addresses using IPAM (IP Address Management). DHCP and DNS connectors are also an important element of the subsystem as they ensure dynamic allocation and management of IP addresses.
- Administration and recordkeeping of virtualized infrastructure, which includes monitoring and management of virtual machines that constitute part of the IT infrastructure.
- Management and monitoring of connections and the technical condition of individual devices within the IT infrastructure, including monitoring of the system's electrical, heating and cooling performance.
- Management of software equipment and licenses that are linked to individual servers and end users. This record helps the organization maintain order and ensure legal use of software resources.

Automation subsystem

The automation subsystem has been designed to execute automated actions on a scheduled basis or in response to events in order to minimize routine and repetitive tasks. These automated actions should include:

- Data consistency checks to ensure that all data in the information system are updated, correct, and meeting the established standards. These checks minimize the risk of inconsistencies or errors in the data, which increases the reliability of the information system as a whole. Such measures prevent situations where a new device is connected to the network but not documented in the asset management system.
- Creation of overview visualization exports to provide users with quick and straightforward access to important information in the form of graphs, tables, or reports. Clear visualizations enhance user orientation and support faster and more informed decision-making. For example, automatic generation of a handover report or an IT loan agreement saves time and helps link these documents directly to specific assets.
- Data synchronization to ensure that data are correctly and reliably transferred across different parts of the information system. As the process is automated, manual intervention is minimized and potential human errors are eliminated,

which increases the overall data integrity and reliability. This is a crucial aspect for an asset management system, as otherwise it would contain faulty configurations that would further affect the system.

Integration layer

The integration layer serves as a unifying element ensuring data consistency across all of the subsystems within the entire solution architecture, which should enable seamless cooperation throughout the system. This layer should also provide space for the modular implementation of advanced functionalities, such as reporting, user and asset auditing, and dashboard creation. This design allows the system to be both expandable in its functionalities and adaptable to specific user requirements. The integration layer should enable seamless integration of other subsystems into the overall solution architecture, so that the system can quickly respond to the growing requirements and needs of the organization. Managing integrated tools within individual subsystems is also a key function of this layer.

Solutions

NetBox

NetBox is an OpenSource solution that was created to meet the needs of IT resource management. The main purpose of the application is to manage IP addresses allocated in the infrastructure and to oversee data center operations. The solution allows proper network management, device tracking and network visualization. Over time, as the application developed, a number of new functionalities have been added to it. Since NetBox is a free on-premises solution, it can be deployed directly within the organization's infrastructure. This tool can generate reports with a breakdown of the owned resources, provide control over users using the application and support API queries. Users can also configure event notifications to be sent by the application via various channels, such as email.

ServiceNow

ServiceNow is a U.S.-based solution for managing corporate resources, created by the company of the same name. The solution has been developed for the cloud, or as a separate instance running on the organization's resources. Currently, ServiceNow is a platform integrating a number of IT asset management products, including agent support, asset security functionality, and IT asset management automation. ServiceNow is a pay-as-you-go solution, offered in a subscription model, with several plans differing with regard to available functionalities. The solution enables its users, among other things, to create separate accounts with assigned roles, generate reports as well as send email and SMS notifications. ServiceNow can be deployed in the High Availability (HA) model, which provides resilience to failure of a single module. Due to its long market presence, ServiceNow is a well-established solution, adapted to the needs of many organizations.

Solarwinds

SolarWinds is an American company which manufactures a solution distributed under the same name. The solution was created to support management and monitoring of networks, systems and IT devices in organizations. The first version of SolarWinds was published as early as 1999, which makes it one of the longest available asset management solutions on the market. SolarWinds can be deployed in an organization in

both cloud and on-premises models, making it an affordable solution for entities that do not have in-house resources or competencies to maintain systems, as well as for those organizations that value greater privacy. The solution is available on a subscription basis and features a dedicated unit tailored to the specific needs of the public sector.

SolarWinds is a solution that is constantly being developed and improved. Regardless of the deployment model chosen, it supports duplication of systems, which enhances its failure resilience. It also features an API that enables automation and integration with other systems.

Asset Panda

Asset Panda is a cloud-based asset management platform developed by Rex Kurzius, an entrepreneur from the United States. Developed to address the challenges of efficiently tracking and managing assets, Asset Panda operates on a subscription-based model, providing a polished, commercial-grade product with dedicated customer support and continuous updates. By offering a Software-as-a-Service (SaaS) implementation model, Asset Panda eliminates the need for on-premises hardware or complex installations, allowing businesses to deploy and scale the platform with minimal overheads. The SaaS model ensures accessibility from any location, enabling teams to manage assets seamlessly across multiple locations using web browsers or mobile devices. The primary purpose of Asset Panda is to simplify asset management by providing organizations with tools to track, audit, and optimize the use of their physical and digital assets. One of the outstanding features of Asset Panda is its mobile app, which allows users to scan barcodes and QR codes for easy asset tracking and updates. This eliminates the need for expensive hardware scanners and ensures that asset data can be accessed and updated in real time. Asset Panda also provides comprehensive reporting and analytics capabilities. With customizable reporting options, organizations can gain insights into asset usage, depreciation, and maintenance costs, helping them make data-driven decisions. Notifications are another key functionality, enabling automated alerts for maintenance reminders, low inventory levels, or other critical events.

OCS Inventory

OCS Inventory (Open Computer and Software Inventory Next Generation) is a comprehensive and open-source IT asset management solution. It was developed by the OCS Inventory NG open-source community, originating in France, with contributions from various developers from around the world. OCS Inventory operates on an on-premises implementation model, and as such it is installed and hosted within an organization's infrastructure. This gives businesses full control over their asset management data, ensuring compliance with internal policies and regulatory requirements. The main purpose of OCS Inventory is to provide organizations with a centralized platform for inventorying and managing IT assets, including hardware, software, and network devices. It automates the collection of asset data across a network, enabling administrators to maintain a comprehensive inventory without manual effort. This capability is especially valuable for IT departments tasked with managing large numbers of devices and ensuring compliance with software licensing agreements. In addition to inventory management, OCS Inventory offers tools for software deployment and remote device configuration. Administrators can use the platform to push software updates or install applications across multiple devices simultaneously, streamlining IT operations. OCS Inventory integrates well with other IT and security tools, enhancing its value as part of a larger IT ecosystem. For example, it can be used in conjunction with vulnerability scanners to identify and remediate security risks across a network.

Table 5 SIEM solutions: comparison table

Feature	NetBox	ServiceNow	SolarWinds	Asset Panda	OCS Inventory
Implementation model	On-Premises	Cloud/On-Premises	On-Premises/Cloud	Cloud	On-Premises
Licensing	Free	Subscription	Subscription	Subscription	Free
Open-Source	Yes	No	No	No	Yes
Release frequency	Regular updates	Regular updates	Regular updates	Regular updates	Regular updates
Vulnerabilities reported (per year)	No data	No data	No data	No data	No data
Age	7 years	19 years	24 years	10 years	18 years
Community size (in thousands)	Data not available	Data not available	Data not available	Data not available	Data not available
Roles and permissions	Yes	Yes	Yes	Yes	Yes
API	Yes	Yes	Yes	Yes	Yes
High Availability (HA)	No	Yes	Yes	No	No
Notifications	Email, Webhooks	Email, SMS, Push Notifications	Email, SMS	Email, SMS	Email
Reports	Yes	Yes	Yes	Yes	Yes

6.5. Network Monitoring Tools

Introduction

The currently available state-of-the-art network monitoring solutions are mostly based on network flow monitoring instead of full packet capture. Network flow monitoring collects only metadata related to the monitored traffic, not the entire communication with the packet's payload. The metadata collected from several packets is aggregated into so-called flows that represent e.g. one TCP connection grouping common attributes such as source IP address and port, destination IP address and port. In contrast, a full packet capture stores full data, which requires significant storage and computing power, limiting the scalability on high bandwidth (100Gbps+) networks. Moreover, the traffic collected by a full packet capture has very limited additional usefulness, considering the fact that most of today's Internet traffic is encrypted by TLS, which prevents any in-depth analysis of packet payloads.

