30-06-2022

Deliverable D8.9
Best Practices for Security Operations in Research and Education

Deliverable D8.9

Contractual Date:	30-06-2022
Actual Date:	30-06-2022
Grant Agreement No.:	856726
Work Package	WP8
Task Item:	Task 3.1. SOC
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	GÉANT Association
Document ID:	GN4-3-22-961B47
Authors:	Bart Bosma (SURF); Kiril Kjiroski (UKIM/MARnet); Panayiota Smyrli, Stephanos Andreou (CYNET-CSIRT); Roderick Mooi (GÉANT Association)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Abstract

This report introduces the concepts of security operations, including its goals, benefits and best practices, and of operational intelligence, as well as Security Operations Centres (SOCs) as a means to realise their practical implementation. It presents three research and education SOC case studies, including utilisation of the SOCTools package developed by GN4-3 WP8 Task 3.1 Security Operations Centre.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This report introduces the concepts of security operations, including its goals, benefits and best practices, and of operational intelligence, as well as Security Operations Centres (SOCs) as a means to realise their practical implementation. It presents three research and education SOC case studies, including utilisation of the SOCTools package developed by GN4-3 Work Package 8 Security, Task 3.1 Products and Services: Security Operations Centre.

At a time of increasing – and increasingly sophisticated – threats to and attacks on organisations' networks and applications, putting critical services and business processes at risk, security is more important than ever. Security operations (SecOps) aims to improve an organisation's security stance and maturity by consolidating the objectives of two often distinct functions, security and operations, aligning their priorities and achieving an effective balance between their goals. Implementing a SecOps model can help reduce the risk and number of security breaches, reduce vulnerabilities, improve incident response times and, as a result, help maintain business continuity.

A key function within SecOps is operational (or threat) intelligence, the goal of which is to have a continuous view of current threats and determine their impact at the operational, tactical and strategic level; and then to implement measures that eliminate or reduce the impact of those threats.

To efficiently implement security operations, a Security Operations Centre (SOC) is used which, in addition to monitoring and managing the security infrastructure, proactively deals with the impact of threats. A SOC can be set up as an internal, outsourced or hybrid service, can be a controlling, monitoring and/or operational type depending on the tasks that are performed, and can also be combined with an existing Network Operations Centre to form a Security & Network Operations Centre (SNOC). The size of the SOC and roles required can vary substantially depending on the type of SOC, services provided, organisational size and needs of the constituency. Typical SOC roles include security analysts, security engineers and information security manager, while specialised roles might include forensics analysts, malware analysts and penetration testers. Fundamental to the success of the SOC is support from senior management.

As the need for SOCs arose within the National Research and Education Network (NREN) community, WP8 Task 3.1 created an interoperable set of tools which can serve as a starting point for an NREN's SOC. This tool set, SOCTools, aims to assist with automation of the NREN's security processes such as collecting, enriching and analysing logs and other security data, threat information sharing and incident handling. While a full stack has been developed using existing tools (including Apache NiFi [NiFi], Open Distro [Open_Distro] for Elasticsearch and Kibana [Elasticsearch], [Kibana], MISP [MISP], TheHive and Cortex [TheHive] and Keycloak [Keycloak]), the focus has been upon easy and modular expandability.

The three case studies - SURFsoc case study, UKIM FCSE SOCTools use cases and CYNET-CSIRT's founding journey – present the experiences of a variety of members of the research and education community along their own SOC/CSIRT journeys, illustrating the concepts outlined above in real-life implementations. Together, these represent a valuable resource for R&E security practitioners and decision makers, to informing their own SOC journeys.

1 Introduction

Deliverable D8.9, *Best Practices for Security Operations in Research and Education*, provides background on the concepts of security operations (SecOps), including its definition, goals, benefits and best practices, and of operational intelligence (Section 2), before progressing to how SecOps can be practically implemented in the form of a Security Operations Centre (SOC). A definition of a SOC is provided, followed by organisational models, in/outsourcing considerations, roles and a description of SOCTools, the interoperable set of tools created by GN4-3 Work Package 8 Security, Task 3.1 Products and Services: Security Operations Centre, to assist members of the research and education community wishing to establish their own SOC; it also outlines some related recommended reading (Section 3).

Three research and education SOC case studies are then presented, to illustrate the concepts and use of the tools as well as share some lessons learned along the way, namely:

- SURFsoc case study – an account of the steps taken within SURF, the Dutch NREN, to set up a SOC (Section 4).
- UKIM FCSE SOCTools use cases – which features seven use cases for the components of SOCTools in the context of the work of the Faculty of Computer Science and Engineering Computer Centre at Ss. Cyril and Methodius University in Skopje (Section 5).
- CYNET-CSIRT's founding journey – a description of the journey taken by CYNET, the NREN for Cyprus, to establish and develop a Computer Security Incident Response Team (Section 6).

Key points from the case studies are drawn together (Section 7), and a list of SOC tasks and a description of two key SOC tools/services are provided in Appendix A and Appendix B, respectively.

2 Security Operations

This section introduces security operations, its goals, benefits and best practices, and the concept of operational intelligence.

2.1 What Is Security Operations (SecOps)?

Traditionally, security and operations have been viewed as distinct functions within organisations. While security is concerned with the triad of confidentiality, integrity and availability, operations is largely focused on service agility and performance, often neglecting aspects of security. Security teams are responsible for protecting infrastructure and securing sensitive information, as well as ensuring regulatory compliance; for operations, meanwhile, the top priority is to keep the organisation running by ensuring infrastructure uptime and service availability.[1]

In research and education organisations, the same individuals may be responsible for both areas. However, due to insufficient resources and time constraints, staff must often choose between conflicting priorities, even though the desire is *to do the right thing*.

Security operations (also known as SecOps) aims to consolidate the objectives of these teams – to align priorities and achieve an efficient balance between operational and security goals. "With SecOps, threat and risk mitigation become a shared responsibility, and operations professionals work closely with security professionals to reduce vulnerabilities without impairing business agility." [CyberArk] SecOps, akin to DevOps, prioritises speed and quality as well as security, providing a consolidated approach to reduce risks. Security becomes a key consideration in procurement, product/service development and, particularly, daily operations – achieving security objectives without jeopardising performance or service level agreements.

2.2 SecOps Goals and Benefits

The overarching goal of security operations is to improve an organisation's security stance and maturity by unifying security efforts and priorities across teams and activities. The high-level goals of SecOps [ServiceNow] are to:

- Facilitate cross-team collaboration with mutual accountability for security.

[1] It is acknowledged that *availability* is usually a shared objective of both operations and security teams.

- Increase security monitoring and visibility, resulting in improved transparency, earlier detection of events and prioritisation of actions.
- Ensure that security is integrated across business processes with appropriate management buy-in.

Furthermore, SecOps reduces:

- Risk.
- Team barriers/conflicts.
- Organisational silos.
- Duplication of effort.

It also improves:

- Teamwork.
- Trust.
- Collaboration.
- Efficiency.
- Quality.
- Response time.
- Consistency.

"Implementing a SecOps model can help identify threats earlier, reduce risk of breaches, [improve] incident response times, and as a result, help maintain business continuity and reputation." [Palo_Alto_Networks]

"Establishing a dedicated SecOps team with a security operations center [*sic*] can also result in:

- **Fewer security breaches** – collaborative network monitoring enables early detection of cyberattacks, reducing the number of breaches and protecting data while maintaining compliance with privacy and security requirements
- **Fewer security vulnerabilities** – code is more secure when it enters the production environment, thanks to input from security professionals at earlier stages of development. As a result, the IT organization experiences fewer security vulnerabilities.
- **Fewer security distractions** – SecOps teams that work to automate things like threat detection and alerts are distracted less by false positives and do a better job of focusing on real security threats that necessitate a response" [Sumo_Logic].

2.3 SecOps Best Practices

According to Microsoft [Microsoft], best practices for security operations include following the National Institute of Standards and Technology (NIST) Cybersecurity Framework [NIST_CF]:

- **Identify** and **Protect**:

- “Prioritize security investments into systems that have high intrinsic value. For example, administrator accounts.”

- **Detect** malicious actors in networks/systems:
  - “Proactively hunt for adversaries as your system matures. This effort will reduce the time that a higher skilled adversary can operate in the environment. For example, skilled enough to evade reactive alerts.”
- **Respond** by quickly determining whether the event is an actual attack/incident or false alarm and triage accordingly:
  - “Acknowledge an alert quickly. A detected adversary must not be ignored while defenders are triaging false positives.”
  - “Reduce the time to remediate a detected adversary. Reduce their opportunity time to conduct and attack and reach sensitive systems.”
- As part of **Recovery**, restore the confidentiality, integrity and availability (CIA) of attacked resources.

A typical incident handling process includes reporting/detecting, triage, response and closure as illustrated in Figure 2.1.

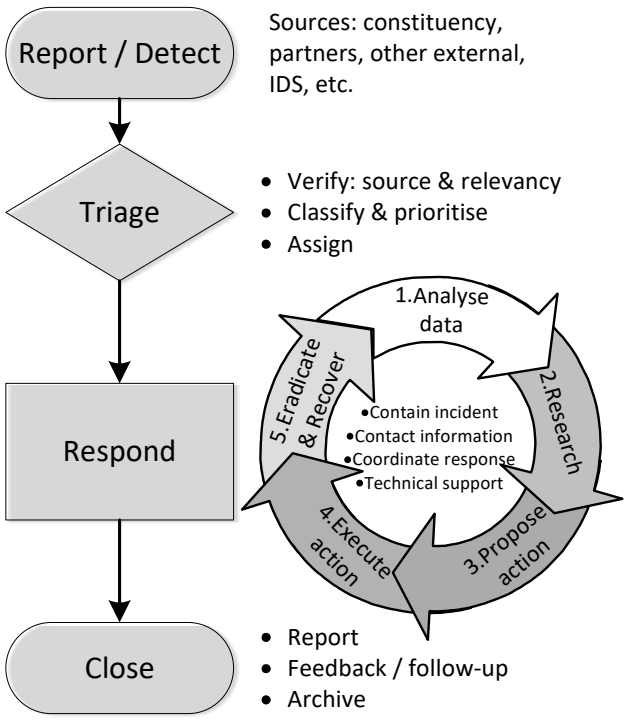

Figure 2.1: Incident handling process (adapted from ENISA *Good Practice Guide for Incident Management* [ENISA_GPGIM])

2.4 What Is Operational Intelligence?

A key function of security operations is operational intelligence. The goal of operational intelligence is first to have a continuous view of current threats and determine their impact at the operational, tactical and strategic level; and then to implement measures that eliminate or reduce the impact of those threats. Terms used as alternatives to operational intelligence include cyber analytics, cyber intelligence and (cyber-)threat intelligence. Gartner defines threat intelligence as follows:

> "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing menace, an emerging menace, or a hazard to IT or information assets. This knowledge can be used to inform decisions regarding the subject's response to that menace or hazard." [Gartner]

The essence of the definition is that the response to a threat/hazard is executed on the basis of fact-based knowledge, gained by collecting and analysing data on the internal network and data from external sources.

To efficiently implement security operations, a Security Operations Centre (SOC) is used which, in addition to monitoring and managing the security infrastructure, proactively deals with the impact of threats.

3 Security Operations Centre

This section defines what a Security Operations Centre is, and discusses organisational models, tasks and in/outsourcing considerations. It also describes SOCTools – the interoperable set of tools created by GN4-3 to assist members of the research and education community wishing to establish their own SOC – and makes recommendations for further reading.

3.1 What Is a Security Operations Centre (SOC)?

A Security Operations Centre (SOC) is a service/function that performs various information security tasks, acting as a hub for security operations. These tasks can be advisory or monitoring, depending on the role assigned to the SOC [PvIB]. A SOC fulfils several goals:

1. Demonstrable control of information security – the SOC can play a major role in complying with laws and regulations that increasingly require demonstrable control over information security, among other things.
2. Effective execution of operational security tasks – because an increasing number of different security solutions are being deployed, more specialised knowledge is required for operation and management. Combining that knowledge in the SOC has a quality-enhancing effect.
3. Incident and risk management – by aggregating and correlating information from various sources, the SOC can respond more effectively to threats. A Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) can be part of the service provided by the SOC.

Before deciding on the setup of a SOC, it should be determined what kind of SOC is desirable, what the scope of the SOC will be, whether it will be an internal SOC or an outsourced SOC and, in the case of an outsourced SOC, what is expected from the Managed Security Service Provider (MSSP) and which matters may still be handled in-house (on the basis of a Service-Level Agreement (SLA) containing a clear description of roles). Even when there is an internal SOC, certain services can still be outsourced (a hybrid SOC). These models, and the tasks they might perform, are discussed in the next section.

3.2 SOC Organisational Models and Tasks

In terms of organisation, a SOC can be set up in various ways: as an internal service (internal SOC), as an external service (outsourced SOC) or as a combination of internal and external services (hybrid SOC), where the SOC is internal, but various tasks are outsourced, for example to obtain specialist data

or to provide a 24x7 service. Furthermore, it is possible to distinguish between different types of SOC based on the tasks that are performed:

- Controlling SOC – performing vulnerability scans, compliance testing.
- Monitoring SOC – monitoring of firewalls, intrusion detection system (IDS), virus scanners.
- Operational SOC – performing management of firewalls, IDS, certificate management.

These are summarised in Table 3.1 (see also Appendix A).

Task	Type of SOC		
	Controlling	Monitoring	Operational
Firewall Log Analysis	√	√	
Firewall Management			√
Intrusion Detection and Prevention (IDP) – log analysis		√	
Intrusion Detection and Prevention (IDP) – management			√
Vulnerability Scanning	√		
Penetration Testing	√		
Compliance Management	√		
Identity and Access Management (IAM)			√
Risk Assessment	√		
Key Management			√
Digital Vault			√
Cyber Intelligence		√	
Forensics		√	
Computer Emergency Response Team (CERT)		√	
Data Loss Prevention (DLP)			√
Security Advice	√	√	√
Security Information and Event Management (SIEM)		√	
Privileged User Management			√

Table 3.1: Example of tasks with different types of SOC (adapted from [PvIB]

Depending on the type of SOC, different tasks are performed:

- Collecting data / performing proactive monitoring, such as:
  - Network traffic data.
  - Data from systems (logs).
  - Data from intrusion detection systems (alerts).

- Data from external sources (e.g., ThreatConnect, AnubisNetworks' Cyberfeed, HackerOne, Shadowserver, Proofpoint/Emerging Threat Intelligence, AlienVault Open Threat Exchange (OTX), abuse.ch, etc.).

- Aggregating and correlating data[2] / performing threat intelligence:
  - The SOC can effectively collect and analyse the data (preferably automated), generating useful alerts that can be acted upon.
- Making reports and giving advice:
  - The SOC has the knowledge and ability to provide advice based on the data analysis.
- Acting on incidents and assisting with recovery:
  - The SOC has the knowledge and skills to implement measures and perform post-incident analysis based on the analysed data.
  - This could include forensics and root cause analysis.
- Ensuring legal and regulatory compliance – either as a direct requirement (e.g. to have a SOC) or through the implementation of security controls.

The Computing Technology Industry Association (CompTIA) offer a complementary perspective of SOC tasks/activities [CompTIA], including the following diagram which effectively illustrates how a SOC performs its functions.

