



D2.1

**Cyber Incident handling Trend
Analysis**

Project number:	833683
Project acronym:	CyberSANE
Project title:	Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures
Start date of the project:	1 st September, 2019
Duration:	36 months
Programme:	H2020-SU-ICT-2018

Deliverable type:	Report
Deliverable reference number:	DS-01-833683 / D2.1/ Final 0.8 2020_CSN_RP_05_Deliverable 2.1_Cyber Incident Handling Trend Analysis_v1
Work package contributing to the deliverable:	WP 2
Due date:	01/03/2020
Actual submission date:	02/03/2020

Responsible organisation:	Inria
Editor:	Inria
Dissemination level:	PU
Revision:	V2.0

Abstract:

This deliverable describes the different incident handling trend analysis performed in Task T2.1. It provides a categorisation of attacks, a description of the different tools identified to be used in the design and development of the CyberSANE infrastructure. In addition, it reviews the related standards and provides the best practices to follow in the rest of the project.

Keywords:

Attacks categorisation and trends, standards, tools



Editor

Nathalie Mitton (Inria)

Contributors (ordered according to beneficiary numbers)

Luís Landeiro Ribeiro (PDMFC)

Luis Miguel Campos (PDMFC)

Oleksii Oслиak (CNR)

Stefen Beyer (S2)

Sergio Zamarripa (S2)

Valeria Loscri (Inria)

Nathalie Mitton (Inria)

Edward Staddon (Inria)

Mania Hatzikou (MAG)

Athanasios Karantjias (MAG)

Spyridon Papastergiou (MAG)

Sophia Karagiorgou (UBI)

Manos Athanatos (FORTH)

Georgios Spanoudakis (STS)

Paris-Alexandros Karypidis (SID)

Anastasios Lytos (SID)

Umar Ismail (UoB)

Haris Mouratidis (UoB)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author’s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability

Contents

1. Introduction	1
2. Cyber Threat and Attacks	2
2.1. Categorisation of threats	2
2.2. Application to Critical Information Infrastructures (CIIs)	12
2.3. Requirements for Critical Information Infrastructures (CIIs)	13
3. Background Solutions Relevant to CyberSANE	14
3.1. eMAS SOM	14
3.2. SiVi Tool	16
3.3. L-ADS	17
3.4. XL-SIEM	18
3.5. CARMEN	20
3.6. OLISTIC Enterprise Risk Management Suite	21
3.7. MEDUSA Cyber Intelligence Suite	23
3.8. Evidence-driven Maritime Supply Chain Risk Assessment (MITIGATE) System	24
3.9. Metadon SIEM	29
3.10. Chimera	31
3.11. SPA	33
3.12. Other Solutions	35
4. Standards, guidelines and best practices	62
4.1. Security Management Standards	62
4.2. Mapping of CyberSANE Solutions to Domains	73
4.3. Open issues, and future challenges in Critical Information Infrastructure Protection	74
5. Conclusion	77
6. List of Abbreviations	79
7. References	84

List of Figures

Figure 1: OSI model, Internet / IoT stack comparison	3
Figure 2: Generalised categorisation for Cyber-Attacks	3
Figure 3: Network-Layer example of the Cyber-Attack Categorisation	3
Figure 4: Incident Handling Life Cycle [94]	4
Figure 5: emas [®] SOM default operational process diagram.....	15
Figure 6: SiVi Tool User Interface	16
Figure 7: L-ADS concepts chart.....	18
Figure 8: XL-SIEM concept chart.....	19
Figure 9: Evidence-driven Maritime Supply Chain Risk Assessment (MITIGATE) System.....	26
Figure 10: MITIGATE High Level Architecture	27
Figure 11: Chimera Diagram.....	31
Figure 12: Chimera Supported Connectors	32
Figure 13: Example of Data Anonymisation with Hashing.....	33
Figure 14: Elastic SIEM Stack	37
Figure 15: IBM Resilient.....	40
Figure 16: Splunk Phantom Example [138]	40
Figure 17: Splunk Phantom Playbook Example.....	41
Figure 18: Types of Cyber Attacks on CI. Image source [48].....	75