There are several different formats in which the flow data can be transported and stored, the most prominent of which are sFlow, Suricata, Netflow v9, and IPFIX. Of all these formats, the IPFIX is the newest and the most commonly used one. The most significant improvement to IPFIX over the Netflow v9 is that IPFIX IETF standard allows the addition of custom fields to the collected flow records.

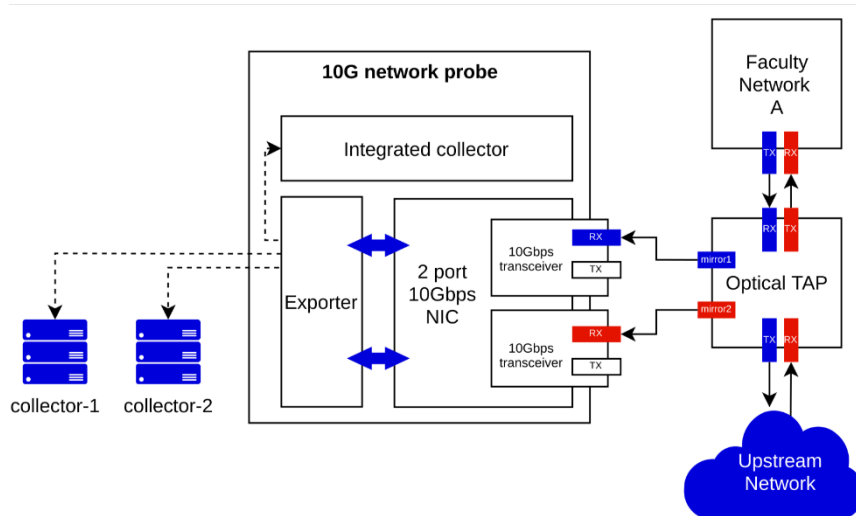


Figure 2 Visualisation of collecting NetFlow traffic

The flow data can either be generated by existing network appliances such as routers or switches, which leads to increased resource utilization of such devices and can result in lower network reliability, or by dedicated hardware, also known as a monitoring probe. Furthermore, the colocation of the flow data exporters and critical network infrastructure can lead to vulnerabilities, and in the case of an incident, the network monitoring is likely to be lost at an early stage. Independent network monitoring probes are a prerequisite for reliable collection of network flow data. The probes utilize TAP (traffic access points) to mirror the traffic on the link.

Traffic access points can be active, passive, metallic, or optical. Passive optical TAPs are the preferred variant as they do not contain any electronic components and work on a

purely optical basis. Power outage in a TAP location and the adjacent probe does not affect the normal communication on the monitored network link. An example of this configuration has been illustrated above.

Network monitoring tools

Flowmon

Flowmon provides network traffic monitoring solutions through two main agendas, namely Flowmon Monitoring Center (FMC) and Anomaly Detection System (ADS).

Flowmon FMC

Flowmon FMC is a user interface designed to provide an overview of information about the current state of collector activity and to offer a better understanding of the organization's network traffic, visualized by particular data sources, i.e. all active probes or their subset. In addition, FMC allows a more in-depth analysis of flows within 5-minute intervals through more complex filters, using query language syntax similar to the well-known pcap library used by *tcpdump*. An example of the FMC Analysis part has been illustrated below, with a query input field shown in the bottom part of the picture.



Figure 3 Example of view from FMC Analysis GUI

Flowmon ADS

Flowmon ADS is a security solution used to detect anomalies hidden in the network traffic, which complements traditional signature and rule-based detection approaches like firewall, IDS/IPS, or antivirus focusing on perimeter and endpoints. Unlike IDS systems and SNMP monitoring, Flowmon ADS monitors the overall behavior of devices on the network to detect and respond to previously unknown or specific threats.

Flowmon ADS provides a variety of predefined detection methods for protocol data traffic anomalies (DNS, SSH, and others), network attacks (port scanning, dictionary attacks, DDoS), unwanted applications or configuration issues, communication with

botnet hosts or other suspicious hosts that may distribute malware, and more. These methods can be easily enabled and used, generating events directly within the platform or sending them to a pre-defined endpoint, such as a ticketing system used by the security team to address security incidents. Flowmon ADS uses straightforward logic in individual detection methods, primarily based on a pre-set threshold limit control, such as the number of SSH attempts while connecting to the monitoring hosts. Therefore, it is an ideal solution for smaller networks with less variability of network devices and their types. However, correlation or combination of the outputs of the individual methods is not possible here.

Suricata

Suricata is an open-source network monitoring system that provides intrusion detection (IDS), intrusion prevention (IPS), and network security monitoring (NSM). Designed for real-time analysis and detailed packet inspection, it is capable of examining network traffic at multiple layers (up to the application layer, L7). Suricata detects threats through a combination of signature-based and anomaly-based methods, which enables the identification of any known vulnerabilities, patterns and unusual behavior indicative of potential threats.

One of Suricata's strengths is its ability to perform **deep packet inspection**, capturing rich metadata and even application-level information, such as HTTP requests and DNS queries. It also supports **multi-threading**, which improves performance on high-traffic networks. Suricata logs data in formats like JSON, which integrates well with external tools for advanced threat analysis, correlation, and reporting. Its extensive configurability makes it suitable for environments where security and detailed traffic analysis are priorities.

Snort

Snort is an open-source network intrusion detection and prevention system (IDS/IPS) developed by **Cisco Systems**. It monitors network traffic in real-time, analyzing packets to detect and block suspicious activities such as intrusions, malware and policy violations.

Snort uses a rule-based language to define attack patterns and supports customization for specific network environments. It can operate in multiple modes, including packet logging, real-time intrusion detection and inline prevention, making it a versatile tool for network security. Widely used for its efficiency and flexibility, Snort is a key component in many security setups.

Zabbix

Zabbix is an open-source network monitoring tool designed to track the performance, availability and health of network devices, servers, applications, and services. It collects metrics in real-time using various methods like SNMP, IPMI and agent-based monitoring.

Zabbix features robust alerting, customizable dashboards and data visualization capabilities, enabling users to quickly identify and respond to problems. Its scalability and flexibility make it suitable for small to enterprise-level environments. Supporting automation and extensive integrations, Zabbix is a powerful solution for comprehensive network monitoring.

NEMEA

NEMEA (Network Measurements Analysis) is an open-source framework developed by CESNET for real-time network traffic analysis and security monitoring. It uses a modular architecture, where each module performs specific tasks such as data preprocessing, anomaly detection or alert generation. These modules work together to process flow data and detect security incidents like DDoS attacks, botnet activity and data exfiltration.

The framework is highly scalable and supports distributed deployments, making it suitable for large-scale and high-throughput environments. NEMEA is extensible, allowing users to add or customize detection modules in order to meet specific security needs. It generates detailed alerts that can be integrated with incident response systems or stored for further analysis. NEMEA is widely used for network monitoring, threat detection and security research.