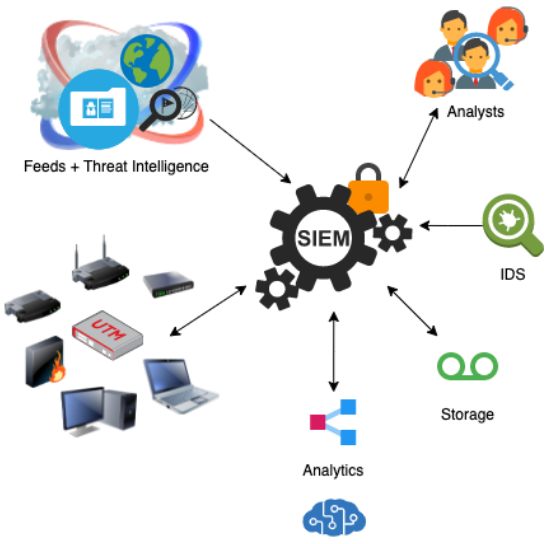

Figure 3.1: SOC functions and data sources (adapted from [CompTIA])

3.3 Internal or Outsourced?

There are advantages and disadvantages to both internal and external models, as listed in Table 3.2 below.

[2] **Aggregation** is the intelligent combination of logging data from various events; **correlation** is the establishment of relationships between events [NORA_Online].

Internal SOC	Outsourced SOC
Own staff for the service; 24x7 more difficult to achieve and expensive	Staffing more efficient because multiple clients can be served with the same people; 24x7 possible
Well-qualified personnel hard to find, but own familiar environment	Well-qualified personnel available and employable for different customers, but no own known environment
No “global view”; patterns on own network are easy to recognise	“Global view”; patterns on internal network of customer harder to recognise
Combination with other internal services easier to realise	Combination with other customer services difficult to realise
If not available, specialised knowledge must be purchased or hired	Specialised knowledge available and efficiently deployable for different customers
Knowledge of tools must be gained if not available beforehand	Knowledge of various tools available
In-house management is more flexible; adjustments can easily be implemented	Standard service; adjustments cannot be implemented easily
No scalable and flexible service; additional functionality requires new investment	Service is scalable and flexible; additional modules can easily be added to the service
Local storage of information; risk of data leakage low as long as access to information is properly set up	Information storage off-premises; risk of data leakage higher – access control must be well set up; requires agreements in SLA
Requires large initial investment (personnel, training, hardware and software, etc.), recurring licence fees; no service fees	No initial investment (unless there is a setup fee) or recurring licence fees; however, there are ongoing costs in the form of service fees
Information from external sources must be purchased	Information from external sources part of the service (depending on agreements/contract)

Table 3.2: Advantages and disadvantages of internal vs. outsourced SOC

A further consideration is the size of the organisation: “Larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such a capability.” ([NIST_SPC], p. 156.)

3.4 Security & Network Operations Centre (SNOC)

If a Network Operations Centre (NOC) is already present in the organisation and operational intelligence is also to be performed in-house, it is conceivable that the NOC and the SOC are combined into a Security & Network Operations Centre (SNOC).

Figure 3.2 below shows the possible layout of a SNOC:

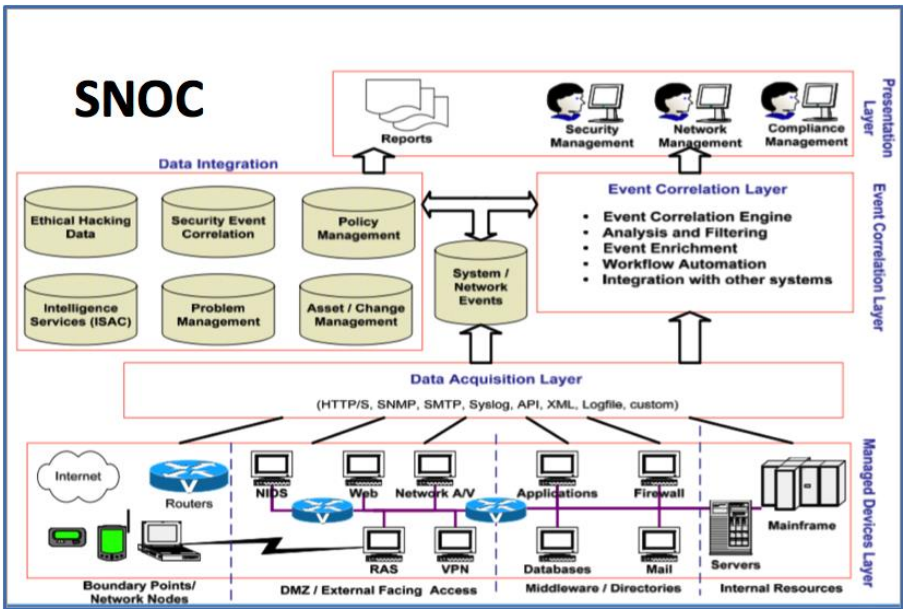

Figure 3.2: Schematic of possible SNOC layout

By combining the NOC and SOC, staff can be used more efficiently:

- The range of tasks is larger, making the time allocation more varied.
- Network specialists often also have security knowledge and vice versa.
- Security incidents are often related to the network infrastructure.

However, there are also disadvantages to combining a NOC and a SOC:

- The function of the NOC is to ensure optimal availability and performance of the network (and possibly of applications), while the SOC must ensure that security incidents are kept to a minimum. As a result, potentially there are conflicting objectives, because preventing and resolving security incidents does not necessarily contribute to optimising network/applications availability and performance, and similarly, optimising network/applications availability and performance does not always contribute to preventing and resolving security incidents.
- Moreover, staffing a NOC requires different skills and expertise from staffing a SOC.
- Also, a SOC requires different tools from a NOC, so combining NOC and SOC does not necessarily result in cost savings.

In addition to combining different services, other services already in place can be integrated; for example, vulnerability management can be one of the services provided by a SOC.

3.5 Roles

Depending on the type of SOC, services provided, organisational size and needs of the constituency, the size of the SOC team and number of roles required can vary substantially. Thus it is crucial to

identify some key business requirements upfront, including the environment, funding, constituency and applicable laws and regulations. Typical SOC roles include security analysts, engineers, team manager and system administrators who generally report to an information security manager or Chief Information Security Officer (CISO) [Palo_Alto_Networks]. Specialised roles such as forensics analysts, malware analysts or penetration testers can be considered, based on the functional requirements. It may make sense to partner with others for these roles as they are often required on an ad hoc basis.

Fundamental to the success of the SOC is support from senior management – including executive and board level. This will ensure that the SOC is empowered to do its job – having appropriate authority – and to do it well. Support can be shown through policy interventions, awareness and visible awareness and training initiatives (including self-compliance) by leadership.

3.6 SOCTools

As the need for Security Operations Centres arose within the National Research and Education Network (NREN) community, the GÉANT project created an interoperable set of tools which can serve as a starting point for an NREN's SOC. This tool set aims to assist with automation of the NREN's security processes and data gathering. While a full stack including the acceptance of log and IDS data has been developed using existing tools, the focus has been upon easy and modular expandability. The layout of the core components is shown in Figure 3.3:

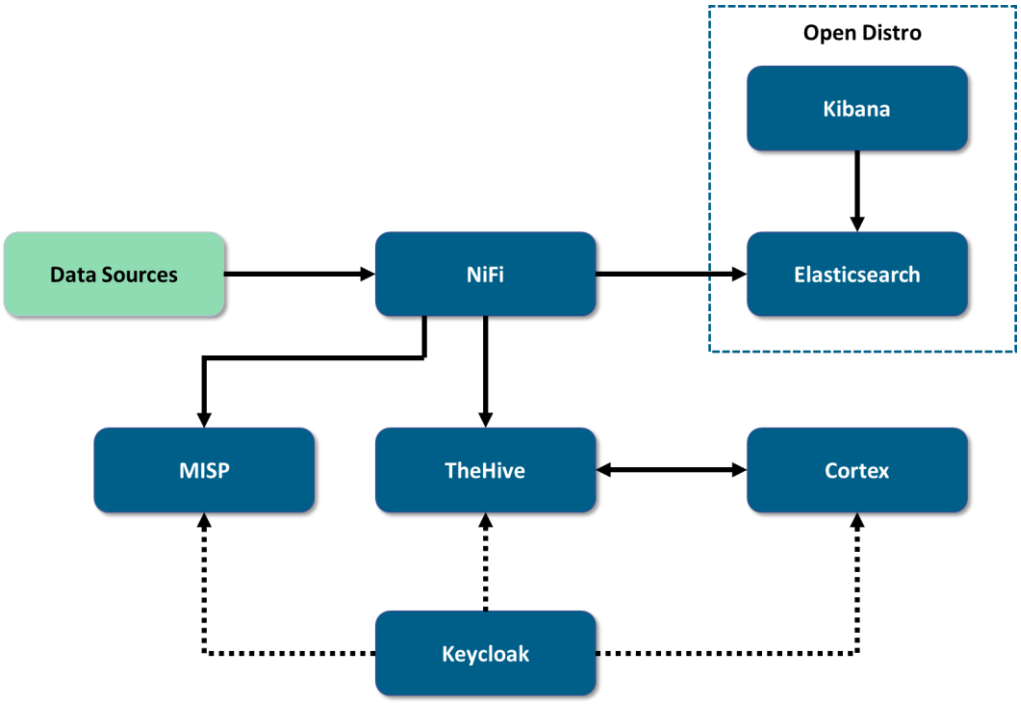

Figure 3.3: Layout of SOCTools core components

SOCTools is a collection of tools for collecting, enriching and analysing logs and other security data, threat information sharing and incident handling. It is comprised of the following components:[3]

- **Apache NiFi** [NiFi], an easy-to-use, powerful and reliable system to process and distribute data.
- **Open Distro** [Open_Distro] for **Elasticsearch** and **Kibana** [Elasticsearch], [Kibana]. Open Distro is an Apache 2.0-licensed distribution of software that includes open-source Elasticsearch and Kibana packaged with a number of feature-adding plugins built by Amazon Web Services (AWS). Kibana is a free, open frontend application that sits on top of the Elastic Stack, providing search and data visualisation capabilities for data indexed in Elasticsearch; Elasticsearch is a distributed, free and open search and analytics engine for all types of data, including textual, numerical, geospatial, structured and unstructured.
- **MISP** [MISP], an open-source threat intelligence platform for sharing, storing and correlating indicators of compromise of targeted attacks, threat intelligence and vulnerability information.
- **TheHive** and **Cortex** [TheHive]. TheHive is a scalable, open-source and free security incident response platform, tightly integrated with MISP. Cortex is a powerful observables[4] analysis and active response engine.
- **Keycloak** [Keycloak], an open-source identity and access management solution.

SOCTools aims at being an easy-to-install, centrally configurable, package of these components.

The tool set can be installed in a Docker environment and is available from GÉANT's GitLab [GN_GitLab_SOCTools].

3.7 Recommended Reading

This section highlights some additional resources to assist the reader on their SecOps/SOC journey.

3.7.1 Mitre: 11 Strategies of a World-Class Cybersecurity Operations Center

11 Strategies of a World-Class Cybersecurity Operations Center commences by introducing the fundamentals of SOC functions, data and tools before progressing on to 11 key strategies the authors have identified for effectively maturing SOC capabilities, namely (and keeping the US English of the source):

1. Know What You Are Protecting and Why.
2. Give the SOC the Authority to Do Its Job.
3. Build a SOC Structure to Match Your Organizational Needs.
4. Hire and Grow Quality Staff.
5. Prioritize Incident Response.
6. Illuminate Adversaries with Cyber Threat Intelligence.

[3] These components, as well as the modular installation thereof, are being revisited as part of GN5-1.
[4] "Observables" include such attributes as IP and email addresses, URLs, domain names, files or hashes.

7. Select and Collect the Right Data.
8. Leverage Tools to Support Analyst Workflow.
9. Communicate Clearly, Collaborate Often, Share Generously.
10. Measure Performance to Improve Performance.
11. Turn up the Volume by Expanding SOC Functionality.

The book is available as a PDF at [MITRE_11Strategies_PDF] (or via [MITRE_11Strategies]).

3.7.2 HEISC: Security Operations Center (SOC) Case Study

This case study paper was prepared by members of the Higher Education Information Security Council (HEISC) in the United States. It is written specifically for those in the higher education sector considering establishing a SOC and/or outsourcing certain SOC functions, and covers similar topics to the present report, including:

- What is a SOC?
- Typical SOC functions.
- Growing a SOC.
- Common SOC Approaches in Higher Education.
- Process Improvement.

Security Operations Center (SOC) Case Study is available as a PDF at [HEISC_SOC_CS_PDF] (or via [HEISC_SOC_CS]).

3.7.3 ENISA: How to Set Up CSIRT and SOC

This publication from the European Union Agency for Cybersecurity (ENISA) includes guidance on typical SOC services, incident handling and monitoring services as well as training for specific CSIRT/SOC roles, amidst many other factors focused on establishing and improving a CSIRT/SOC.

How to Set Up CSIRT and SOC is available as a PDF at [ENISA_HTSUC&S_PDF] (or via [ENISA_HTSUC&S]).

4 SURFsoc Case Study

4.1 Introduction

Hackers and cybercriminals are always ahead of security professionals when it comes to innovation. All kinds of malware are offered commercially on underground forums and kept up to date, botnets are available as a service, and carrying out a denial-of-service attack or sending spam is easily accomplished [SANS_Shackleford]. Therefore, accurate threat information is very important for any organisation to be able to take quick and effective measures.

The purpose of this section is to describe the steps taken within SURF, the Dutch NREN, to identify the possibilities for security operations, including security intelligence, and thus provide the impetus for a feasibility study on setting up a Security Operations Centre within SURF. The underlying idea is that institutions need centrally organised security monitoring and alerting, and perhaps also a service that carries out those types of task within the institutions themselves. The section covers the scope and setup of a SOC at SURF, the phases of the SOC activity (as originally envisaged), current status, and conclusions, including lessons learned.

4.2 Scope and Setup of a SOC at SURF

SURF is an organisation with its own office environment, which requires good security; at the same time, it is an organisation that supports member institutions. For example, SURFcert is a service SURF provides that is primarily concerned with supporting and sharing knowledge with member institutions regarding network security and attacks [SURFcert].

Therefore the SOC could be used for SURF's office environment exclusively, or as a service to monitor and control the SURFinternet [SURFinternet], thus improving services to the member institutions. Furthermore, the SOC can offer controlling and monitoring within the institutions as a service. In all cases, consideration must be given to exactly what services the SOC will provide and whether an in-house, outsourced, or hybrid SOC is preferable.

Figure 4.1: SOC building blocks (Source: [SANS_Torres])

Furthermore, it is important to identify if, or to what extent, privacy aspects play a role. When data is stored and analysed that (potentially) contains personal data, SURF must comply with the General Data Protection Regulation (GDPR) including, as of 1 January 2016, the mandatory data breach notification. This affects the way the SOC is set up.

When setting up the SOC, the categories people, process and technology must be taken into account: people in different functions must work together, various processes must be set up, and all kinds of technologies are deployed (see Figure 4.1 above).

People

- What roles need to be filled?
- What role can SURFcert play?
- What external services, if any, are needed?
- In which department will the SOC be positioned?

Process

- Which workflows are needed?
- Which Standardised Operating Procedures (SOPs) will be set up?
- Which (ITIL) processes within SURF match the SOC processes?

Technology

- What products are needed to support the SOC?
- Which data will be collected and analysed?
- To what extent are forensic tools needed?