List of Tables

Table 1: Strengths and Weaknesses of emas [®] SOM	16
Table 2: Strengths and Weaknesses of L-ADS.....	18
Table 3: Strengths and Weaknesses of XL-SIEM	20
Table 4: Strengths and Weaknesses of CARMEN	21
Table 5: Strengths and Weaknesses of Metadon	31
Table 6: Strengths and Weaknesses of Chimera.....	33
Table 7: Strengths and Weaknesses of SPA	34
Table 8: SIEM Pros and Cons	57
Table 9: SOAR Pros and Cons	57
Table 10: Forensics Pros and Cons.....	58
Table 11: NBADS Pros and Cons	59

D2.1 – Cyber Incident Handling Trend Analysis

Table 12: Honey Pots Pros and Cons	59
Table 13: NAC Pros and Cons	60
Table 14: EDR Pros and Cons	61
Table 15: Cyber-Security Standards Compliance Domains	71
Table 16: Mapping of Cyber-Security Standards to Security Domains	72
Table 17: CyberSANE Solutions to Domains	74

1. Introduction

This deliverable includes the outcome of the Trend Analysis, performed as part of Task T2.1. Task 2.1 has been devoted to the elicitation, analysis and documentation of trends associated with the effective and efficient prevention, detection, response and mitigation of various advanced persistent threats against Critical Information Infrastructures (CIIs). In this context, this task provides a desk research assessment of the available cyber threat detection and risk management tools and technologies with respect to their suitability in the CIIs. Systems and frameworks, used in various security-related projects, and best practices are also assessed against their applicability in CyberSANE. In addition, emphasis is laid on capturing the incident handling awareness of the involved CIIs.

In this deliverable, we first provide a categorisation of inventoried attacks that could occur on a Critical Information Infrastructure (Section 2) from an overview of different categorisation approaches. We continue with an outline of the main approaches and techniques in identification, detection and the different manners in responding to threats efficiently. This section will be used as a basis for two deliverables, providing the categorisation and detection approaches for further study in deliverable **D3.1 – Taxonomy of threat landscape for CIIs**, and the response methodologies through the presentation of Incident Handling techniques in deliverable **D5.1 – Prevention and response to advanced threats and anomalies**.

The detection methods presented will pave the way to the study of the different tools which exist (Section 3) and how they could be used in the CyberSANE framework. Their different applications towards efficiently securing CIIs against the afore mentioned attacks will also be studied. Each tool will present its strengths as well as its limitations, but also how they could apply their methodological approach to the envisioned CyberSANE framework.

Finally, since these tools must operate seamlessly on devices and evaluating traffic, they must abide by different security standards which will be defined and presented (Section 4). Here we shall highlight the important elements which must be respected and detail the relevant best practices which will guide the work during the rest of the project. This presentation will guide the development of the system architecture which will be presented in **D2.4 – System architecture and technical specifications**.

The work achieved in this deliverable will serve as a base reference document to the other WPs and deliverables of the project since it gathers main information useful for the project. The general instructions to follow all along the deployment of the CyberSANE infrastructure will guide our achievements to assure the correct establishment of an acceptable result.

2. Cyber Threat and Attacks

One of the largest leap forwards in computer history was the creation of an interconnected web now known as the Internet. In recent years, with the adoption of wireless technologies as the industry standard for inter communication, more and more devices are being connected to this web. This network paradigm has opened the door to numerous possibilities in the industry as well as the home. Devices can therefore send data to distant servers, such as in remote sensor networks, or even be controlled from across the globe, such as turning off a central heating system.

However, this connectivity comes at a cost. When a device is connected to the outside world, it is linked to hundreds of thousands of other people, not all of whom have good intentions. These devices are therefore at risk of a Cyber-Attack, with objectives ranging from stealing private information to taking control of the victim device, causing potentially catastrophic damage, or even death. Consequently, it is important to categorise these possible attacks and explore the different handling and response techniques, detection techniques as well as different risk management methodologies.