PRTG (commercial solution)

PRTG Network Monitor, developed by Paessler, is a comprehensive monitoring solution designed to manage and monitor network performance, applications, and systems in real time. PRTG uses a sensor-based approach, with each sensor monitoring a specific parameter, such as CPU usage, bandwidth or application status. It supports a wide variety of monitoring protocols, including SNMP, WMI, NetFlow, sFlow, and packet sniffing, which allows this tool to provide deep insights into both physical and virtual network environments.

PRTG features an intuitive web-based interface with customizable dashboards, alerting systems, and visualizations to simplify network management and troubleshooting. It is suitable for businesses of all sizes, and its modular, sensor-based licensing model allows scalability according to the organization's monitoring needs.

Arkime

Arkime is an open-source network capture and analysis tool designed for indexing, storing, and visualizing network packet data. **It captures raw packet data (PCAP files)** and enables efficient search and analysis of large amounts of network traffic. Arkime provides a web-based interface for exploring captured packets and offers powerful search capabilities, which allow security analysts and network administrators to investigate network activity, identify security incidents, and troubleshoot issues.

Key features of Arkime include:

- **Scalability** - designed to handle massive volumes of network traffic in large environments.
- **PCAP Storage** - storing captured packets in standard PCAP format, which allows integration with other tools.
- **Indexing and Search** - using Elasticsearch for indexing packet metadata, which enables fast searches across vast datasets.
- **Security Monitoring** - useful for threat hunting, incident response, and compliance, with features for filtering and isolating specific types of traffic.

- **Integration** - compatible with other analysis tools, such as Wireshark, and supports API integrations.

Arkime is particularly useful for security operations centers (SOCs) and cybersecurity teams for the purpose of tracking malicious activity, understanding network behavior, and maintaining long-term network data retention.

However, Arkime is not recommended for monitoring larger networks. As it captures entire packets, the resource requirements are much higher than for the tools that leverage NetFlow.

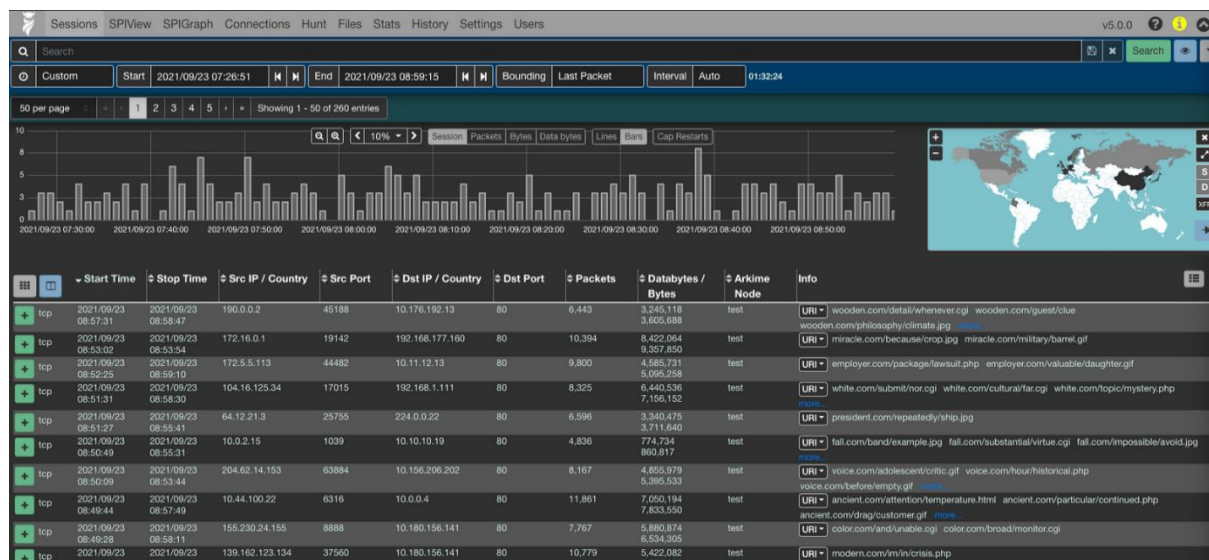


Figure 3 Example of view from Arkime GUI

Table 6 Network Monitoring Tools: comparison table

Feature	Flowmon	Suricata	Snort	Zabbix	NEMEA	PRTG Network Monitor	Arkime
Implementation model	On-Premises / Cloud	On-Premises	On-Premises	On-Premises / Cloud	On-Premises	On-Premises / Cloud	On-Premises
Licensing	Subscription	Free	Free	Free	Free	Subscription	Free
Open-Source	No	Yes	Yes	Yes	Yes	No	Yes
Release frequency	Regular updates	Biannual	Approximately quarterly	Approximately every six months	Irregular	Regular updates	Approximately quarterly
Vulnerabilities reported (per year)	No data	Approximately 1-2	Approximately 1-2	Approximately 1-2	No data	No data	No data
Age	14	15	25	18	10	22	10
Community size (in thousands)	Data not available	10+	100+	30+	Data not available	Data not available	Data not available
Roles and permissions	Yes	Yes	Yes	Yes	No	Yes	Yes
Integrations with other security solutions	Yes	Yes	Yes	Yes	Yes	Yes	Yes
API	Yes	Yes	Yes	Yes	No	Yes	Yes
High Availability (HA)	Yes	No	No	Yes	No	Yes	No

Notifications	Email, SMS, Webhooks	Email, Syslog	Email, Syslog	Email, SMS	Email, Syslog	Email, SMS, Webhooks	Email, Syslog
Reports	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit logs	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scalability	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Packet decryption	Yes	Yes	Yes	No	No	No	Yes

6.6. Incident management - Solutions review

There are two core types of functionalities that are essential in incident management. One of them is a ticket response functionality, which enables SOC teams to register information while an incident is being processed. The other functionality is the incident register – a resource where SOC can store information about every resolved incident and submit incident reports. This is also the functionality from which incident statistics will be generated. In many cases, a single solution can be used for both purposes.

Incident management solutions

OTRS (Znuny)

OTRS (Open-source Ticket Request System) is software used to manage requests received from internal and external clients. The system uses email as the main communication channel. In addition, the system allows the user to add notes to notifications or track any phone calls made. Even though a project called OTRS was terminated in 2020, a fork of the code was made at that time for future reference. Currently, the solution operates under the name Znuny and is distributed under GNU General Public License (GPL v3).

Notifications created in the system can be assigned to individual queues, which facilitates task management. Dependencies between notifications are possible. A ticket created in the system can be assigned to only one user. OTRS offers automatic PGP/GPG integration to sign, verify, and encrypt/decrypt messages directly in the interface without external tools, which can help security teams to exchange information about incidents. OTRS (Znuny) can also create reports on tickets with statistics based on selected ticket attributes, such as ticket age, ticket owner, priority, SLA, type. It provides some basic incident register functionalities, without covering their entire scope.

The solution is based on the Perl language and is only available in self-hosted version. Thanks to its modular design and open-source code, new functionalities can be added to the system.

With its functionalities, the tool can serve CSIRT teams to efficiently manage reports of suspected incidents or the actual incidents, yet it requires an additional solution to cover the incident register.