- Is there an up-to-date Configuration Management Database (CMDB)?

4.3 Phases

4.3.1 Phase 1

In early 2015, Gijs Rijnders conducted a pilot as part of his graduation project using Elastic Stack/ELK as a Security Information and Event Management (SIEM) solution and Syslog data, Netflow data and Suricata IDS as data sources, as shown in Figure 4.2 [Rijnders]:

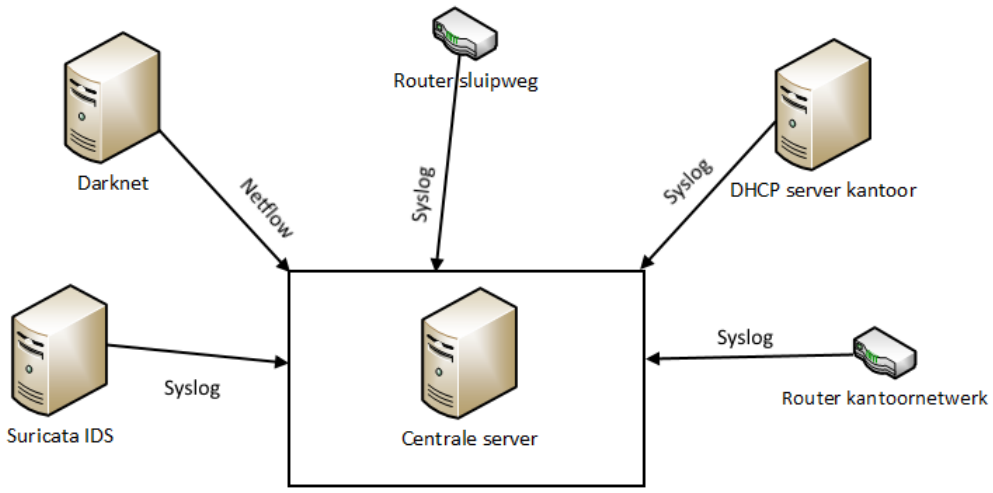

Figure 4.2: Gijs Rijnders' schematic setup

The goal of his research was to find out to what extent a SIEM solution is suitable for centralising security logs and which products can be used for that purpose. Gijs' conclusion was that both products he investigated (Elastic Stack/ELK [Elastic_Stack] and Splunk [Splunk]) are suitable and sufficiently flexible for an organisation such as SURF, noting that the licence costs for Splunk are so high that Elastic Stack is preferred, despite some (solvable) limitations regarding access management.

The setup shown in Figure 4.2 can be used as a starting point for piloting an internal SOC. By continuing with Elastic Stack/ELK, experience can be gained with the possibilities provided by a SIEM solution for collecting and processing data, creating dashboards, generating alerts and creating reports. This experience can be used to determine what else is needed to set up a SOC effectively and how much manpower is required. Consideration can also be given to whether SURFcert can make use of this setup as well as creating added value for monitoring the SURFinternet, so that member institutions can also benefit from the intelligence that is gained.

4.3.2 Phase 2

Before this phase begins, the implementation from Phase 1 will be evaluated and necessary changes determined. Items that should be considered during the evaluation are, as a minimum:

- Does an internal SOC work or should an outsourced SOC be considered?
- Can an internal SOC be combined with the NOC?
- What services for an internal SOC should be sourced externally?
- Should the SOC be limited to SURF's office environment?
- Can the SOC monitor the SURFinternet?
- What information will be collected and analysed?

The answers to these questions will be used to determine how Phase 2 will be designed.

4.4 Current Status

At the end of 2019 the University of Maastricht was hit by a ransomware attack, which caused the university to be offline for a considerable time. As examinations were about to start and the next semester was imminent, the university decided to pay the ransom in order to obtain the decryption key.

The incident caused considerable concern among Dutch universities and other educational organisations in the Netherlands. A number of universities initiated a working group to investigate possibilities for a joint SOC/SIEM solution and engaged SURF to coordinate the effort.

Whereas interest in setting up or joining a SOC had been low until then, it now became a high priority. As SURF did not have the resources to set up a SOC at such short notice, it was decided to issue a tender for a joint SOC solution, managed or coordinated by SURF but delivered by a commercial party.

Some of the considerations were:

- The number and complexity of threats are increasing (and public attention follows suit).
- ICT is a fundamental component of the primary processes (education and research).
- An incident can have a great impact on the institution and its primary processes.
- Pressure on ICT departments is high and increasing.
- Politics is more focused on cybersecurity, because of the increasing number and impact of incidents.
- Cybersecurity resources and expertise are scarce.
- Education and research environments are quite different from regular office networks, which means a traditional SOC does not fit the bill:
    - Open networks.
    - Used for research (high bandwidth, few limitations).
    - Characteristics of traffic are completely different.

The approach taken to the tender was to establish a working group, with experts provided by five universities and led by an external project manager, to define the requirements.

The working group came up with a number of requirements/components:

- Security Information and Event Management (SIEM) with 24x7 service.
  - Monitoring and accompanying infrastructure.
- Create use cases and implement use case management.
  - Know what to monitor and why.
- Share knowledge among the organisations.
  - Automation, indicators of compromise (IoCs), MISP.
- Vulnerability scanning.
  - Which systems are vulnerable.
  - Which vulnerabilities are exploitable.
  - Periodic scans for “bad practices”.
- SURFcert keeps handling incidents.
  - Based on vulnerability scan results and IoCs detected.
- One point of communication between SOC and organisation.

The SURFsoc architecture is shown in Figure 4.3 below.

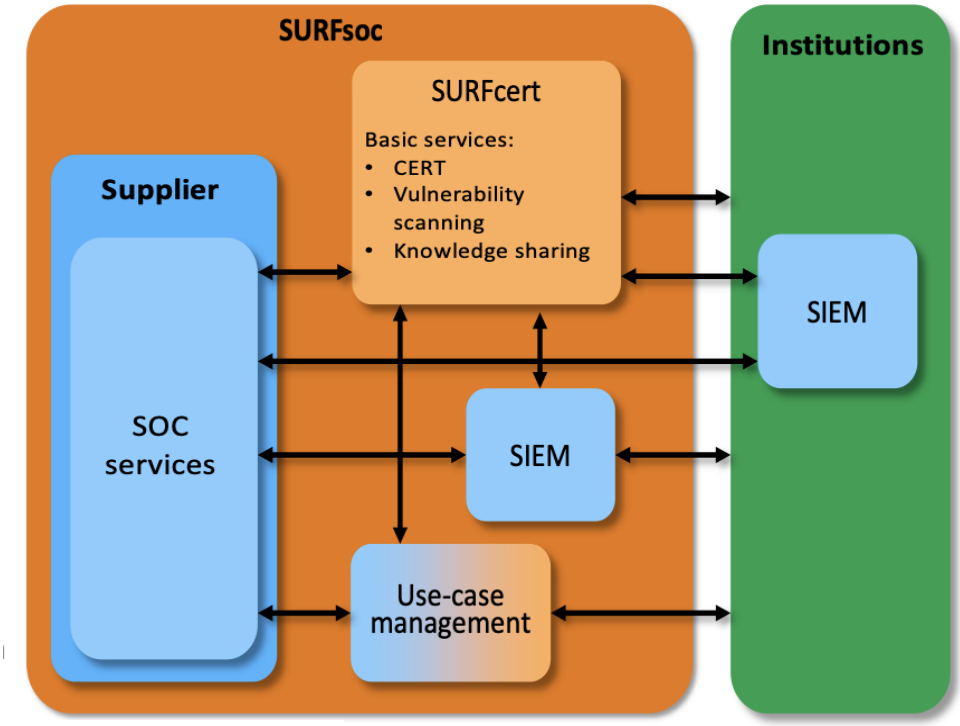

Figure 4.3: SURFsoc architecture

The working group defined 10 initial use cases to be part of the standard offering. Nine parties responded to the tender, and two were selected based on the quality of the offering; of those, one was selected based on price. From inception of the working group until the first implementation took approximately one year. As of today (June 2022), 23 organisations are connected to the SURFsoc, and the number is still increasing.

4.5 Conclusion and Lessons Learned

Operational intelligence can be achieved by setting up a Security Operations Centre (SOC) (in-house, outsourced or hybrid). In addition to control and monitoring functions, the management of security components can be housed at the SOC. Moreover, the SOC can respond more adequately and proactively if it has access to external threat intelligence. For this, various collaborations exist and open-source and commercial services are available.

An essential tool of the SOC is a Security Information and Event Management (SIEM) system to aggregate and correlate data from various sources, both internal and external. When an internal Network Operations Centre (NOC) exists, a combined SNOC (SOC + NOC) could be more efficient, as long as the different objectives of network operations and security operations are taken into account.

Building on the pilot conducted in early 2015 with Elastic Stack/ELK by Gijs Rijnders, an internal SOC can be set up, to determine from experience what type of SOC is needed and whether outsourcing might be a better option than hosting a SOC internally. Furthermore, one can look into the possibility of performing security operations on behalf of affiliated institutions.

At the same time, an inventory can be made of whether institutions have a need for centrally implemented security intelligence and what services would then be required.

Lessons learned to date include:

- A SOC is not a panacea. You are not safe all of a sudden and it does not reduce workload; on the contrary, it increases workload for the organisation:
  - Requires setting up a logging and monitoring infrastructure, including sensors/agents to collect (log) information.
  - Requires implementing use cases and follow-up on alerts.
  - Requires a lot of work initially, to get everything set up and organised.
  - Requires thought on relevant risks and mitigation thereof.
- Contractual negotiations take time.
  - Several institutions that were interested had requirements, especially regarding privacy (GDPR), that did not match the standard offering.
  - Many service-level discussions took place, about what is included or not.
- Cost.
  - In spite of the collective tender, the costs of using a SOC are high.
  - For a SIEM solution, more data means higher fees.
  - Maintaining use cases and following up incidents and alerts takes a lot of resources.
  - An internal CSIRT is (almost) required.

5 UKIM FCSE SOCTools Use Cases

5.1 Introduction

This section features seven SOCTools use cases of the Ss. Cyril and Methodius University Faculty of Computer Science and Engineering (FCSE) Computer Centre (FCC). It outlines the systems and solutions for which the FCC is responsible, and the SOCTools components, before describing the operational context for the use cases and the use cases themselves, then summarising future work and challenges.

5.1.1 Scope of Managed Systems and Solutions

Employees at the Faculty of Computer Science and Engineering (FCSE) Computer Centre (FCC) have been implementing and maintaining a number of systems fulfilling different needs of the Faculty, as well as helping other members of the Ss. Cyril and Methodius University in Skopje (UKIM in the following text) implement and maintain common solutions. These solutions include:

- iKnow (UKIM student services system) [iKnow].
- iLearn (Moodle for all UKIM members) [iLearn].
- UKIM help system [UKIM_Help].
- Repository of UKIM publications [UKIM_Repos].
- UKIM Identity Provider system implementing SAML2 for authentication, using iKnow database, UKIM Active Directory (AD) domain, IdP proxy, etc.

FCC also provides hosting and support for systems for the Ministry of Health (MoH) and Ministry of Education and Science (MoES), including:

- Electronic diary for all students at elementary and secondary schools [e-Dnevnik].
- National e-health system [MojTermin].
- Web sites/portals for the ministries.
- Mail systems for the ministries (hybrid Microsoft Exchange systems).
- Learning Management System for all primary and secondary schools in North Macedonia [MK_LMS].
- Learning Management System and Web Conference System for the Bureau of Education.
- Logging, preparing and visualising events for all systems, using ELK stack [Elastic-Stack].

Besides maintaining the abovementioned systems and applications, the primary focus of FCC is implementing and maintaining FCSE's systems, such as:

- Active Directory domains (ADDs) for students and faculty.
- Central Authentication and Authorisation System implementing Central Authentication Service (CAS).
- Moodle installations for learning materials, teaching and exams.
- Web conference clusters (BigBlueButton/Scalelite cluster implementations).
- Hypervisor clusters (VMware ESXi and vCenter).
- OpenStack private cloud.
- Mail systems for students and faculty.
- Various Faculty administration systems, such as dossiers, files, document management system, asset management system, faculty web portal, etc.
- FCSE Help Ticketing System, Redmine (project management web application), Projects system and other resource planning and management systems.
- Internet Exchange Point [MK_IXP].
- GÉANT-supported systems, such as eduGAIN, eduroam, etc.

The complex ecosystem at FCSE requires constant monitoring, encompassing insight and a deep understanding of how different environments are integrated, not just from the viewpoint of implementation and management, but also from the security viewpoint. Employees at FCC need to have a complete picture of it, in order to be able to provide the necessary level of support and to provide mitigation for all security threats. The complexity of the schools.mk system and all involved databases and systems is shown in Figure 5.1.

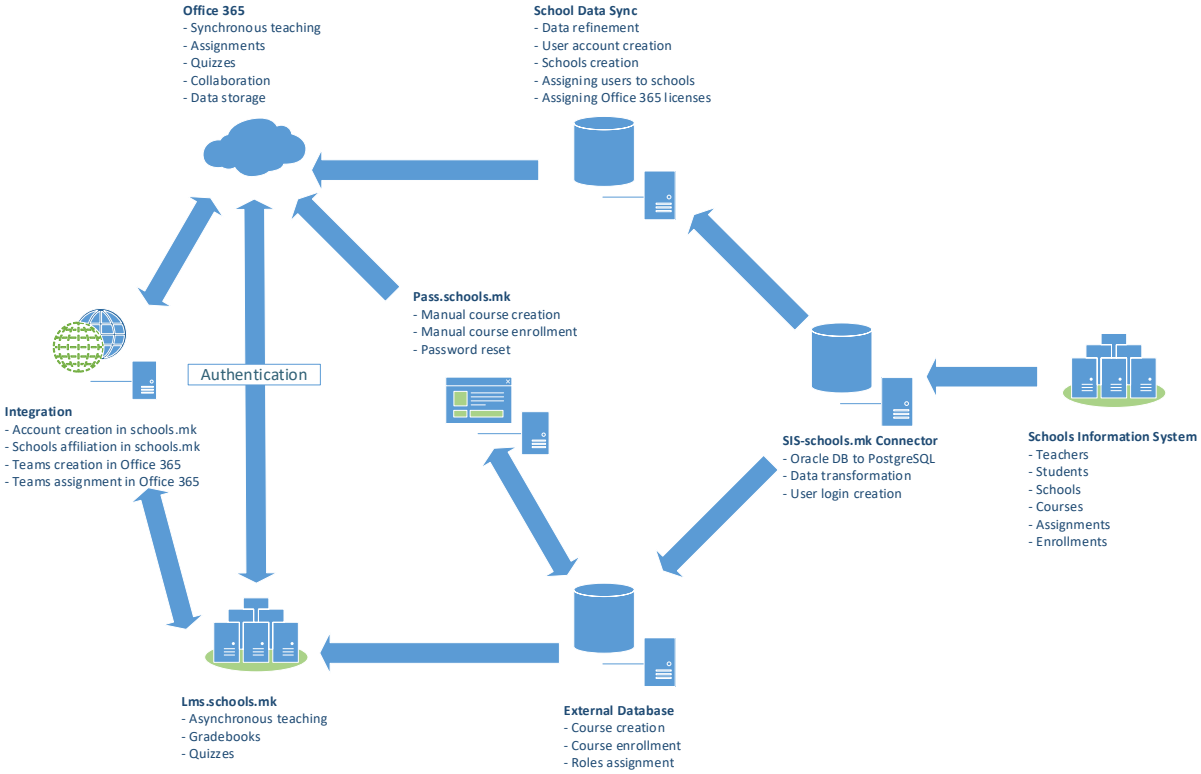

Figure 5.1: schools.mk ecosystem and all interconnected systems, services and databases used to accomplish various tasks in it

5.1.2 SOCTools

Under SOCTools FCC brings together several applications that are used by Security Operations Centres for various purposes, mainly in order to help security engineers to receive information about new security threats, to create cases and incidents, to organise and to manually visualise the vast amount of data gathered from different sources, and to use manual or automated tools for the analysis of different objects appearing in these reports. FCC's SOCTools also include a few components that enable services such as single sign-on, proxying, load-balancing and service synchronisation. FCC uses the following SOCTools in various use cases:

- **Apache NiFi** [NiFi] is used for **data transport** and as the key component that collects data from data sources, normalises it, does simple **data enrichment** and then ships it to one or more of the other components in the architecture.
- **Elasticsearch** [Elasticsearch] is used in SOCTools for **data storage**.
- **Kibana** [Kibana] is used for **manual analysis and visualisation** of collected data in the current version.
- **MISP** [MISP] collects and analyses **threat intelligence data**. It represents the typical source for enrichment data.
- **TheHive** and **Cortex** [TheHive] are used for **threat analysis** and new cases can be created automatically from manual analysis in Kibana.