This section will not go into specifics, but will present a global overview of the various Cyber-Threats and Cyber-Attacks which exist, as well as a proposed threat categorisation. Incident handling methodology, followed by various threat detection approaches will also be presented. Finally, the notion of risk management will be explained. These notions may be further explored and detailed in future project deliverables.

2.1. Categorisation of threats

Before the different techniques and approaches for cyber detection and attack countering can be examined, it is important to understand the notion of Cyber-Threat and Cyber-Attack. Although generally assimilated to meaning the same thing, as in [109], there is a difference between the two. In [110], a Cyber-Threat is presented as a potential means to violate the security of a certain Cyber-Physical System (CPS). A Cyber-Attack on the other and is explained as a physical attempt to gain unauthorised access to a system or its data, as well as going against normal system operation. An example of this would be where a non-patched smartphone presents a vulnerability allowing an attacker access to the persons messages. A Cyber-Threat would be the presence of this vulnerability breaching the integrity of the device's security, whereas a Cyber-Attack would be the attempt to extract these messages, or installing a trojan to forward messages directly to an undisclosed location. An overview of Cyber-Threats as well as the top 15 threats and trends in 2018 is available in [108].

With this definition, we can now examine various structural principals to organise the different possibilities into distinct categories. Previous works such as [1], [2] and [3] each used different means to categorise various attacks. Gupta in [1] categorised different attacks based on their impact such as Authentication, Confidentiality or Integrity. On the other hand, Singh et al. [2] defined their attacks based on the methodology, such as Man in the Middle (MitM), Denial of Service (DoS) or Brute Force. As for Elbez et al., they based their work in [3] on the specific attack targets relative to Smart Grids, targeting power and energy systems, the Information Technology (IT) controllers or all network communications. In this case, we notice that the classification is use case specific, which, in using for a global categorisation, is not possible.

To implement a global Cyber-Attack categorisation scheme, a common standing ground is needed. Such a thing is presented in [4], [5] and [6]. In their paper, Chelli [4] categorised attacks into three large categories: Goal-Oriented, Performer-Oriented and Layer-Oriented. Goal-Oriented Attacks, also presented by Shahzad et al. in [5], can be decomposed into two distinct categories: Active and Passive. As their names state, they separate attacks whose goal is to simply listen and not intervene from attacks designed to destroy or wreak havoc. Performer-Oriented Attacks depend on where the attack takes place, whether from the outside of the network, or from the inside. As for Layer-Oriented Attacks, also presented by Karchowdhury et al. in [6], the different attacks are defined dependent on where they occur in the Open Systems Interconnection (OSI) network model.

Since Cyber-Attacks are most commonly initiated through, but not limited to, a network connection, it is therefore logical to use the OSI model. Through its standardised nature, it can be used to specify the different

protocols used in various networking paradigms. The most common being the Internet Stack, for everyday activities traversing the Internet, but it also specifies information relative to the rising Internet of Things (IoT) environment. Figure 1 shows a comparison between the two network stacks relative to the OSI model. Using this model, it is now possible to structure and classify all attacks, dependent on their intended behaviour. The advantage of this approach is to remove redundant appearances of the same attack in multiple categories since no identical attack can exist on multiple layers. It is also possible to specify further by incorporating the same Goal-Oriented approach presented in [4] and [5] to each layer of the OSI model. One factor of Cyber-Attacks which is more than often overlooked, is the notion of Physical Cyber-Attacks. In this case, the attacker is in direct contact with the target machine, allowing them to remove and replace hardware or data, or even install a back door, allowing access from the outside world. This also includes insider attacks where a disgruntled employee can turn on their company causing damage to cyber systems or granting access to outside malicious entities.