JIRA

Jira Service Management by Atlassian provides SOC teams with a flexible incident response tool designed for efficiently tracking, organizing and responding to security incidents. JIRA is a paid solution with pricing that varies based on the team size. Through integration with multiple communication channels, incidents can be logged and categorized according to urgency and impact. Each incident ticket in JIRA can be assigned a status, priority level and owner, enabling SOC analysts to monitor progress and respond to requests in real time. The platform also includes detailed workflows which help to streamline incident management from identification to resolution. Notably, JIRA's automation rules allow recurring tasks, such as ticket assignments or status updates, to be handled automatically, therefore reducing response times and potential errors. In addition to its incident response capabilities, JIRA also serves as an incident register solution. This function allows the team to maintain a detailed archive of

resolved incidents in order to create a comprehensive database for future reference. Each incident report stored in JIRA includes vital information such as resolution steps, affected systems and lessons learned. The search and filter functionalities make it easy to retrieve historical data, which is crucial for analyzing patterns and improving incident handling procedures. The system also facilitates generating incident statistics and reports, providing valuable insights into the effectiveness of the team. This record-keeping process supports compliance and governance requirements by ensuring that all incident documentation is retained and easily accessible. The tool's self-hosted and cloud versions support flexible deployment depending on security requirements. Integrations with other Atlassian tools and third-party applications make it versatile for complex environments, providing a well-rounded solution for incident tracking and resolution.

Request Tracker (RT)

Request Tracker (RT), developed by Best Practical Solutions, is an open-source ticketing system designed to track and manage requests, tasks and workflows. RT is free for on-premises deployments. In addition, Best Practical offers paid support for self-hosted deployments or cloud plans hosted by Best Practical. It is built primarily over e-mail communication, which allows easy contact and communication with the team. RT – like OTRS – offers automatic PGP/GPG integration.

The key advantage of RT is that it organizes requests into tickets which can be categorized, prioritized and assigned to teams or individuals with a detailed role-based access control (RBAC), thus allowing administrators to define what actions can be performed by different users, whether they are agents, requesters, or managers. Tickets include information such as request status, history, internal comments, and communication logs. RT also allows users to customize ticket workflows based on their specific processes and allows setting up automatic triggers, ensuring that tickets move smoothly through each stage of resolution. The system allows for the creation of custom ticket fields to capture specific data while tickets can be organized into different queues representing departments or request types.

The customization is further extended by custom scripts triggered by ticket actions. This feature can be used to send alerts (e.g., to the team's instant messaging platform), close tickets, assign them to specific queues or perform other automated tasks. Additionally, RT provides an API for integration with other systems, allowing teams to integrate RT into their existing IT infrastructure. RT has a large community of users who contribute plugins and extensions. These extend the functionality of the system, offering integrations with third-party software, enhanced reporting tools and additional workflow features.

The Hive

The Hive is a ticketing system designed specifically for security teams, developed by StrangeBee. It closely integrates with Cortex to enrich cybersecurity data (IoCs) with contextual information from many external sources as well as to perform some actions automatically. It also supports marking tickets with cybersecurity-specific tags, such as TLP or PAP.

The Hive offers flexibility in deployment, enabling organizations to set it up in ways that best suit their infrastructure and operational needs. The solution can be deployed in the on-premises model, on a standalone server, in cloud or as a Docker container. The Hive is distributed as a community version – free to use, but limited (e.g. number of users, import/export cases, LDAP/AD synchronization, some automated actions), or in the subscription model, with full support and unlimited functionalities. The Hive is also offered as Software as a Service (SaaS) with subscription plans.

The Hive allows users to create, track and manage incidents, but, unlike the previously

mentioned solutions, it is less oriented towards processing requests from customers or external entities (or communication in general). Instead, it assumes that tickets will be created by a SOC team or by dedicated internal automation tools. It is therefore more suitable for proactive SOC teams than reactive CSIRT teams. The Hive enables users to collaborate in incident analysis. In addition, users can generate reports and statistics from tracked incidents. They can also use automated reports or create their own custom report templates.

This solution appears to be a reasonable choice for SOC teams, but with no updates released over the last 2 years the project seems to have been terminated.

FIR (Fast Incident Response)

FIR (Fast Incident Response) is a tool created by CERT Société Générale for tracking and reporting cyber security incidents. The solution is made available under the GPL-3.0 license, which makes it a good free alternative to other solutions of this type. The application was developed to meet the needs arising from the tasks handled by CERT Société Générale unit. Written using Django, FIR is a tool that must be implemented on-site. It can be installed directly from source code published on GitHub, or from a prepared Docker image. The solution allows its users to track active and closed incidents, along with determining their criticality, assignment, type, etc. Unfortunately, the application has a closed set of fields/characteristics for incident description. Adding new fields (e.g. incident reporter contact information) requires changes to be made to the application code. The application also has a fairly powerful module for generating statistics and charts related to recorded incidents. This allows the incident response team to provide a graphical representation of the tasks performed by the team.

HESK

HESK (<https://www.hesk.com>) is an easy-to-use and free ticketing system created by Klemen Stirn in 2005 in Slovenia. This software is available as a free on-premises version and as a paid cloud-based service.

The solution simplifies the complex process of managing customer support and incident tickets, allowing users to effortlessly create, prioritize, and categorize cases. With its customizable interface, HESK provides a tailored experience for organizations, enabling them to define custom fields and personalize submission forms to suit their specific requirements. For teams handling high volumes of inquiries, HESK's automated ticket assignment ensures efficient workload distribution, while built-in features such as canned responses and a robust knowledge base reduce response times and empower customers with self-service solutions.

Collaboration and communication are central to HESK's functionality. The platform supports multiple users with role-based access, allowing secure information sharing and task assignment. Email notifications and real-time updates keep both support staff and customers informed, fostering transparency and timely responses. The system's response rating feature provides valuable feedback, enabling teams to refine their service quality and ensure customer satisfaction.

For organizations seeking deeper insights into their support operations, HESK offers comprehensive reporting and analytics tools. These features allow managers to track ticket resolution times, identify recurring issues and optimize processes based on data-driven insights. Visual representations of trends and metrics further enhance decision-making and strategic planning.

Table 7 Comparison table:

Feature	Znuny	JIRA	Request Tracker	The Hive	Fast Incident Response (FIR)	HESK
Implementation Model	On-Premises	On-Premises/ Cloud	On-Premises	On-Premises/Cloud	On-Premises	On-Premises/ Cloud
Licensing	Free	Subscription	Free	Free / Subscription	Free	Free
Open-Source	Yes	No	Yes	Yes	Yes	Yes
Release Frequency	Approximately quarterly	Approximately quarterly	Approximately annually	Approximately annually	Approximately annually	Approximately annually
Vulnerabilities reported (per year)	Approximately 1-2	Approximately 1-2	Approximately 1-2	Approximately 1-2	Approximately 1-2	Approximately 1-2
Age	22	21	24	7	7	19
Community size (in thousands)	10+	100+	10+	5+	1+	5+
Roles and permissions	Yes	Yes	Yes	Yes	Yes	Yes
Ticket management	Yes	Yes	Yes	Yes	Yes	Yes
Email handling	Yes	Yes	Yes	Yes	Yes	Yes
Email encryption	Yes	Yes	Yes	Yes	No	No
Integrations with other security solutions	Limited	Yes	Limited	Yes/limited in free version	Yes	No

Automatic ticket assignment	Yes	Yes	Yes	Yes	Yes	No
Incident reports	Yes	Yes	Yes	Yes	Yes	Yes
Custom fields in reports	Yes	Yes	Yes	Yes	Yes	Yes
Statistics	Yes	Yes	Yes	Yes	Yes	Yes

Availability of some features may depend on specific configuration, plugins or additional modules.