The interaction of the three threat intelligence data sharing and analysis components is shown in Figure 5.2 below.

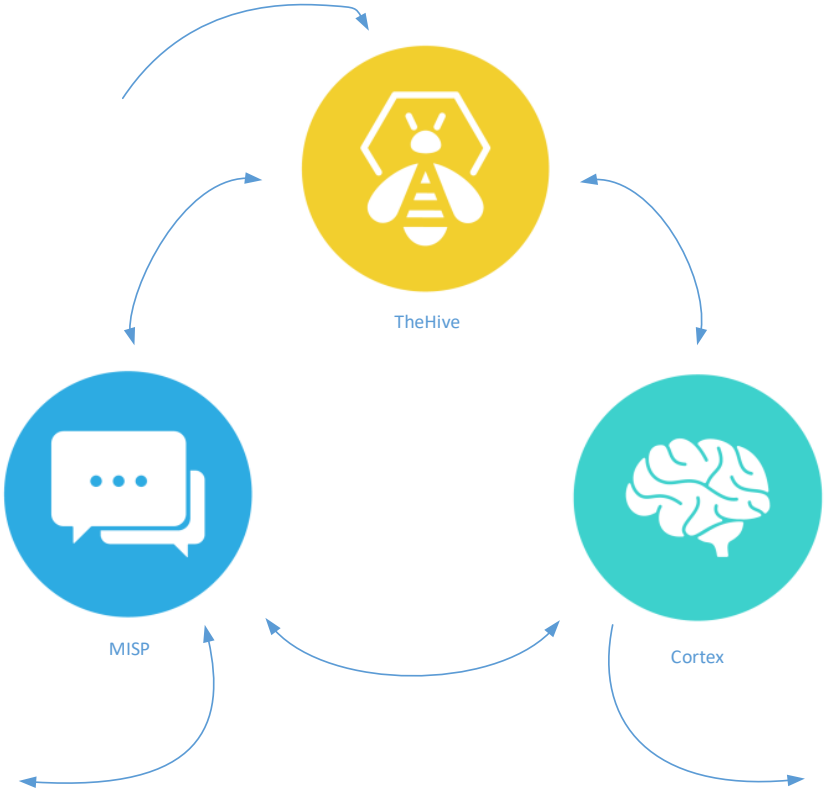

Figure 5.2: MISP, TheHive and Cortex, the interconnected threat intelligence data sharing and analysis trio

5.2 Operational Context and Security Challenges

FCC is in charge of all FCSE's activities involving computing, networking, storage and other IT resources. FCC was established along with the creation of the Faculty for Computer Science and Engineering in 2010, by merging faculty and administrative staff from two ICT institutes at the Faculty of Electrical Engineering and Information Technologies and the Faculty of Mathematics and Natural Sciences in Skopje. The team has grown from two employees at the start to six employees in 2022, mainly engineers and administrators.

Unfortunately, FCC does not have enough human resources to assign them to dedicated network and security roles. Therefore, most of the employees at FCC have to handle different networking and security issues. There is no formal Security Operations Centre as such, but most experienced network engineers are involved in designing and implementing various security measures and monitoring and alerting systems. Having in mind the kind of faculty, university and country services hosted at FCSE, it is understandable that a lot of security challenges are presented during everyday work.

FCC employs multiple Active Directory domains (ADDs) to provide authentication services for different users at FCSE, the University, Ministry of Health, Ministry of Education and Science, and for all students and teachers in primary and secondary schools in the Republic of North Macedonia. These user accounts are created:

- On multiple on-premises ADD servers, in the cases of FCSE and the University.
- In Azure ADD, in the case of primary and secondary schools (schools.mk).
- In a hybrid environment, in the cases of MoH and MoES.

These users also need to be authenticated and authorised to use different services using different roles, so there are implementations of different authorisation tools such as:

- Central Authentication Service (CAS) – for student and faculty accounts at FCSE.
- SAML2 – for students and faculty at the University.
- OpenID Connect – for students and teachers in schools.mk.

FCSE uses network assets in order to provide different services to all stakeholders. FCC has provisioned a number of networks for different use cases and user profiles. Networks are planned and implemented using different network policies (default drop or default accept), depending on the needs of the intended audience.

Networks and/or subnets with applications containing personal or confidential data use the default drop policy and only selected ports are open per IP address. Security in these networks is implemented both on an edge firewall and on servers hosting sites and services. The need to constantly monitor these network ports is imperative.

The other types of networks are intended for education and/or research. These networks are open by design, since they are mostly hosted as part of the private cloud at FCSE. The default policy in the cloud is to close all access on a public network, but educators and researchers have all necessary privileges to change this policy and implement a new one in any way they see fit.

Hacker attacks are some of the most important security issues manifesting during everyday network operation. These attacks vary in form, source, target, intensity and severity, but represent some of the major threats for any institution or organisation. The problem with hacker attacks is that they may be successful in compromising network security, but they can be hard to detect if the attacker is careful and is trying to discover as much information as possible without giving away successful network and/or systems penetration. Usually, this kind of intrusion is detected much later, when the attacker is trying to cover his tracks.

FCSE, in cooperation with the Macedonian Ministry of Education and Science, is in the process of procuring computing resources, intended to be used by all academic and research communities in Macedonia. It will involve a cluster for general purpose computing on graphics processing units (GPGPU), a private OpenStack Cloud, as well as a Hadoop cluster. Since it will be available for usage by individuals and organisations outside of the University, it will be necessary to provide the means for securing and monitoring their access to FCSE's network. Monitoring and hardening of the network and its endpoints are of utmost importance for the efficient and safe utilisation of the computing resources that will be made available through this project.

5.3 FCSE Use Cases

The above are some of the security challenges that have been identified in the normal course of everyday business at FCSE. FCSE is aware that these are not the only issues present in its ecosystem, but these are of special interest due to their capability to affect FCSE as a whole, their significance for the confidentiality, integrity and availability of hosted services, as well as for the overall image of the University in Macedonian society. The selected SOCTools use cases are therefore the following:

1. User authentication and authorisation in Active Directory domains and Azure Active Directory domains.
2. Identification and accounting of all network ports reachable from outside of FCSE networks.
3. Logging of source IP addresses and destination ports for servers and services reachable from outside of FCSE networks.
4. Monitoring general reachability of FCSE services due to network instability or physical damaging of optical links.
5. Monitoring traffic behaviour on network edges, IXP transit traffic, and their influence on the local network.
6. Managing general cases of hacker attacks, such as attempts of brute force attacks, zero-day attack exploitation, hacked email accounts (and subsequent abuse of these accounts), denial of service attacks, etc.
7. Managing usage of FCSE IT resources during their entire lifecycle.

5.3.1 User Authentication and Authorisation in ADD and Azure ADD

Active Directory login events are of utmost importance for the security of the domain, whether it is on-premises, hybrid, or entirely implemented in Azure. FCC is currently working on the following use case:

- The user tries to access one of their services.
- The user is forwarded to the appropriate authentication endpoint.
- The user authenticates using their appropriate authentication method and a login event is created in the AD log.
- Create alerts:
  - Automate exporting of on-premises AD security event log to **Elasticsearch**.
  - Create triggers for alerting about “interesting” login events from Azure AD.
- Create filters in **Kibana** for different AD security log sources.
- Create and use dashboard in **Kibana** for AD security logs.

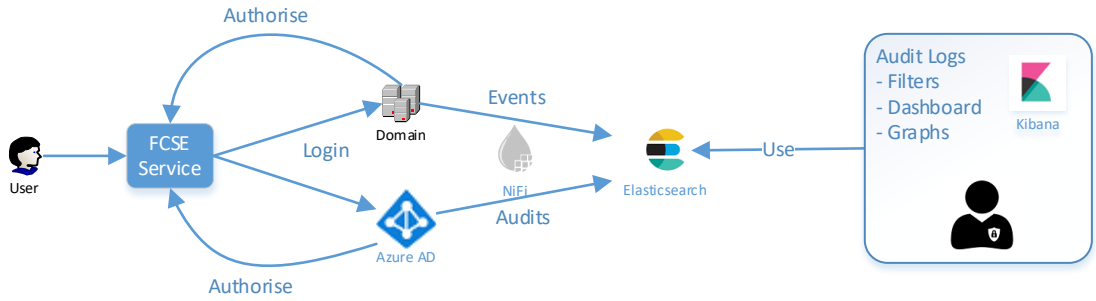

Figure 5.3: Use case workflow: user authentication and authorisation in ADD and Azure ADD

5.3.2 Identification and Accounting of All Network Ports Reachable from Outside

Both employees and external associates of FCSE perform different tasks on development, test and production servers for the applications, as well as for the education and research part of the network. FCSE is currently working on enabling SOCTools to fulfil its goals using the following workflow:

- **MISP** implements multiple modules that can utilise external resources that extend MISP for new services such as expansion, import and export. Shodan [Shodan] is one of these services, providing information about publicly available ports from the organisation's network.
- The Shodan module will create **MISP** incidents regarding monitored IP addresses and open ports.
- **TheHive** will poll the MISP instance for new or updated events.
- In case of such events, **TheHive** will create cases and/or alerts for system engineers.
- The FCC employee (system engineer) will perform analysis and/or interview appropriate person(s) for the justification of the opened ports, and act accordingly – opened ports will either be closed, or the information and justification will be included in TheHive case.

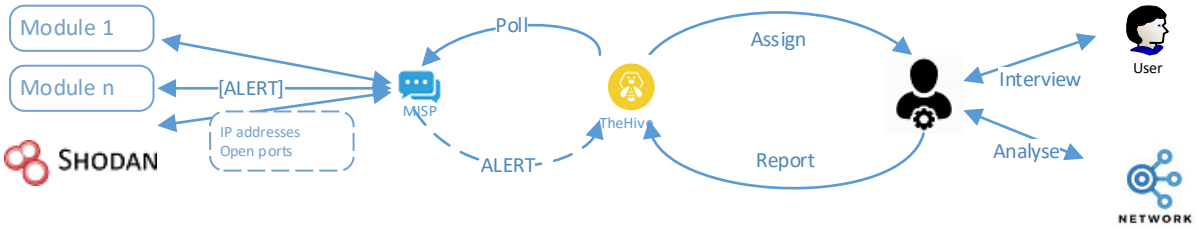

Figure 5.4: Use case workflow: identification and accounting of all network ports reachable from outside

5.3.3 Logging of Source IP Addresses and Destination Ports for Servers and Services Reachable from Outside

This is an extension of the previous use case. In this case, information about Internet-accessible IP addresses and corresponding open ports is already known. Since there is a substantial number of sites

and services hosted in FCSE networks, a need arises to closely monitor any activity that may be of interest.

Most of the sites and services hosted at FCSE have one or another form of user authentication. The use case in Section 5.3.1 described how to use SOCTools to monitor and analyse suspicious login events when using Active Directory as an authentication source. Unfortunately, not all services hosted at FCSE are able to use these mechanisms. Services using any kind of local authentication (or that have no authentication whatsoever) also need to be closely monitored for suspicious login attempts on ports usually open for outside access, both authenticated and/or anonymous. These events are handled using the following scenario:

- An excessive number of failed login attempts will trigger an alert notification, which is sent to an Internet Message Access Protocol (IMAP) folder.
- The IMAP mailbox is polled for new ("unread") messages from **TheHive**, using TheHive4py module. If the email subject contains "[ALERT]", an alert is created; otherwise, a case with a set of predefined tasks will be created.
- After assignment, a security engineer needs to perform manual analysis of the alert and act accordingly:
  - The case can be closed after submission of the findings.
  - Additional **Cortex analysers** can be deployed for further investigation of the login source(s).
- If further analysis of the created case is needed, appropriate actions can be taken to:
  - Create an event in **MISP** using the source IP address(es) and/or domain, as well as the local IP address and port. This action may include referring to the SOCTools use case on GÉANT GitLab.
  - Use **Kibana** to find further events involving the attacker and/or target.
  - Devise and implement additional security measures on the target server(s) and/or service(s).
  - Document events and steps in **TheHive case**.

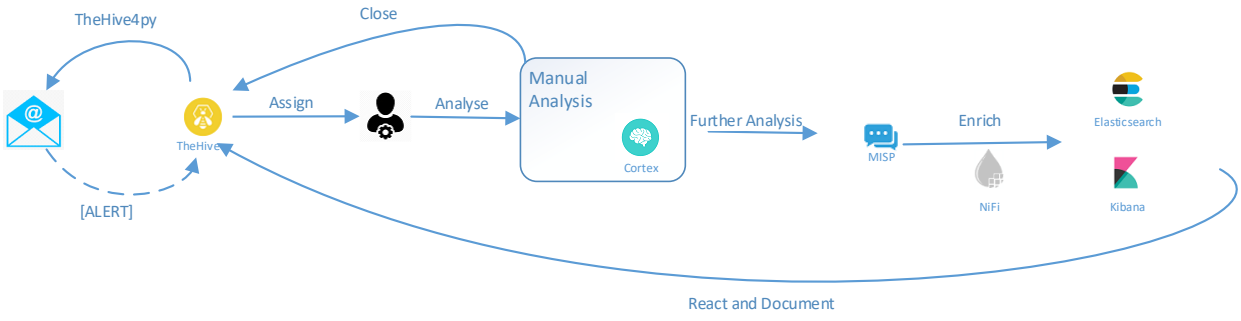

Figure 5.5: Use case workflow: logging of source IP addresses and accessed destination ports for servers and services reachable from outside

5.3.4 Monitoring General Reachability of FCSE Services

Today, Internet connection is one of the most important assets for every organisation. Therefore, having failing devices and/or connections may represent a major disruption of the organisation's business processes. It also affects one of the pillars (Availability) of the Confidentiality, Integrity and Availability (CIA) triangle and can be classified as a security issue. The following scenario will be implemented at FCSE:

- Network monitoring tools create a notification in the event of a failing Internet connection.
- **TheHive case** will be created by FCC security engineers in order to document all events and steps taken to handle the failed device and/or link.
- Using **TheHive** and **Cortex Redmine Responder**, the FCC manager will assign person(s) to the case and enable himself to be notified of the case progress.
- Depending on the event occurrence behaviour, appropriate action will be taken:
  - For a repeated event, **TheHive case** will be examined for the steps necessary to recover the failed resource. If any new information can be deduced, it will be noted in the case.
  - For a newly occurring event, the security engineer will create a new **TheHive case**, in order to document the information needed for successful event resolution.