6.7. CTI sources, CTI sharing platforms

Introduction

Cyber Threat Intelligence (CTI) is a broad term referring to any information about potential or actual cyber threats as well as the process of its collection, analysis and dissemination. This information includes details of cyber threats, their capabilities, intentions and indicators of compromise (IOCs).

There are three levels of CTI that are commonly recognized: strategic, operational and tactical.

Strategic CTI focuses on high-level insights and long-term trends related to cyber threats. It helps senior management and decision-makers understand the broader threat landscape, anticipate future threats and develop proactive strategies to mitigate risks. It usually takes the form of text reports or articles.

Operational CTI deals with the mid-level details of emerging threats, such as threat actor tactics, tools and procedures (TTPs), ongoing attack campaigns or information about vulnerabilities.

Tactical CTI is the most technical level and also the one that is most commonly used by organisations. It focuses on short-term, technical details of individual attacks or attackers. It mostly consists of indicators of compromise (IoCs), such as malicious IPs, domains and file hashes. These can be directly used in SIEM tools, firewalls and IDS/IPS systems.

This document mostly focuses on tactical/technical CTI, but some examples of sources of strategic and operational CTI are also included.

Strategic and operational CTI

Exchanging higher-level, non-technical CTI is more closely related to communication methods and communities rather than software, and as such, it falls outside the scope of this solution review. Still, we provide some tips on where and how to obtain such information.

The publicly available information often takes the form of articles, blog posts, reports, etc., published on web pages of originating organizations. Presentations and in-person discussions at conferences, workshops and similar events can also serve the purpose of exchanging strategic and operational CTI. Lastly, on the operational level, mailing lists and similar communication channels are often used to exchange information among members of a community – often limited to a specific location (country) or sector. Some examples are given below.

GÉANT Academic Cybersecurity Newsletter – a monthly newsletter with links to various articles about cybersecurity issues in academia – caters mainly to the academic community. The service offers free subscription to everyone interested.

- Basic information: <https://connect.geant.org/2023/12/01/empowering-academic-security-introducing-geants-cybersecurity-news-for-academia>

- Archive and subscription: <https://security.geant.org/security-newsletter/>

Other sources and mailing lists are rather regional. For example, CESNET operates open mailing lists for exchange of information about current threats for its members as well as for a broader security community in the Czech Republic (including lists specific for e.g. hospitals). These lists are mostly populated with information about new vulnerabilities relevant to a community or sector, as collected, assessed and enriched by the CESNET-CERTS team, but other issues, e.g. related to ongoing campaigns, are sometimes discussed there as well.

Estonian Information System Authority Operational Cybersecurity Department (CERT-EE) monitors and analyses events in Estonian cyberspace and publishes daily assessments and monthly summaries. Anyone interested can subscribe to the Cyberspace newsletter for daily updates. CERT-EE also uses Mattermost to share current information on Estonian cyber scene as well as an instance of MISP to share data in a structured way. These services are, however, only accessible by invitation.

A Mattermost server for quick information exchange is also operated by CERT.LV for cybersecurity affiliated individuals in Latvia.

In the United Kingdom, members or customers of Jisc (UK's NREN) can join the Cybersecurity Community Group, which provides monthly, quarterly and annual threat reports, vulnerability notifications, a MISP sharing group and other CTI services.

Similar initiatives are likely available in many other countries as well, run by national CERTs or local NRENs. Readers are advised to look for similar services in their own countries.

Tactical CTI sources (IoCs)

The tactical CTI sources are mostly feeds (or “blacklists”) of Indicators of Compromise (IoCs) – malicious IP addresses, URLs, domains, file hashes, etc. There are many such feeds available for free, but they vary considerably in terms of focus (general or focused on a specific type of threat), size, coverage, level of detail (plain list of IoCs vs. detailed data for each entry), reliability and trustworthiness (some feeds are provided by well-known reputable organizations, others are anonymous with no information on the origin of the data). There are also many commercial providers of IoC feeds, some of which are probably of higher quality than the ones provided free of charge. Below we present a list of recommended free feeds and services providing IoCs or similar data:

List of CTI sources:

- **Spamhaus DNSBL blocklists**
 - <https://www.spamhaus.org/blocklists>
 - IoC type: IPv4, IPv6, domains, hashes
 - Threat type: spam, phishing, infected devices (separate lists for individual threat types)
 - Details: none
 - Data source: multiple proprietary methods/sources, details not known
 - Access: via [DNSBL](#); free for non-commercial use for small and medium-sized organizations ([terms of use](#) apply)
 - Potential uses: email filtering based on sender's IP address or message content.

- **Spamhaus Don't Route or Peer list (DROP)**

- <https://www.spamhaus.org/blocklists/do-not-route-or-peer/>
- IoC type: IPv4/IPv6 ranges (prefixes), ASNs
- Threat type: networks used solely for malicious purposes
- Details: none
- Data source: unknown/proprietary
- Access: downloadable JSON files
- Potential uses: blocking all traffic coming from malicious networks.

Note: More Spamhaus lists are available from the Spamhaus Technology company. To access the lists, users typically need a paid account. However, small non-commercial organizations may open accounts for free. ([more info](#)).

- **AbuseIPDB**

- <https://www.abuseipdb.com/>
- IoC type: IPv4, IPv6
- Threat type: various
- Details: yes (number of reports, categories, timestamps, numeric score (confidence of abuse)).
- Data source: crowdsourcing, reports can be freely submitted (subject to credibility of reporters), making this solution effectively a sharing platform.
- Access: Web UI and API for querying individual IPs; simple blacklist download (up to 10000 entries) available for free via API; more options available in paid plans
- Potential uses: checking suspicious IPs during triage; blocking traffic from IPs with high confidence of abuse (using downloadable blacklists).

- **Data from Abuse.ch**

- **ThreatFox**
 - <https://threatfox.abuse.ch/>
 - IoC type: IP:port, URL, hash, domain
 - Threat type: malware (C&C, delivery site, payload hash)
 - Details: date, malware type, threat type, tags, confidence level
 - Data source: crowdsourcing (contributions by users; reports by new users are manually vetted)
 - Access: via API or downloadable in multiple formats; free for any use (CC0)
 - Potential uses: detecting and blocking access to this type of IP: port combinations or URLs, detecting malware through hashing.
- **Malware Bazaar**
 - <https://bazaar.abuse.ch/>
 - IoC type: Hash
 - Threat type: malware
 - Details: malware family, delivery method, matching YARA rules, threat intelligence from various vendors, user comments
 - Data source: crowdsourcing (contributions by users, authentication via X is required)
 - Access: API or web UI for querying individual samples, downloadable lists of IoCs in CSV or as daily MISP events
 - Free for any use (CC0)