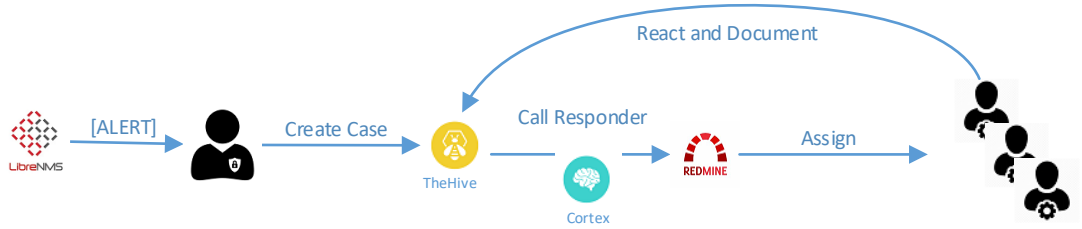

Figure 5.6: Use case workflow: monitoring general reachability of FCSE services

5.3.5 Monitoring Traffic Behaviour and Its Influence on the Local Network

Complex networks, such as the FCSE network, need to be monitored and managed. With increased complexity, a great deal of network traffic may be introduced by auxiliary network elements and services. Even the monitoring and management tools themselves may introduce excess network traffic. There may also be cases of network attacks creating network traffic, that may otherwise be unnoticeable.

As a result of the need to note and analyse traffic and traffic behaviour – on network edges and IXP transit traffic – FCSE is implementing a scenario that should help capture, analyse and document traffic patterns in the local networks:

- LibreNMS [LibreNMS] as a monitoring tool creates alerts and email notifications.
- The IMAP mailbox is polled for new ("unread") messages from **TheHive**, using TheHive4py module. If the email subject contains "[ALERT]", an alert is created; otherwise, a case with a set of predefined tasks will be created.

- The security engineer appoints the **case** to a corresponding network engineer and may invoke **Cortex Redmine Responder** for appointing certain tasks and for tracking purposes.
- **TheHive case** will be used to document the results of task fulfilment and the steps taken to resolve the cause of the unsolicited traffic.

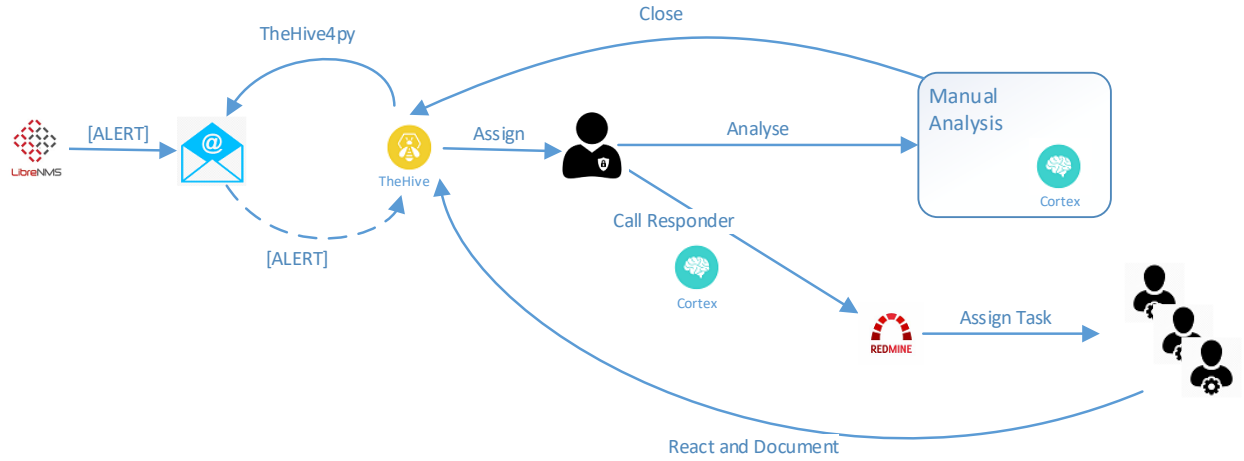

Figure 5.7: Use case workflow: monitoring traffic behaviour and its influence on the local network

5.3.6 Managing General Cases of Hacker Attacks

Exchanging information, regular monitoring of malware information-sharing platforms and sites, updating, network security hardening, etc. are some of the necessary steps that must be taken in order to restrict the influence of unsuccessful or successful hacker attacks. FCC is working on implementing following scenario:

- FCC will use **MISP** as a primary platform for malware information sharing, using feeds from the most relevant sources, both domestic and international:
  - MKD-CIRT MISP platform.
  - Computer Incident Response Centre Luxembourg (CIRCL) Open Source Intelligence Feed (OSINT) and the Botvrij.eu data (included in SOCTools by default).
  - Other feeds that may present themselves as relevant.
- Using information collected through the feeds, as well as their practical knowledge of the network, operating systems and applications, security engineers will identify potential endangered systems and possible attack sources. This information will be used to enrich **MISP events**.
- Event enrichment information may include source IP addresses or domain, destination IP addresses or domain, email addresses or domains, threat actors, files, hashes, etc.
- Using SOCTools' **ELK stack and visualisation**, the security engineer will try to identify possible compromised nodes, as well as possible attack sources and their occurrence in the FCSE network.
- **TheHive case** will be created using the available information, and appropriate **Cortex analysers** will be invoked to further analyse possible threats and incidents.

- If positive identification of an incident is achieved, the security engineer will take the necessary measures to contain and mitigate the threat. All actions will be documented in **TheHive case**.
- An event describing the incident will be created in **MISP** and shared with the community.

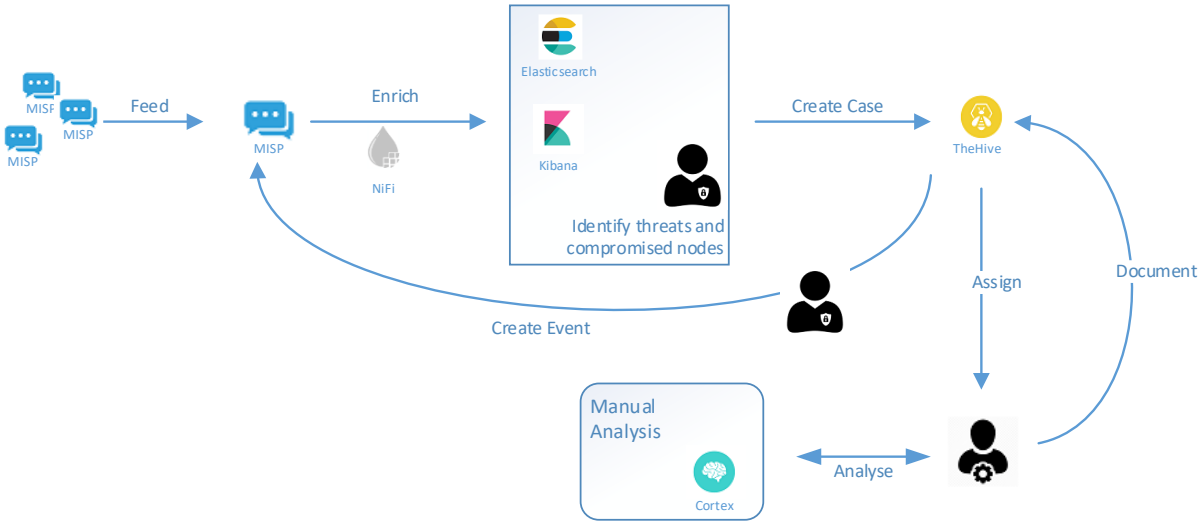

Figure 5.8: Use case workflow: managing general cases of hacker attacks

5.3.7 Managing Usage of FCSE IT Resources during their Entire Lifecycle

The central user portal for requesting IT resources is info.finki.ukim.mk. All users, including students and faculty staff, can request IT resources. These requests need to be evaluated and approved before provisioning the required IT resources. Due to its limitations, the user portal is not a suitable place for managing these resources.

In order to fulfil these goals, FCC is implementing the following workflow:

- For all approved resources, FCC intends to implement lifecycle management via **cases** created in **TheHive**.
- Using **TheHive** and **Cortex Redmine Responder**, the IT manager will create tickets for tasks that need to be executed by certain members of FCC staff.
- Cases will be maintained long term, and all further changes should be logged there by FCC staff, either directly or through Redmine tickets.
- Any incidents involving provisioned IT resources will be associated with the case, **Cortex analysers** will be used to analyse them and, as a result, it may create corresponding **MISP events**.

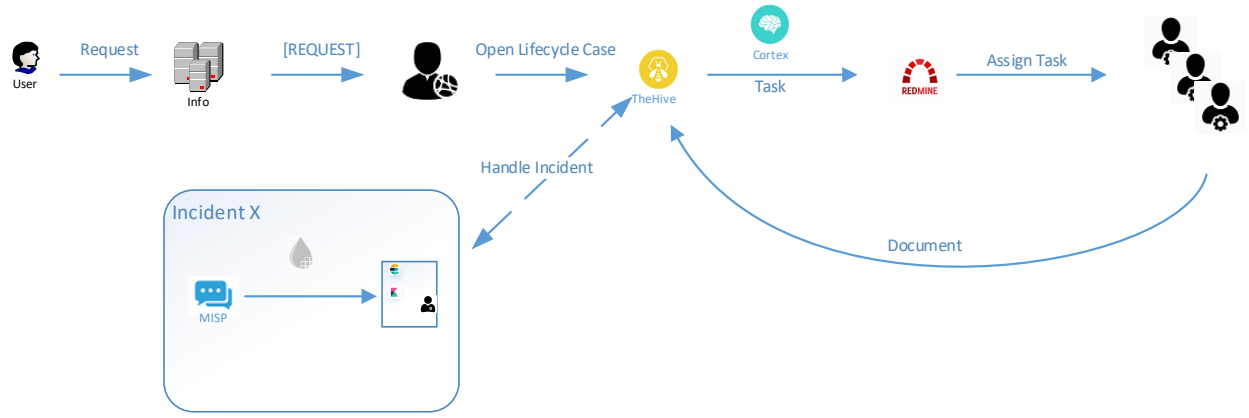

Figure 5.9: Use case workflow: managing usage of FCSE IT resources during their entire lifecycle

5.4 Conclusion and Lessons Learned

Employees from FCSE have been involved in developing and testing GÉANT SOCTools since the beginning of GN4-3, and in all stages of the development and implementation of the SOCTools architecture.

FCSE is aware that building a functioning SOC represents a real challenge, but, as the recent past has shown, it is imperative to increase the security of the institution's network as all kinds of security threats will keep emerging in the future. FCSE regards SOCTools as an important step in the right direction. Most chatter is about implementation of a Security Information and Event Management (SIEM) solution, as if it represents a "silver bullet" that will take care of everything security related. Unfortunately, this is not the case, since a lot of manual effort is still required.

Developing and testing SOCTools has helped FCSE understand how different services can coexist and collaborate in order to produce a range of security-related workflows, and that they can be used to establish a correlation between different network monitoring, system monitoring, ticketing and even accounting tools that the organisation has been using for a long time. There are even services that have been locally developed and used for internal needs. Some of these tools have been mentioned in the use cases since FCSE can develop or has already developed the means to feed their logs and alerts to the SOCTools.

6 CYNET-CSIRT's Founding Journey

6.1 Introduction

This section describes CYNET's journey to establishing and developing a Computer Security Incident Response Team (CSIRT). It covers the following aspects:

- Establishment and mission statement.
- Scope, including types of incidents and level of support; services; and development of tools for cyberattack prevention.
- Generic architecture.
- Test scenarios and results.
- Use case scenario: PYSA ransomware attack.
- Annual CYNET-CSIRT incidents.
- Cooperation, interaction and sharing of information.
- Lessons learned.

Note: although this case study is of a CSIRT, many experiences will be similar for those establishing/maturing a Security Operations Centre (SOC) and the authors felt it was a relevant contribution.

6.2 Establishment and Mission Statement

CYNET-CSIRT [CYNET-CSIRT] is the academic Computer Security Incident Response Team (CSIRT), under the Cyprus National Research and Education Network (CYNET). CYNET-CSIRT was established in 2017 in accordance with the Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR) decision Action No. 358/2010. The effective start date, i.e. when the team became operational, was 1 September 2018. CYNET-CSIRT coordinates incidents on behalf of its constituency. CYNET-CSIRT is authorised to take operational actions regarding vulnerabilities and mitigation of incidents. Such actions may include but are not limited to blocking access to the CYNET network.

CYNET-CSIRT provides incident response and security services to all academic institutions, research institutes and educational networks that are members of the Cyprus National Research and Education Network (CYNET). It provides early warnings, alerts, announcements and dissemination of information

to its constituency and relevant parties regarding risks and incidents. This is accomplished by acting as an intermediary between affected parties and offering, when required, technical advice leading to the resolution of the incident. The affected parties may be internal or external entities to CYNET. CYNET-CSIRT also educates its members about the effects of cyber threats and cyber crime, and trains them to provide early warnings, alerts, announcements and efficient use of the respective tools.

6.3 Scope

6.3.1 Types of Incidents and Level of Support

CYNET-CSIRT is authorised to address all types of computer security incidents that occur, or threaten to occur, at CYNET and its members. CYNET-CSIRT is committed to informing its constituency and to issuing alerts and warnings. Furthermore, it analyses the logs from incidents, vulnerabilities, artefacts and performs incident response. The team actively maintains and tests a list of updated security software tools that are used to assist in various activities such as system audits, vulnerability analysis, antivirus and malware-handling tasks. These tools are available to all interested parties and to the best of the team's knowledge do not contain software that may exploit known or unknown system vulnerabilities. In addition, it collects various documents related to security issues, such as technical "how to" guides, and documentation on system security-related techniques, such as system installations, evidence handling, etc.

CYNET-CSIRT will respond to requests for assistance by other CSIRTs external to CYNET. CYNET-CSIRT will usually respond within the same working day to requests for incident response.

The level of support offered by the CYNET-CSIRT depends on the type of constituent, the severity and the impact of the incident.

6.3.2 Services

CYNET-CSIRT's services can be divided into reactive services, proactive services and security quality management services. Each of these is described below.

Reactive Services

Alerts and Warnings

This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus or hoax, and providing any short-term recommended course of action for dealing with the resulting problem. The alert, warning or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected.

Incident Response and Management

CYNET-CSIRT informs and assists IT-security teams and Network Operations Centres (NOCs) in handling and responding to incidents. In particular, it provides assistance or advice with respect to the following aspects of incident management:

- Incident Triage
  - Investigating the validity of the incident.
  - Determining the operational impact of the incident.
  - Assigning a priority for incident response.
- Incident Coordination
  - Documenting the incident.
  - Coordinating contact with other sites that may be involved.
  - Coordinating contact with CYNET Management.
  - Providing information reports to other CSIRTs.
  - Providing announcements to users, if applicable.
- Incident Resolution
  - Providing technical assistance and analysis of compromised systems.
  - Providing support in restoring affected systems and services to their previous status.
  - Collecting statistics and evidence about incidents that could be used for protecting against future attacks.

If CYNET-CSIRT members are under attack, they may report an incident using the online reporting form that is available on the CYNET-CSIRT website [CYNET-CSIRT_RIForm] or call us at 1490 on a 24/7 basis. Members can also report an incident via email on csirt@cynet.ac.cy.

Proactive Services

The proactive services of CYNET-CSIRT include:

- Issuing security announcements (including, but not limited to, intrusion alerts, vulnerability warnings, and security advisories).
- Development of security tools (see Section 6.3.3).
- Monitoring intrusion detection systems.
- Threat intelligence sharing.

Security Quality Management Services

Besides the technical side of its work, CYNET-CSIRT will perform coordinated actions for:

- Awareness building.
- Education and training.

6.3.3 Development of Tools for Cyberattack Prevention

To supplement the necessary system infrastructure that was adopted based on the best practices of the Open CSIRT Foundation's Security Incident Management Maturity Model (SIM3) and the European Union Agency for Cybersecurity (ENISA), CYNET-CSIRT designed and incorporated an initial selection of self-developed machine-learning-based tools.

The team had to take careful design decisions to strike a balance between different inherent trade-offs. Approaching security from an academic perspective may seem fairly counterintuitive compared with real-world security. For instance, in an academic setting, the goal is innovation. On the other hand, tracking real attack incidents may be much more practical and more important. In order to strike a balance between these two worlds, the team has carefully considered incorporating traditional techniques with modern research-oriented approaches in the underlying technologies, techniques and tools used by CYNET-CSIRT. Each decision on which technologies, techniques and tools should be supported was hard. During the development phase of CYNET-CSIRT, the team decided to:

- Incorporate traditional techniques with modern research-oriented approaches. For instance, one of the tools that monitors network traffic can leverage the advances of modern machine learning.
- Be conservative by leveraging existing services – for instance, for the Malware Classification tool – while, in parallel, offering additional more radical approaches, such as clustering results of the malware analysis for offering rich malware taxonomies.
- Implement small security utilities that solve entirely different problems by realising some basic functionality, which nevertheless can be easily extended.

Following the aforementioned rationale, the team developed the following:

- **Real-Time Data Analysis (RTDA)**: a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. The system passively records network traffic on the entire subnet for identifying particular patterns that are related to documented attacks. Once an attack is identified or abnormal behaviour is observed, the alert is sent to the administrator.

- **Malware Classification (MC)**: a tool for labelling and categorising an unidentified binary file under a particular class or family of other, previously identified, malicious binary files. Such tools are usually operated by domain experts and involve static and dynamic analysis of a given software.

- **Vulnerability Analysis (VA)**: a tool for identifying and classifying potential vulnerabilities in several components in a network such as servers, applications, routers, and firewalls. The tool focuses on particular known vulnerabilities with an assigned Common Vulnerabilities and Exposures (CVE) ID.

The tools are all integrated in a unified modern user interface (UI). Through the UI, a cybersecurity analyst can configure and inspect the progress of the different tools, apply them to particular cases (for instance, analyse a specific program or scan a given host), and export various statistics. For each tool, the team carefully and thoroughly defines the problem that it needs to tackle, enumerates the challenges, and stresses the final rationale behind the approach it followed. This initial setup of security utilities, in combination with an extensive series of open-source tools and other auxiliary tools, such as the Request Tracker for Incident Response (RTIR) ticketing system [RTIR] and our in-house-developed email parser, help the team to automate its services to a great extent.

6.4 Generic Architecture

The Cybersecurity Platform (CYNET-CSIRT/CSP) architecture has been designed and developed based on Model-View-Controller (MVC) web application principles (Figure 6.1). More precisely, the system has two major modules: A. the Windows-based web application module and B. the Linux cybersecurity tools. The web application module is divided into three submodules: a. the administration screens, b. the data analyst screens and c. the reporting screens. All the frontend screens have a backend module to support them which communicates with the controller (Web Logic) of the system. The controller can access the data from or to the database. It can also interact with the APIs subsystem of the project. The APIs subsystem is responsible for communicating with the cybersecurity tools, which are all installed on a Linux virtual machine.

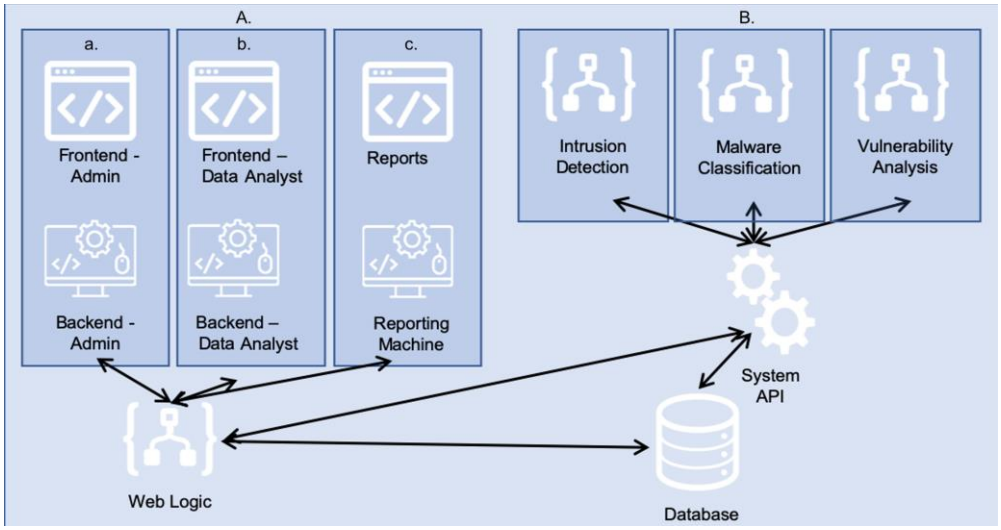

Figure 6.1: CYNET-CSIRT/CSP architecture

6.5 Test Scenarios and Results

As an integrated system, consisting of both hardware and software components, there was a need to have a broader view of the behaviour of the system the team had developed. For this reason, a variety of tests were run to meet a wide range of the team's expectations as cybersecurity analysts. Different categories of tests were carried out, in addition to testing the core functionality shown in Figure 6.1 above. The taxonomy of system tests the team followed is shown in Figure 6.2 below.

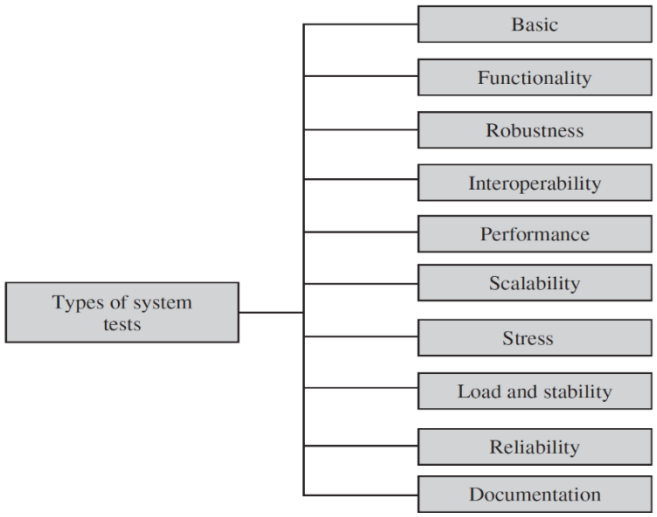

Figure 6.2: Taxonomy of system tests

The results of these tests were very encouraging and showed a high degree of accuracy. More precisely, the team evaluated the RTDA tool with a dataset that contained both benign data and the most up-to-date common DDoS attacks. After running the tool with the aforementioned dataset, 89% of the malicious activity was correctly classified with more than 98% accuracy, leading to a low false-positive rate. Moreover, 99% of the benign activity was correctly classified, while 1% of the benign activity was incorrectly classified, leading, again, to a low rate of false negatives. Additionally, for the MC tool, the percentage of successful identification and classification of malware, compared to results of other respected commercial tools, was more than 90%, while the Vulnerability Analysis tool managed to scan a set of vulnerable hosts (one being a Metasploitable 3 Ubuntu, another one being a Metasploitable 3 Windows 2008, among others) with an overall success rate of more than 99%.

Further changes may be needed in the future, while the team runs the tools in a systematic fashion on an everyday basis and for a long period of time.

6.6 Use Case Scenario: PYSA Ransomware Attack

The COVID-19 pandemic has encouraged cybercriminals to take advantage of cybersecurity weaknesses across many sectors, including the academic environment. In March 2021, the FBI warned of an increase in PYSA ransomware targeting educational institutions [FBI_PYSA]. A PYSA ransomware notification is shown in Figure 6.3. Recently, one of CYNET-CSIRT's members came across such an attack.

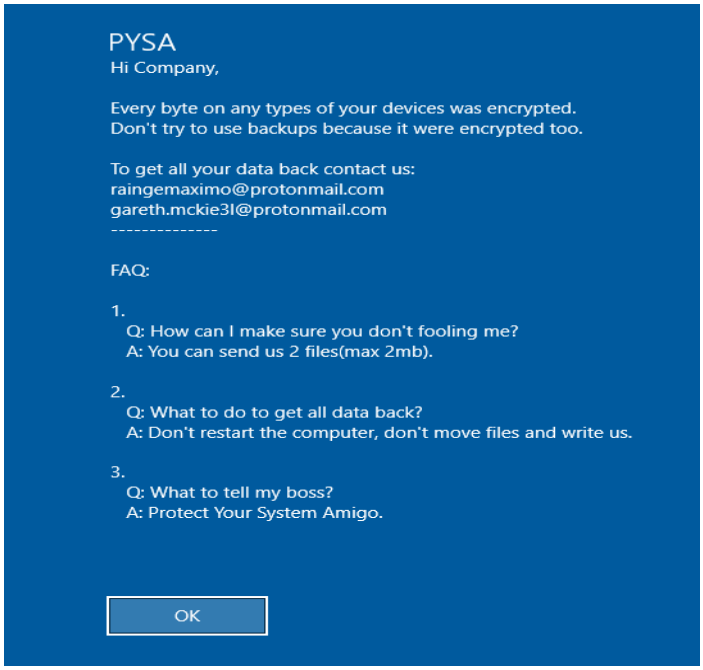

Figure 6.3: PYSA ransomware notification

PYSA (which stands for Protect Your System Amigo) is human-operated ransomware that does not have self-propagation capabilities. Threat actors manually deploy the PYSA ransomware as part of full attack operations. The PYSA ransomware operators typically gain initial access to target systems through phishing email messages or by compromising credentials, such as brute-forcing Active Directory domain credentials or Remote Desktop Protocol (RDP) credentials.

Prior to the deployment of the PYSA ransomware on a compromised system, the malicious actors use publicly available and/or open-source tools for credential theft, stealthiness, privilege escalation, lateral movement, and so on. For example, they use the Advanced Port Scanner [APS] and Advanced IP Scanner [AIPS] tools, which are port-scanning and information-gathering tools that enable users to discover and gather information on services running on network computers.

In addition, the ransomware operators use tools, such as PowerShell Empire [PSE], PsExec [PsExec], etc., for credential theft and lateral movement. Before deploying the PYSA ransomware, the actors execute PowerShell scripts that stop or remove system security mechanisms, such as Windows Defender. They also delete system restore snapshots and shadow copies so that victims cannot restore data encrypted by the ransomware.

The PYSA ransomware is implemented in the C++ programming language and uses the open-source CryptoPP [CryptoPP] C++ library for data encryption. The ransomware encrypts data by applying a hybrid encryption approach that combines the use of the Advanced Encryption Standard – Cipher Block Chaining (AES-CBC) and the RSA encryption algorithms. This is to maximise both encryption performance and security.

As soon as CYNET-CSIRT was informed of the attack, the team proceeded immediately to incident analysis and to the restoration of the institution's systems via its backups.

One of the most significant findings of the team's investigation was, inter alia, the change of the NTDS database location. It seemed that many replays of NTDS database logs had been made and a new LSASS instance had initiated. The ntds.dit file is a database that stores Active Directory data, including information about user objects, groups, and group membership. It includes the password hashes for all users in the domain on every domain controller. To gain access to the ntds.dit file on a domain controller, an adversary must have already gained administrator access to Active Directory. Alternatively, an adversary could compromise the backup solution responsible for backing up domain controllers, and copy the ntds.dit file from a backup. This is a common adversary technique for credentials theft and data compromise.

Furthermore, many login attempts and unauthorised login/logoff events were also detected through the analysis. It seemed that non-technically literate users had been targeted in an attempt by the attacker to steal their credentials.

Another significant finding of the team's forensic analysis was the detection of the failed attempt to execute the so-called "svchost[.]exe" within the faulting application path. From there on the attacker proceeded to dump the domain controller password through LSASS and the NTDS database.

As soon as the team completed its investigation it proceeded with all the necessary remediation recommendations on how an organisation can protect its systems in the foreseeable future. In addition, it has put in place an ongoing training programme for staff to avoid similar pitfalls in the future.

6.6.1 Remediation Recommendations

This is a small sample of CYNET-CSIRT's recommended actions regarding the aforementioned incident.

1. One of the best ways organisations can prevent ransomware from infecting backups is to implement a 3-2-1 backup process strategy:
   3. Hold three copies of the data.
   2. Use two different backup methods or mediums.
   1. Store one copy offline.

2. Use multi-factor authentication (MFA) solutions, including:
   a. Smartcards and cryptographic hardware tokens.
   b. SMS-based one-time passwords (OTPs).
   c. Soft token Software Development Kits (SDKs).
   d. Standalone OTP mobile applications.
   e. Hardware OTP tokens.

3. Block all of the executable files, container formats and files potentially carrying active content from the mail and web gateways.

4. Create monitoring scripts to keep track of systems modifying a lot of files in a short period of time. This monitoring can be used to proactively detect infected systems during encryption.

5. Implement a data loss prevention (DLP) solution. Since confidential data can reside on a variety of computing devices (physical servers, virtual servers, databases, file servers, PCs, point-of-sale devices, flash drives and mobile devices) and move through a variety of network access points (wireline, wireless, VPNs, etc.), there is a variety of solutions that are tackling the problem of data loss, data recovery and data leaks.

6.7 Annual CYNET-CSIRT Incidents

A combination of CYNET-CSIRT's aforementioned services, its in-house-developed cybersecurity platform and the technical expertise acquired through trainings and certifications has contributed significantly to the gradual reduction of cybersecurity incidents. Furthermore, the awareness campaigns offered to CYNET-CSIRT's members made a considerable contribution to the reduction of incidents too, as they boosted members' level of security readiness. As shown in Figure 6.4 below, in 2018 there were approximately 27,000 cybersecurity incidents in the research and education community of Cyprus, while in 2021 these incidents have been reduced to approximately 16,000. The list of incidents includes, without being exhaustive, DDoS attacks, ransomware, phishing and smishing attacks, etc.