- Potential uses: malware detection/analysis
- **YARAify**
 - <https://yaraify.abuse.ch/>
 - IoC type: Hash
 - Threat type: malware
 - Details: list of matching YARA rules, number of sightings
 - Data source: repository of YARA rules (contributed by users and obtained from sources such as Malpedia), database of public scan results
 - Access: API or web UI
 - Free for any use (CC0)
 - Potential uses: scanning suspicious files for malware
- **PhishTank**
 - <https://www.phishtank.com/>
 - IoC type: URL
 - Threat type: phishing
 - Details: yes (timestamp, target organization, website online status check)
 - Data source: crowdsourcing, manually verified by multiple users
 - Access: search via web UI, download full list via API
- **Blocklist.de**
 - <https://www.blocklist.de/>
 - IoC type: IPv4
 - Threat type: attacking IPs (separate lists for different protocols/services; e.g. ssh, mail, apache and others)
 - Details: yes
 - Data source: attacks detected on Blocklist's servers and on servers of contributing users
 - Access: DNSBL, HTTP API, downloadable lists (CSV)
 - Potential uses: Blocking / reporting traffic from IPs.
- **CINS**
 - <https://cinsscore.com/>
 - IoC type: IPv4
 - Threat type: unspecified
 - Details: none
 - Data source: crowdsourcing (reports collected from users running [Sentinel IPS](#))
 - Access: downloadable blacklist
- **PSBL**
 - <https://psbl.org/>
 - IoC type: IPv4
 - Threat type: spam
 - Details: none
 - Data source: proprietary detection system (spam traps running [Spamikaze](#))
 - Access: downloadable (rsync) blacklist
- **SURBL**

- <https://www.surbl.org/>
- IoC type: URL, IP
- Threat type: malware, phishing (malicious or targeted websites)
- Details: none/unknown
- Data source: proprietary research, multiple third-party sources
- Access: Web-based lookup and DNSBL (free for non-commercial use), paid data feeds
- Potential uses: email filtering based on message contents
- **IBM X-Force Exchange**
 - <https://exchange.xforce.ibmcloud.com/>
 - IoC type: IP, URL, domain, hash
 - Threat type: various
 - Details: yes (numerous details depending on IoC type)
 - Data source: proprietary methods (IBM telemetry), third-party integrations
 - Access: Web UI and API for individual queries, downloadable data collections (STIX format)
 - 50 free queries weekly
 - Potential uses: checking information about IoCs, scanning files for malware

The above list is not exhaustive as there are numerous other sources of CTI or data potentially useful for SOC teams. For more information and tips we recommend the following resources:

- An extensive list of IP feeds with various statistics for individual feeds, by FireHOL: <http://iplists.firehol.org/>
- A curated list of threat Intelligence resources by Herman Slatman: <https://github.com/hslatman/awesome-threat-intelligence?tab=readme-ov-file#sources>
- A collection of APIs for OSINT automation curated by *cipher387*: <https://github.com/cipher387/API-s-for-OSINT>

Aggregation services

There are various services that aggregate CTI data from multiple sources. In many cases they are easier to use, compared to querying the original sources independently.

Selected examples of online services have been listed below:

- **NERD (Network Entity Reputation Database)**
 - <https://nerd.cesnet.cz/nerd/>
 - Database of malicious IP addresses aggregated from multiple sources.
 - Gathers data from Warden (CESNET's system for sharing alerts from tens of different IDS systems and honeypots), DShield, selected feeds at AlienVault Open Threat Exchange and many public blacklists.
 - Provides detailed information about each IP address, including its history.
 - API available on request.
 - Developed and operated by CESNET.
- **Valli MultiRBL**

- <https://multirbl.valli.org/>
- Searches hundreds of DNSBL blacklists for IP addresses.
- Available solely as a web interface, no API (for automation, one should query the blacklists directly)
- **Blacklist check at whatismyipaddress.com**
 - <https://whatismyipaddress.com/blacklist-check>
 - Looks up an IP address in around 80 DNSBL blacklists.
 - Available solely as a web interface, no API (for automation, one should query the blacklists directly)
- **URLVoid / IPVoid**
 - <https://www.urlvoid.com/>, <https://www.ipvoid.com/>
 - Provides basic information about domains and IP addresses, these are verified with various blacklists and reputation databases.
 - Free via web interface, API available (paid)

There are also tools that can be installed locally for the purpose of gathering CTI and IoC enrichment:

- **Cortex (part of The Hive Project)**
 - <https://github.com/thehive-project/Cortex/>
 - Cortex is an open-source tool designed to enrich and analyze IoCs through automation. It supports a wide range of analyzers (pre-built modules) that connect to external APIs and services to provide data on IP addresses, domains, hashes, and more.
 - Cortex is highly integrated with The Hive (a popular case management platform for security teams), but it can also be connected to MISP or function independently.
 - Key features include asynchronous processing of enrichment jobs, user-defined permissions for analyzers, and creation of custom analyzers using Python.
 - The tool is particularly useful for SOC teams looking to centralize and automate their IoC analysis workflows.
 - The tool is apparently no longer actively developed. We recommend IntelOwl for new teams.
- **IntelOwl**
 - <https://intelowlproject.github.io/>
 - Similarly to Cortex, IntelOwl is an open-source platform for IoC enrichment and threat intelligence analysis. It uses a large set of built-in modules (analyzers) to fetch and aggregate data from APIs of various online services, public databases and local resources.
 - Supported IoCs include file hashes, IP addresses, domains, URLs and more. IntelOwl can also analyze files using various malware analysis tools.
 - The tool offers a web interface, RESTful API, and CLI, making it adaptable to various operational needs.
 - IntelOwl's modular architecture allows users to configure the choice of analyzers to use, making it a highly customizable solution. It also supports automated workflows for handling high volumes of data.
 - It is actively developed and continuously improved.

- **YETI**

- <https://yeti-platform.github.io/>
- YETI (Your Everyday Threat Intelligence) is an open-source threat intelligence platform designed to collect, analyze, and share CTI.
- Unlike tools focused solely on IoC enrichment, YETI also serves as a CTI management platform, allowing users to define threat actors, campaigns, and TTPs. It is designed for both CTI and DFIR practitioners.
- It includes built-in enrichers that fetch data from external sources to provide context to observed IoCs. The platform supports integration with other tools and services for advanced analysis and reporting.
- YETI is ideal for teams seeking a comprehensive approach to both IoC enrichment and threat intelligence lifecycle management.

Those using MISP (described below) for storing and/or sharing CTI can also use it for enrichment. MISP Modules is an extensive set of modules that enrich IoCs with data from various threat intelligence sources, such as VirusTotal, PassiveTotal, and Shodan. The modular nature of MISP also allows users to create custom enrichers to address their specific needs.

CTI sharing platforms

MISP

MISP (Malware Information Sharing Platform & Threat Sharing) is an open-source platform designed to facilitate the collection, analysis and sharing of threat intelligence. Originally developed to support detection and mitigation of malware, MISP has evolved into a comprehensive platform for managing all types of cybersecurity indicators, events and contextual information.

The platform is widely adopted by security teams in both public and private sectors, including academia, government, and industry. It fosters collaboration among trusted parties, enabling efficient exchange of structured information about cyber threats. By doing so, MISP helps organizations improve their situational awareness and readiness to defend against malicious activity.

MISP supports a wide range of features, such as automated correlation of indicators, enrichment of data from external sources and visualization of relationships between threat elements. Its robust API allows seamless integration with other security tools, while its modular architecture accommodates additional functionality through plugins and extensions.

A key aspect of MISP is its emphasis on privacy and trust. The platform includes granular access controls which enable users to define how and with whom information is shared. This is of particular importance in academic environments, where confidentiality and compliance with data protection regulations are critical.

Overall, MISP empowers security practitioners to strengthen their defenses through collaboration and data-driven decision-making, making it an essential tool for building and operating a Security Operations Center (SOC).