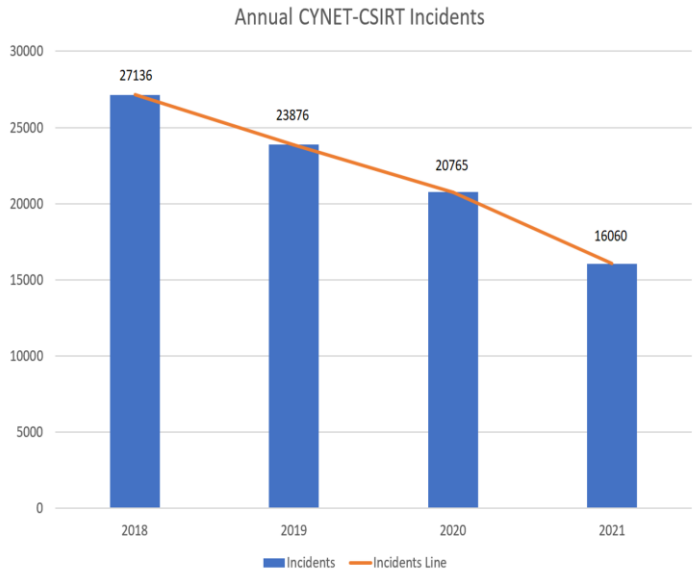

Figure 6.4: Annual CYNET-CSIRT incidents

The team hopes to achieve an exponential reduction of cybersecurity incidents through the new services that CYNET-CSIRT intends to provide in the foreseeable future.

6.8 Cooperation, Interaction and Sharing of Information

CYNET-CSIRT continuously enhances its cybersecurity skills on cutting-edge technologies and state-of-the-art techniques. Also, it has succeeded in being involved in different security projects and establishing joint efforts with other security teams. A big part – and benefit – of these collaborations is the exchange of knowledge and the enrichment of experience. During an incident it is important to have a common understanding and enough maturity to react in a fast and efficient manner, collaborating in a secure way with other teams. The increased ability to communicate with peer entity teams allows faster resolution of computer security incidents, regardless of their source, destination, or transit path.

CYNET-CSIRT recognises the importance of operational cooperation and information sharing between Computer Security Incident Response Teams, and also with other organisations that may contribute towards or make use of their services. All sensitive data and information (personal data, system/service configuration, vulnerabilities with their locations) are transmitted encrypted. CYNET-CSIRT operates in accordance with the GDPR and supports the Traffic Light Protocol (TLP).

More precisely, CYNET-CSIRT has established various international collaborations with other CSIRTs/CERTs (national CSIRT-CY, CERT.PT, GRNET), cybersecurity teams (URAN) and the pan-European data network for the research and education community (GÉANT), among others, for sharing knowledge and experience.

Through those exceptional collaborations, CYNET-CSIRT found its two "sponsors" who nominated the team as one of the prerequisites of the membership process of the Forum of Incident Response and Security Teams (FIRST) and TF-CSIRT Trusted Introducer (TI), respectively. Both of the sponsors are Full Members of FIRST and Certified and Accredited teams of TI, respectively. CYNET-CSIRT worked efficiently with both entities in order for them to acquire a thorough understanding of the team. CYNET-CSIRT succeeded in becoming a Listed team in the Trusted Introducer community on 30 June 2020 (please see [TI_List] for the list of all "listed" teams). Afterwards, CYNET-CSIRT proceeded with the membership process of FIRST, and succeeded in becoming a Full Member on 14 June 2021 (please see [FIRST_CYNET-CSIRT] for all the necessary information). In accordance with its demonstrated and checked level of maturity, CYNET-CSIRT proceeded with its application for TI Accreditation. This verification and feedback cycle was finalised successfully on 19 August 2021. The TI team has verified that CYNET-CSIRT has met all requirements, and CYNET -CSIRT's status has been changed from "accreditation candidates" to "accredited". Although, with the new status, the team gained access to the complete set of TI services, it is considering the possibility of proceeding with the Certification process in order to raise its maturity to a higher level.

CYNET-CSIRT can bring to FIRST and TI its experience in addressing all types of computer security incidents that may occur or threaten to occur in its constituency. It can also bring its considerable experience in developing state-of-the-art machine-learning-based cybersecurity tools and its thorough knowledge of detecting and preventing malicious and abnormal activity in its constituency infrastructure via continuous monitoring of their network.

CYNET-CSIRT's membership in FIRST and TI was an achievement and a step towards a higher level of maturity. Such a membership verifies that the team is following best practices and accepts the necessary procedures for successful collaboration. This official recognition adds value not only to the

team itself but, consequently, to its constituents as well, i.e., achieving a position in the cybersecurity community will lead CYNET's Members to gain more knowledge and insight that will, eventually, have a positive effect on the prevention and protection of CYNET-CSIRT's beneficiaries.

6.9 Lessons Learned

During its cybersecurity journey CYNET-CSIRT has learned many important lessons, including the following:

- The team realised how significant collaborations are and is open to new ones. A big part of a CSIRT collaboration is the exchange of knowledge and the enrichment of experience. This is one of the advantages of being part of the CSIRTs community. You are never alone. The team learns the modus operandi of other teams, and how to avoid the pitfalls encountered by other teams. With this knowledge, CYNET-CSIRT can advance its cybersecurity system too. Equally, the team shares its experience of vulnerabilities, incidents, tools and all other security issues with other colleagues, in order to help them improve cybersecurity for the research and education community of their country, such as the Ukrainian NREN. This can only have positive outcomes and it is a great pleasure every time the team has the opportunity to take part in such collaborations.

- A great lesson learned is that everyone was faced with the impacts of an unexpected circumstance: that of the COVID-19 pandemic. The COVID-19 pandemic, in addition to the upheaval it caused to peoples' lives, families and communities and its continued health threat, also had a significant impact on the team's project plans for the most part of 2020, such as the cancellation and postponement of training and events activities and the exchange of visits with other CSIRT teams.

- Another useful aspect proved to be the pre-existing knowledge of the national CSIRT-CY on fundamental issues, such as the selection of subcontractors. It has proved wise and very effective to collaborate with them, because of their considerable experience and accurate knowledge in the relevant fields.

- Finally, the team realised that finding effective solutions to complex problems is not easy, but with the use of the right methods and state-of-the-art techniques, you can help your team to be **more efficient** in the process.

CYNET-CSIRT's cybersecurity journey has been successful so far, and the team looks forward to its equally successful continuation in the future.

7 Conclusion

This report introduced Security Operations (SecOps) – including goals, benefits and best practices – operational intelligence and Security Operations Centres (SOCs) as a means to practically implement SecOps. SOC organisational models, in/outsourcing considerations, roles, tools and additional recommended reading were included. A good understanding of both SecOps and SOCs serves as a necessary foundation in determining if, when and how an R&E organisation should embark on its own journey to establish or mature a SOC service.

Three R&E case studies were then presented:

SURFsoc case study

This case study reveals the significance of the different SOC models and functions in determining the type of SOC that is most suitable for the environment. In the case of SURF, an internal SNOC (SOC+NOC) initially appeared to be the most logical choice. In practice, however, it emerged that outsourcing the SOC service to an external provider, particularly in the face of recent university ransomware incidents, was the best choice considering the constituency, funding, service availability requirements, etc. The case study illustrates the importance of evaluating the environment and alternatives in close consultation and engagement with all stakeholders, particularly customers. The theoretical and preliminary investigation / proof-of-concept phases, together with a follow-up working group, were invaluable in providing the use cases and business model, and the questions emerging therefrom proved invaluable for the next phase – tender scope and requirements. Although implementation took approximately one year, the service has been extremely successful, with 23 institutions connected to SURFsoc to date. Lessons learned from SURF's experience include:

- A SOC is not a panacea. You are not safe all of a sudden and it does not reduce workload; on the contrary, it increases workload for the organisation.
- Contractual negotiations take time.
- The costs of running/outsourcing a SOC are high.

UKIM FCSE SOCTools use cases

Staff of the Faculty of Computer Science and Engineering (FCSE) at the Ss. Cyril and Methodius University in Skopje (UKIM) have been experimenting with SOCTools [GN_GitLab_SOCTools] to automate and improve several incident response and related processes. This case study scopes their environment, systems and responsibilities before diving into their integration and application of SOCTools to expedite user monitoring, asset and service discovery, logging, general network availability, traffic behaviour, investigations of information security events/incidents, and resource management. SOCTools is shown to be particularly useful for organisations with limited resources and looking to automate similar activities. Integrating the SOCTools components with existing systems was

fairly straightforward and yielded great benefits to the use cases presented. This has helped make the case for a more formal SOC with minimal resource requirements: “Developing and testing SOCTools has helped FCSE understand how different services can coexist and collaborate in order to produce a range of security-related workflows, and that they can be used to establish a correlation between different network monitoring, system monitoring, ticketing and even accounting tools that the organisation has been using for a long time.” With the future developments and integration of SOCTools with other tools from GN4-3 WP8, this will be even further enhanced for other organisations in a similar position.

CYNET-CSIRT’s founding journey

The CSIRT of the Cyprus National Research and Education Network (CYNET) is young compared to many others in Europe. This case study illustrates how developing NRENs can effectively establish a CSIRT (also known as SOC for the most part) with minimal resources and some creativity. CYNET-CSIRT’s journey highlights the importance of buy-in from stakeholders (especially funders), training as well as knowledge exchange and collaborations with forums such as TF-CSIRT (the community that maintains the TI service) and FIRST. Indicators are provided, showing how the basic incident response services can be offered as well as development of tools and even awareness building and training. CYNET-CSIRT staff utilise their design and development skills to provide these services very effectively, with limited resources, yet tailored to the needs of the constituency. Lessons learned include:

- Build and utilise community collaborations – exchange knowledge, share experiences and learn together (do not re-invent the wheel).
- Make the most of major events/incidents to develop SOC capabilities and services.
- Utilise existing knowledge and experience – not just direct technical skills but also in areas such as procurement – to optimise implementation.
- Be creative and build on current knowledge and skill sets to gain efficiency.

These case studies present the experiences of a variety of members of the research and education community (NRENs, university) along their own SOC/CSIRT journeys, illustrating the concepts outlined in Sections 2 and 3 of the report in real-life implementations. Together, these represent a valuable knowledge base for others on their own SOC journeys, particularly those in the research and education sector.

Appendix A SOC Tasks

This appendix includes a list of operational security functions identified in a PvIB expert brief [PvIB]. The list is not exhaustive. Depending on the type of SOC and the principles used, these operational security functions can be performed by a SOC; not every SOC performs all of these functions.

Function	Description
Firewall log analysis, firewall management	Firewall management can be roughly divided into two functions: • Analysis of firewall log files and assessing whether security incidents are occurring. • Management of the entire firewall environment. This concerns the functional and operational management of firewalls (updates to software, hardware and OS, but also the filtering rules). Functional management is generally difficult to separate from operational management of firewalls. Therefore, the management is often done by one party, which can be the SOC.
Intrusion Detection and Prevention (IDP)	IDP systems, like firewalls, need functional and operational management. You could elect to have the monitoring/analysis of IDP logging performed by the SOC. Possible suspicious events and security incidents can then be followed up. When the choice is made to place the entire management at the SOC, a separation of functions (with respect to the regular management organisation) is realised and use can be made of the general security knowledge of the SOC when performing the task.
Vulnerability scanning, penetration testing	An organisation can choose roughly two models for vulnerability scanning: • A vulnerability scan requested by responsible line manager. In this case, the SOC is a service provider to the internal organisation and performs a vulnerability scan when requested by the organisation or department. If desired, the client can ask to have the report analysed by the SOC. • Structural and periodic scanning of the entire domain. With this option, the SOC is commissioned by the (sub)organisation to structurally and periodically scan the entire domain for vulnerabilities and report to the appropriate responsible manager. If the choice has been made to place the responsibility for information security as much as possible with the responsible line manager, option 1 fits best. The line manager just has to demonstrate that the information security has been set up properly, and a vulnerability scan can help with that. Of course, it is less effective if all responsible line managers give a separate assignment to perform a scan. Therefore, option 2 is more interesting for a more mature organisation in the field of vulnerability scanning and information security.

Function	Description
Compliance management	Compliance scanning is similar to vulnerability scanning. The major difference is that with compliance scanning a test is often done on the basis of the corporate security policy based on internal and/or external regulations, while with vulnerability scanning a test is done on the basis of known vulnerabilities. Furthermore, the two variants of service provision that can be assigned to the SOC also apply here: • Execution on behalf of the responsible line manager and thus supporting them in their risk management responsibility. • Periodically performing compliance scans in order to make a structural contribution to the enforcement of a corporate security policy.
Identity and Access Management (IAM)	Once an authorisation request for a particular business application is approved by the owner, the handling of this request can be perfectly well delegated to a SOC. The SOC is then authorised to assign a user to a predefined role. In this situation, it is wise to realise segregation of duties by assigning the management of roles to a separate department to prevent one department from being able to both create roles and assign users to the roles. Either role management or authorisation management can be tasked to the SOC; however, combining the two is not advisable. The SOC then first checks whether the authorisation request in question meets the requirements and authorisation matrix. The major advantage of this method is that all authorisations are handled and documented in one place. When a change in function occurs or if an employee leaves, the authorisations that have to be changed or removed are well documented and handled efficiently.
Risk assessment	The SOC can perform risk analysis in several ways. Risks can be extracted from the analysis of logging, performing vulnerability and compliance scans, and from the analysis of security incidents (also from internal or external CERTs). Thus, these analyses are primarily focused on operational risks, such as identifying increased threats from internal or external attacks.
Key management	More and more cryptographic technology is applied to ensure the confidentiality and integrity of information. Several solutions are applied for this purpose, such as Public Key Infrastructure (PKI), Transport Layer Security (TLS), Pretty Good Privacy (PGP) and the like. These solutions work with electronic keys (symmetric or asymmetric). For electronic keys, two options have been identified: • Key escrow. Management of keys needed in exceptional situations, such as recovering encrypted information where the original key has been lost. The SOC makes electronic keys available based on a rigorously executed procedure. • Key issuance and management. The SOC can supervise the issuance of keys for employees, for example the issuance of certificates at a PKI. This feature provides a single view of which electronic keys have been requested and who is using them.

Function	Description
Digital vault	A digital vault refers to a solution that allows sensitive information such as important documents and/or privileged accounts to be stored encrypted in the infrastructure. It is important to use strong authentication (e.g. 2-factor) for access to a digital safe. The functional management (including the issuing of digital keys) can be entrusted to the SOC in its entirety.
Cyber intelligence	It is important for an organisation to be able to anticipate threats from the Internet. Viruses and spam are two examples of threats that are better managed by organisations today. But newer and more complex threats are emerging. How should an organisation prepare for them? Having knowledge of these threats from the Internet can be invested in the SOC. In doing so, make sure that there is no overlap with tasks that may be assigned to a CERT. But attacks or organised crime directed at the organisation from the Internet should also be identified as quickly as possible. Help from external organisations (such as the NCSC, suppliers or competing organisations) is valuable in this regard. The SOC can organise the information from these sources and distribute it internally to the responsible managers. The SOC can also be used to investigate threats on the Internet itself (such as communications that may pose a threat to the organisation). The SOC then performs a kind of Internet investigation task.
Forensics	The SOC can be used to conduct forensic investigations. Depending on the tasks the SOC performs, the SOC has insight into a lot of security information from different IT systems. In addition, the SOC can have an independent function. Conducting an investigation into possibly unauthorised actions by an employee could be delegated to the SOC. Here it is important that the SOC has the competence to properly handle the specific technical and legal aspects.
Computer Emergency Response Team (CERT)	The SOC can play a valuable role in a CERT. The SOC can assume the role of responsible party for conducting CERT tasks. In the event of a major security incident, the SOC then takes responsibility for limiting consequential damage and restoring primary business processes. Because such incidents require the involvement of several disciplines and also involve major business interests, a CERT is often set up as a separate entity in which the SOC is involved from an operational security perspective.
Data Loss Prevention (DLP)	DLP is very similar to firewall management with respect to tasks for the SOC. The analysis of logging of DLP can be assigned as a task to the SOC, but also the complete operational management of DLP.
Security advice	Because the SOC has a central operational role in security, it is quite possible it also gives advice on security solutions and implementations. Of course, the dual interest that may arise (advice and control) should be carefully considered. But in general this can be well organised internally.
Security Information and	With a SIEM system/service it is possible to recognise and raise alerts on suspicious or unwanted patterns based on logging from IT components, but also from security systems (firewalls, IDS, etc.) and applications. SIEM is often outsourced to a SOC,

Function	Description
Event Management (SIEM)	because a SOC can work independently. In addition, a SOC has the proper knowledge to operate a complex system like SIEM.
Privileged user management	A SOC can play a role in monitoring sensitive accounts. These are accounts within an organisation that have an elevated risk profile. Activities may include user control or monitoring of activities performed by these types of accounts.
Brand protection	A less common function for a SOC is the protection of an organisation's trademarks (brand protection). This involves managing the domain names of the organisation and its variants. The communications department focuses on protecting other expressions (e.g. in the media) of the trademark. A derivative domain name of the organisation may pose a threat to the organisation. If the domain name is "companyX" and someone else opens a website under the name "companyX-news" and posts misleading or other incorrect information on it, this can lead to substantial damage. Therefore a quick and appropriate response is required. The SOC can fulfil the role of guarding the domain name. In addition, brand protection can be used to specifically find information about what outsiders are saying about a company, complaints, plans for attacks. In addition, information can be found in this way about the company, showing that employees do not adhere to company policies. This form can also be extended to brand intelligence, where it looks further into, for example, social media.
Fraud prevention	Because of the complexity of interactions between the various systems and business applications, an overview is needed to detect possible fraud scenarios. A possible approach for this is to house security monitoring for critical applications in a SOC with specialist knowledge. Think, for example, of Internet banking. This type of application is often heavily and separately monitored by banks.

Table A.1: SOC functions (illustrative)

Appendix B Key SOC Tools and Services

B.1 Security Information and Event Management (SIEM)

One of the important tools a SOC needs is a Security Information and Event Management (SIEM) system to analyse all the data, correlate it and generate a proper response, as summarised in Figure B.1:

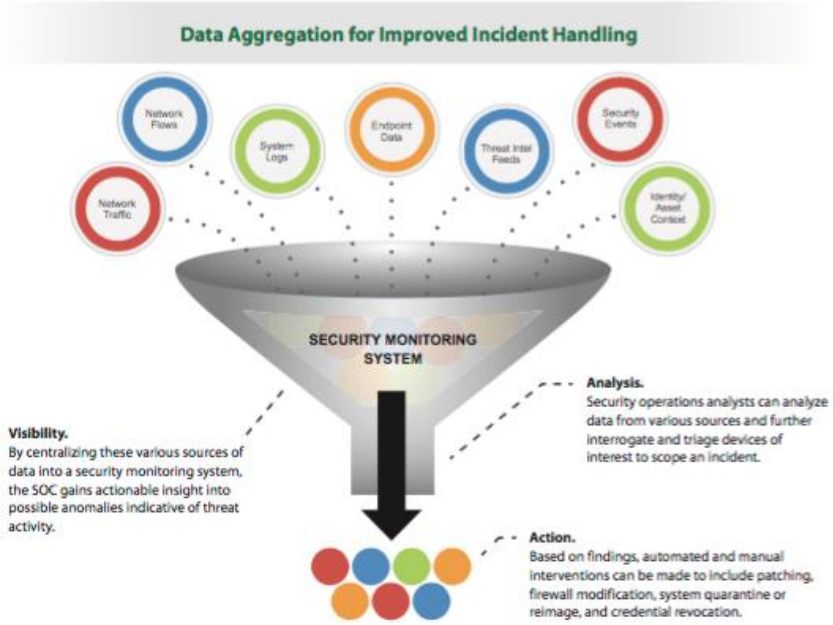

Figure B.1: SIEM (Source: [SANS_Torres]

Examples of SIEM solutions are Elastic Stack/ELK [Elastic_Stack], Splunk [Splunk], Aanval [Aanval] and Cloud SIEM [Cloud_SIEM].

B.2 Threat Intelligence

In addition, a threat intelligence service can provide useful information that can be integrated into the knowledge infrastructure of the SOC. An example of such a service is the (Dutch) National Detection Network (under the banner of the Ministry of Security and Justice), which aims to share threat

information so that participants have the opportunity to take appropriate and timely action to mitigate or prevent potential damage.

Other examples of threat intelligence services are: ThreatConnect [ThreatConnect] (an example of the ThreatConnect dashboard is shown in Figure B.2), AnubisNetworks' Cyberfeed [Cyberfeed], HackerOne [HackerOne], Shadowserver [Shadowserver], Team Cymru [Team_Cymru], Proofpoint/Emerging Threat [Emerging_Threat], AlienVault OTX [AlienVault_OTX], and abuse.ch [abuse.ch].

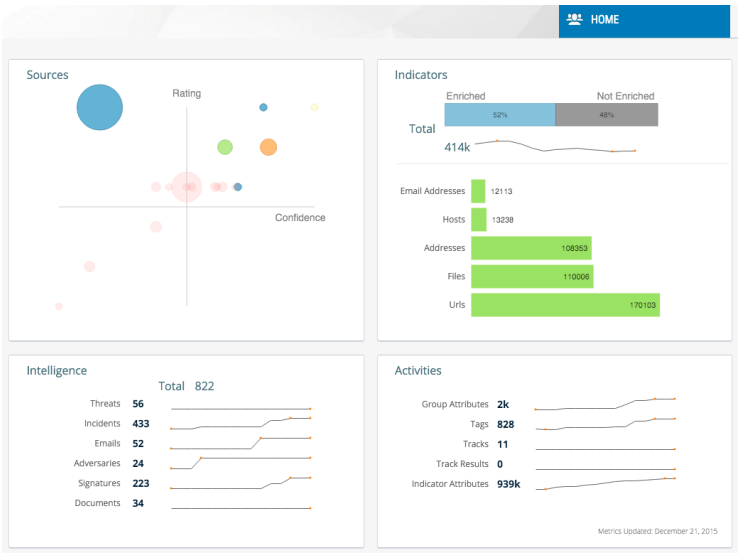

Figure B.2: ThreatConnect dashboard

Which threat intelligence services are appropriate depends largely on the services the SOC has to provide and the resources the SOC has at its disposal, and thus depends on the type of SOC chosen.

References

[Aanval]	https://adaptive.codes/
[abuse.ch]	https://abuse.ch/
[AIPS]	https://www.advanced-ip-scanner.com/
[AlienVault_OTX]	https://otx.alienvault.com/
[APS]	https://www.advanced-port-scanner.com/
[Cloud_SIEM]	https://www.sumologic.com/solutions/cloud-siem-enterprise/
[CompTIA]	https://www.comptia.org/content/articles/what-is-a-security-operations-center
[CryptoPP]	https://www.cryptopp.com/
[CyberArk]	https://www.cyberark.com/what-is/security-operations/
[Cyberfeed]	https://www.anubisnetworks.com/email-security
[CYNET-CSIRT]	https://csirt.cynet.ac.cy/
[CYNET-CSIRT_RIForm]	https://csirt.cynet.ac.cy/report-incident/
[e-Dnevnik]	https://ocjene.skole.hr/login [login required]
[Elasticsearch]	https://www.elastic.co/what-is/elasticsearch
[Elastic_Stack]	https://www.elastic.co/elastic-stack/
[Emerging_Threat]	https://www.proofpoint.com/uk/products/advanced-threat-protection/et-intelligence
[ENISA_HTSUC&S]	https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc
[ENISA_HTSUC&S_PDF]	*How to Set Up CSIRT and SOC: Good Practice Guide*, ENISA, 2020. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc/@@download/fullReport
[ENISA_GPGIM]	https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[FBI_PYSA]	https://www.cisa.gov/sites/default/files/publications/PYSA%20Flash.pdf
[FIRST_CYNET-CSIRT]	https://www.first.org/members/teams/cynet-csirt
[Gartner]	R. McMillan and K. M. Kavanagh, “How to Select a Security Threat Intelligence Service”, Gartner, 2013. https://www.gartner.com/en/documents/2608415
[GN_GitLab_SOCTools]	https://gitlab.geant.org/gn4-3-wp8-t3.1-soc/soctools
[HackerOne]	https://www.hackerone.com/
[HEISC_SOC_CS]	https://library.educause.edu/resources/2019/6/security-operations-center-soc-case-study
[HEISC_SOC_CS_PDF]	*Security Operations Center (SOC) Case Study: HEISC Working Group Paper*, HEISC, 2019. https://library.educause.edu/-/media/files/library/2019/6/HEISCsoc.pdf
[iKnow]	https://iknow.ukim.edu.mk [login required]
[iLearn]	https://ilearn.ukim.edu.mk [login required]

[Keycloak] https://www.keycloak.org/

[Kibana] https://www.elastic.co/what-is/kibana

[LibreNMS] https://www.librenms.org/

[Microsoft] https://docs.microsoft.com/en-us/azure/architecture/framework/security/monitor-security-operations

[MISP] https://www.misp-project.org/

[MITRE_11Strategies] https://www.mitre.org/11strategies

[MITRE_11Strategies_PDF] K. Knerler, I. Parker and C. Zimmerman, *11 Strategies of a World-Class Cybersecurity Operations Center*, MITRE, 2022. https://www.mitre.org/sites/default/files/publications/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

[MK_IXP] https://ixp.mk

[MK_LMS] https://lms.schools.mk [login required]

[MojTermin] https://mojtermin.mk [login required]

[NiFi] https://nifi.apache.org/

[NIST_CF] https://www.nist.gov/cyberframework

[NIST_SPC] "Security and Privacy Controls for Information Systems and Organizations", NIST Special Publication 800-53, Revision 5, NIST, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[NORA_Online] http://www.noraonline.nl/wiki/Patroon_voor_security_information_event_management

[Open_Distro] https://opendistro.github.io/for-elasticsearch/

[Palo_Alto_Networks] https://www.paloaltonetworks.com/cyberpedia/what-is-security-operations

[PSE] https://github.com/EmpireProject/Empire

[PsExec] https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

[PvIB] K. Rorive, M. Beerends, L. Bordewijk, F. Breedijk et al., "Security Operations Center: Een inrichtingsadvies", PvIB, 2011. https://www.pvib.nl/kenniscentrum/documenten/expertbrief-security-operations-center-een-inrichtingsadvies/downloaden

[Rijnders] G. Rijnders, "Inzichtelijk maken beveiliging", Utrecht, 2015.

[RTIR] https://bestpractical.com/rtir

[SANS_Shackleford] D. Shackleford, "Who's Using Cyberthreat Intelligence and How?," SANS, 2015. https://cdn-cybersecurity.att.com/docs/SANS-Cyber-Threat-Intelligence-Survey-2015.pdf

[SANS_Torres] A. Torres, "Building a World-Class Security Operations Center: A Roadmap", SANS, 2015. https://www.academia.edu/38868050/Building_a_World-Class_Security_Operations_Center_A_Roadmap

[ServiceNow] https://www.servicenow.com/products/security-operations/what-is-secops.html

[Shadowserver] https://www.shadowserver.org/

[Shodan] https://www.shodan.io/

[Splunk] https://www.splunk.com/

[Sumo_Logic] https://www.sumologic.com/glossary/secops/

[SURFcert] https://www.surf.nl/en/surfcert-247-support-in-case-of-security-incidents
[SURFinternet] https://www.surf.nl/en/surfinternet-fast-and-reliable-internet-connection
[Team_Cymru] https://team-cymru.com/
[TheHive] https://thehive-project.org/#
[ThreatConnect] https://threatconnect.com/
[TI_List] https://www.trusted-introducer.org/directory/country_LICSA.html
[TLP] https://www.first.org/tlp/
[UKIM_Help] https://help.ukim.mk
[UKIM_Repos] https://repository.ukim.mk

Glossary

AD	Active Directory
ADD	Active Directory Domain
AES-CBC	Advanced Encryption Standard – Cipher Block Chaining
API	Application Programming Interface
A/V	Audio/Visual
AWS	Amazon Web Services
CAS	Central Authentication Service
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity and Availability
CIRCL	Computer Incident Response Centre Luxembourg
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
CompTIA	Computing Technology Industry Association
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DMZ	Demilitarised Zone
DDoS	Distributed Denial of Service
DoS	Denial of Service
ELK	Elasticsearch, Logstash, and Kibana
ENISA	European Union Agency for Cybersecurity
FBI	Federal Bureau of Investigation (US)
FCC	Computer Centre (UKIM FCSE)
FCSE	Faculty of Computer Science and Engineering (UKIM)
FIRST	Forum of Incident Response and Security Teams
FoD	Firewall on Demand
GDPR	General Data Protection Regulation
GPGPU	General Purpose Computing on Graphics Processing Units
HEISC	Higher Education Information Security Council (US)
HTTP/S	Hypertext Transfer Protocol/Secure
IAM	Identity and Access Management
ICT	Information and Communications Technology
IdP	Identity Provider
IDP	Intrusion Detection and Prevention
IDS	Intrusion Detection System

IMAP	Internet Message Access Protocol
IoC	Indicator of Compromise
IP	Internet Protocol
ISAC	Information Sharing and Analysis Centre
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LSASS	Local Security Authority Subsystem Service
MC	Malware Classification
MFA	Multi-Factor Authentication
MISP	Threat Intelligence and Sharing Platform (formerly known as Malware Information Sharing Platform)
MoES	Ministry of Education and Science (North Macedonia)
MoH	Ministry of Health (North Macedonia)
MSSP	Managed Security Service Provider
MVC	Model-View-Controller
NCSC	National Cyber Security Centre (UK)
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology (US)
NMS	Network Monitoring System
NOC	Network Operations Centre
NREN	National Research and Education Network
NTDS	NT Directory Services
OCECPR	Office of the Commissioner of Electronic Communications and Postal Regulation (Cyprus)
OS	Operating System
OSINT	Open Source Intelligence Feed
OTP	One-Time Password
OTX	Open Threat Exchange
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PvIB	Platform voor InformatieBeveiliging (Information Security Platform)
PYSA	Protect Your System Amigo
R&E	Research and Education
RAS	Remote Access Service
RDP	Remote Desktop Protocol
RSA	An asymmetric cryptography algorithm named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman
RTDA	Real-Time Data Analysis
RTIR	Request Tracker for Incident Response
SAML	Security Assertion Markup Language
SDK	Software Development Kit
SecOps	Security Operations
SIEM	Security Information and Event Management
SIM3	Security Incident Management Maturity Model
SIS	Schools Information System
SLA	Service-Level Agreement
SMS	Short Message Service

SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNOC	Security & Network Operations Centre
SOC	Security Operations Centre
SOP	Standardised Operating Procedure
TF	Task Force
TF-CSIRT	Task Force on Computer Security Incident Response Teams
TI	Trusted Introducer
TLP	Traffic Light Protocol
TLS	Transport Layer Security
UI	User Interface
UKIM	Ss. Cyril and Methodius University in Skopje
UTM	Unified Threat Management
VA	Vulnerability Analysis
VPN	Virtual Private Network
WP	Work Package
WP8	GN4-3 Work Package 8 Security
XML	Extensible Markup Language