AV OTX

AlienVault Open Threat Exchange (OTX) is a collaborative threat intelligence platform designed to empower organizations and security professionals with actionable threat data. Managed by AT&T Cybersecurity, OTX enables users to access, contribute and share insights into emerging threats, indicators of compromise (IOCs) and malicious activities. OTX is free to use, making it an accessible resource for security teams of all sizes. Users can sign up for an account to access the platform, browse publicly shared data and contribute to the growing pool of global threat intelligence. While the platform itself is free, integrations with premium services and tools may require additional licensing. OTX is available via web portal or API. This solution is fully hosted by AT&T. OTX is designed to integrate seamlessly with numerous security tools, enhancing their threat detection and response capabilities. Notable integrations include:

- **SIEM Systems:** integrates with solutions like Splunk and AlienVault USM for enriched security event correlation.
- **Endpoint Detection and Response (EDR):** provides IOCs for EDR platforms to improve malware detection and mitigation.
- **Threat Hunting and Analysis Tools:** supplies actionable intelligence to tools like The Hive and Cortex for investigative purposes.
- **Firewalls and IDS/IPS Systems:** shares malicious IP addresses, domain names and other IOCs to enhance perimeter defences.

OTX supports ingestion of CTI data from public and commercial Threat feeds as well as from communities. In summary, AlienVault OTX is a robust, community-driven CTI platform that empowers users with real-time threat intelligence and a collaborative network.

OpenCTI

OpenCTI is an open-source Cyber Threat Intelligence (CTI) sharing and analysis platform designed to help organizations centralize, analyze and share threat intelligence data effectively. Developed by the French National Cybersecurity Agency (ANSSI) and Luatix, OpenCTI enables collaboration among security teams, enhances situational awareness and supports proactive security measures against evolving cyber threats. It is distributed under the Apache 2.0 License, making it free and open for use, modification and distribution.

OpenCTI can be deployed as an on-premises solution, in a standalone server or in cloud. OpenCTI is delivered as docker images. The platform relies on modern technologies such as GraphQL for its API, Elasticsearch for indexing, and RabbitMQ for event management.

OpenCTI supports seamless integration with various tools and platforms, allowing users to incorporate threat intelligence into existing workflows and security operations. Key integrations include:

- **SIEM and SOAR Solutions:** connecting with platforms like Splunk, IBM QRadar, and The Hive to enrich incident response and security monitoring.
- **Threat Intelligence Feeds:** ingesting data from providers like MISP, AlienVault OTX, and external APIs to centralize threat intelligence.

- **Vulnerability Management Tools:** integrating with tools such as Nessus or OpenVAS to correlate threat data with known vulnerabilities in the environment.
- **Endpoint Protection and Firewall Solutions:** sharing actionable intelligence with EDR and firewall systems to improve defensive measures.

Additionally, OpenCTI's modular design allows organizations to develop custom connectors and integrations to cater to their unique requirements. OpenCTI supports ingestion of CTI data from STIX, MISP, public and commercial threat feeds and communities. OpenCTI is a powerful, flexible and community-driven CTI platform that integrates seamlessly with modern cybersecurity ecosystems.

Table 8 CTI sharing platforms: comparison table

Feature	MISP	AlienVault OTX	OpenCTI
Implementation model	On-Premises	Cloud	On-Premises
Licensing	Free	Free	Free
Open-Source	Yes	No	Yes
Release frequency	Approximately monthly	Regular updates	Approximately quarterly
Vulnerabilities reported (per year)	Approximately 1-2	No data	No data
Age	12	11	4
Community size (in thousands)	5+	100+	Data not available
Roles and permissions	Yes	Limited	Yes
Integrations with other security solutions	Yes	Yes	Yes
Integrations with CTI sources	Various open-source and commercial feeds	Community contributions and public threat feeds	Various open-source and commercial feeds
API	Yes	Yes	Yes

Availability and extent of features may vary based on specific configurations and versions.

6.8. Vulnerability assessment and scanning tools

Introduction

This document outlines a number of tools that can be utilized for vulnerability assessment and scanning. Academic SOC teams may prefer open-source tools over commercial ones due to their recruitment strategies and specific needs. Given that these SOC teams frequently collaborate with IT faculties, they have access to skilled personnel who can customize open-source tools to meet specific requirements. While commercial tools may offer fewer options for modifications, they typically offer a user-friendly interface and a shorter learning curve.

Vulnerability Scanning Tools

Nmap --script vuln

Nmap is an industry-standard port scanning tool. Its basic functionality is extended by the Nmap Scripting Engine (NSE), which divides scripts into several categories (Vuln, Vulners and Vulscan). Vuln is a category of scripts that checks for specific vulnerabilities and reports them if found. The tool actively validates vulnerabilities, thus allowing disruption of the integrity or availability of the target. Nmap Vulners uses additional resources about known services to provide data on vulnerabilities and links with more details. The script allows users to list known vulnerabilities of a given target with a corresponding CVE id and CVSS score. For vulnerability intelligence, <https://vulners.com/> is used. Another solution – vulscan – is an extension that allows scanning similarly to vulners, but it uses a downloaded copy of the vulnerability database instead of sending queries to a live database. This can be useful if the organization is concerned about the privacy of their environment and aims to avoid exposing any information to third-party databases. However, unlike the two previous scripts, vulscan is not included in the Nmap official distribution and needs to be downloaded separately.

Greenbone (OpenVAS)

OpenVAS - a free network scanner - is a very good alternative to Tenable's popular paid solution - Nessus. All functionalities offered by Greenbone are available for free. However, to increase the quality of the scans, additional feeds (i.e. vulnerability tests) can be purchased. OpenVAS performs a scan of a specified area of the network in search of shared services with the option of performing unauthenticated or authenticated vulnerability identification on the detected services. Vulnerability feeds are updated daily and the solution itself has been in continuous development since 2006. With free access, it is a very good alternative to other paid network scanners.

Nessus

Nessus is a paid network scanner released by a US company Tenable. Its main task is to scan a preset area of a network for services hosted within it and subsequently verify

whether the detected services are vulnerable to any known attacks. Nessus is the leading solution of its kind on the market. The first part of the process (identification of services) is performed using the Nmap tool, while the second part (vulnerability check) is carried out using an extensive database of plug-ins containing vulnerability information. For better accuracy of the scan, users can provide access data to shell accounts on analyzed systems in the scan settings or use agents installed on servers, which collect real-time data on the system and services running on it. In addition, by installing the appropriate components, Nessus also enables automatic auditing of web applications. The results of the scan are presented in the form of an extensive report containing not only information about services and vulnerabilities, but often also indicating how a given vulnerability can be removed or suggesting how to verify whether the vulnerability actually exists. The report from such a scan can be exported to various formats – including PDF.

Nessus is available as a Cloud (SaaS) version and as a solution installed on the user's own infrastructure (on-premises). It can be deployed on operating systems from the Windows, Linux or Mac OS families.

Shodan

Shodan is a search engine that indexes internet-connected devices, including servers, routers, webcams, and IoT devices. Shodan's scanning process systematically indexes the internet by actively probing public-facing devices and services. In the context of vulnerability scanning, Shodan can be used for:

1. discovering exposed services: identify devices and services exposed to the internet that may be improperly configured or vulnerable.
2. searching for known vulnerabilities: Shodan's integration with CVEs can be used to find devices with unpatched vulnerabilities, based on their banners or configurations.
3. assessing attack surface: with Shodan, users can gain insights into the publicly visible infrastructure of an organization in order to prioritize securing exposed systems.
4. passive scanning: unlike active vulnerability scanners, Shodan gathers information from its database without directly interacting with the target environment, reducing detection risks.

In addition, Shodan offers an additional functionality that triggers notifications about the organization's resources that are detected by Shodan during the scan. Shodan can provide information about:

- newly launched services
- vulnerabilities in running services
- detected malware
- end-of-life services
- configuration errors (exposed databases, IoT, building management systems).

Table 9 Vulnerability Scanner solutions: comparison table

Feature	Nmap with Vuln/Vulners/Vulscan	OpenVAS	Nessus	Shodan
Implementation model	On-Premises	On-Premises	On-Premises/Cloud	Cloud
Licensing	Free	Free	Subscription	Subscription
Open-Source	Yes	Yes	No	No
Release frequency	Approximately annually	Approximately annually	Approximately quarterly	Continuous updates
Vulnerabilities reported (per year)	Approximately 1-2	Approximately 1-2	Approximately 1-2	No data
Age	26	17	25	14
Community size (in thousands)	100+	10+	100+	Data not available
Roles and permissions	No	Yes	Yes	No
Integrations with other security solutions	Limited	Yes	Yes	Yes
API	No	Yes	Yes	Yes
High Availability (HA)	No	Yes	Yes	Yes
Notifications	None	Email, SMS, Webhooks	Email, SMS, Webhooks	Email, Webhooks
Reports	Limited	Yes	Yes	Yes
Audit logs	No	Yes	Yes	No

Vulnerability Management

Rapid7 InsightVM

Rapid7 InsightVM is an advanced vulnerability management platform designed to help organizations identify, prioritize, and remediate security risks across their IT environments. Its robust features, including live dashboards and asset tagging, make it ideal for organizations seeking to improve visibility and control over their security posture. InsightVM is a subscription-based solution available for both on-premises and cloud-based deployments, catering to organizations of varying sizes and complexities. It integrates seamlessly with Rapid7's Insight platform, providing centralized access to tools like threat detection and incident response. Its scalable architecture supports high availability (HA), ensuring uninterrupted vulnerability management even in large, distributed environments. InsightVM boasts several standout features, such as a RESTful API for automating vulnerability management workflows and integrations with other security solutions, including SIEMs, IT service management tools, and orchestration platforms. It provides real-time analytics and reporting, enabling security teams to track remediation progress and meet compliance requirements. Advanced notification options, including email, SMS, and webhooks, ensure timely alerts for critical vulnerabilities. Rapid7 InsightVM is a powerful solution for organizations looking to strengthen their vulnerability management practices.

Anchore

Anchore is widely recognized for its focus on Software Bill of Materials (SBOMs), which are critical for understanding the components and dependencies within software or containers. It provides capabilities for vulnerability detection, compliance checks, and supply chain security. Anchore claims to integrate well with CI/CD tools like Jenkins, GitLab CI, and GitHub Actions, allowing automated scans during the build process.

In addition to its SBOM functionality, Anchore includes support for customizable policies, which can help teams enforce security standards tailored to their environments. The commercial platform offers additional features and scalability for larger teams and enterprises.

DefectDojo

DefectDojo is AppSec platform developed by OWASP. It is designed to simplify and centralize the tracking and triage of security findings across various applications and environments. DefectDojo can aggregate vulnerability data from multiple scanning tools, allowing organizations to efficiently manage findings within a single, unified interface. DefectDojo is freely available and can be deployed on-premises, offering complete control over data and configurations. DefectDojo integrates seamlessly with numerous security tools, including vulnerability scanners, code analysis tools, and penetration testing utilities, consolidating results to provide a comprehensive view of security risks. Its powerful RESTful API enables automation and integration with other security systems, making it easier to align vulnerability management with existing workflows. It provides detailed reporting and tracking features which help organizations maintain compliance by generating audit logs and monitoring the progress of remediation efforts. With features like custom risk scoring, defect lifecycle tracking, and integration with DevSecOps pipelines, DefectDojo stands out as a versatile and cost-effective solution for organizations aiming to strengthen their application security posture.

Pakiti

Pakiti is a monitoring mechanism for checking the patching status of Linux systems developed by CESNET. The solution is provided for free and has been designed to install agents on the systems which send information about installed packages to the server. This server analyzes information for vulnerabilities and then presents results in a user-friendly web interface. Security teams can view and analyze vulnerability data, track remediation efforts, and generate reports. It also supports customizable vulnerability scoring, allowing security teams to prioritize fixes based on the risk levels specific to their environments.

Table 10 Vulnerability management solutions: comparison table

Feature	Rapid7 InsightVM	Anchore	DefectDojo	Pakiti
Implementation model	On-Premises/Cloud	On-Premises/Cloud	On-Premises	On-Premises
Licensing	Subscription	Subscription	Free	Free
Open-Source	No	No	Yes	Yes
Release frequency	Approximately quarterly	Approximately quarterly	Approximately monthly	Approximately annually
Vulnerabilities reported (per year)	Approximately 1-2	Approximately 1-2	Approximately 1-2	No data
Age	13	7	8	10
Community size (in thousands)	100+	10+	1+	Data not available
Roles and permissions	Yes	Yes	Yes	Yes
Integrations with other security solutions	Yes	Yes	Yes	Yes
API	Yes	Yes	Yes	Yes
High Availability	Yes	Yes	No	No
Notifications	Email, SMS, Webhooks	Email, Webhooks	Email, Webhooks	Email
Reports	Yes	Yes	Yes	Yes
Audit logs	Yes	Yes	Yes	Yes

Table of figures

1. SOC models in Academia

2. Maturity models for SOC-s

Figure 1 - Example of organisation units for a bigger CSIRT [18] 39

Figure 2 - Example of the TLP color-coding in RGB, CMYK and Hex 64

Figure 3 - Example of TLP labelling in an email message 65

Figure 4 - Assessment Form SIM3 v2 interim Self-Assessment Tool 71

Figure 5 - Spider-Chart in SIM3 v2 interim Self-Assessment Tool 72

3. SOC organizational and environmental requirements for Academia

Figure 1 – Data Source in the context of the SOC Usage and Volume 133

Figure 2 – Suggested Minimum Data Retention Time Frames 133

Figure 3 – Constituency size (users, endpoints, or IPS) 138

4. SOC technical architectures

Figure 1 - Architecture of the centralized logging infrastructure being developed at MUNI 174

Figure 2 - An OpenSearch dashboard displaying the number of unique event producers across four separate pipelines (Windows devices, Unified login, M365 cloud, and SMART proxy service) within the selected time frame. 177

Figure 3 - A Grafana dashboard visualizing the input rate of received events per aggregator source 179

Figure 4 - A Grafana dashboard visualizing the output rate of processed events per Vector sink 179

Figure 5 - A diagram illustrating an example of tool integration (image source: Flaticon.com) 188

5. Introduction to digital forensic and incident response (DFIR)

Figure 1 - Phases of security incident resolution according to NIST 800-61 r2. 193

Figure 2 - Proposed phases of security incident resolution - Appoint security team members - Impact evaluation 194

6. Review of software and hardware solutions

Figure 1 - Layout of the interfacing requirements; Asset Management System at MUNI	227
Figure 2 - Visualisation of collecting NetFlow traffic	232
Figure 3 - Example of view from FMC Analysis GUI	233
Figure 4 - Example of view from Arkime GUI	236