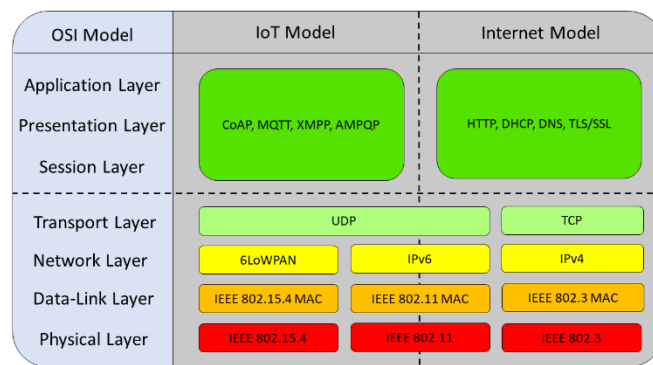


Figure 1: OSI model, Internet / IoT stack comparison

As Singh et al. pointed out in [2], two large categories of attack methodology are MitM and DoS attacks. MitM attacks force traffic to transit through an attacking device, allowing information theft as well as information modification. DoS attacks on the other hand reduce the availability of a specific service, severely impacting network efficiency or even rendering the target unavailable. These methodologies can be applied to various attacks regarding the consequences which could lead to a DoS or using MitM to execute specific attacks.

From these different categorisation methodologies, we can create a Cyber-Attack classification model, adaptable to multiple network paradigms. With the reduction of redundant apparitions of each attack, it is easier to associate them with specific layers and goals. However, many attacks can possess different goals and, therefore, impact different layers. Such is the case of DoS attacks for example, which can be done through various means on different network layers to achieve different objectives. That being said, it is possible to deconstruct certain attacks to identify singular techniques and approaches, thus associating them with a specific layer and goal.

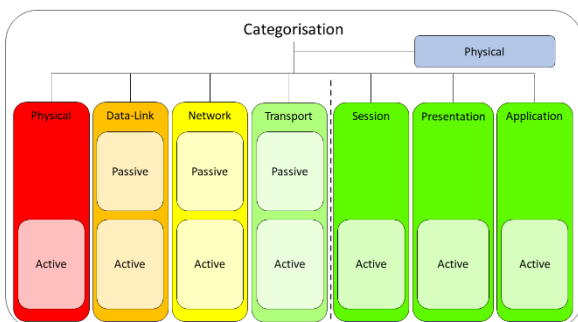


Figure 2: Generalised categorisation for Cyber-Attacks

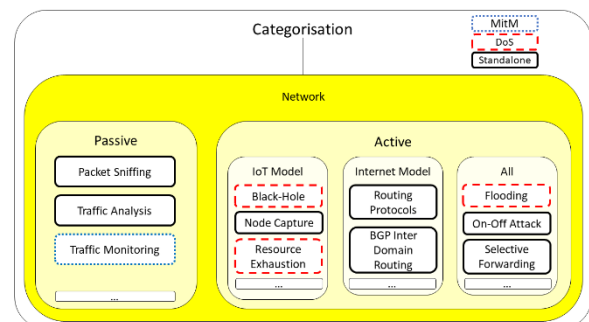


Figure 3: Network-Layer example of the Cyber-Attack Categorisation

On top of this, Cyber-Attacks are not all possible across paradigms or protocols, such as TCP/IP specific attacks cannot occur when UDP is used, or dependant on the physical organisation of the network, such as IoT devices compared to a standard computer. Thus, certain Active attacks on various layers need to be categorised further, separating for example where possible specific attacks on the Internet Stack from those on the IoT Stack. Although certain attacks impact both paradigms, many exist impacting either one or the other, such as upper layer protocol based attacks as presented in Figure 1 (HTTP – Internet + CoAP – IoT) or even lower layer protocols such as the use of 6LoWPAN on IoT devices. This separation helps organise attacks based on their implementation, reducing the need to study non applicable attacks.

On top of this categorisation, it is possible to go even further in distinguishing attacks. As presented previously, there are two types of attack which contain a multitude of different methodological approaches: DoS and MitM. These attacks can impact different layers as well as different protocols or stacks, so it is necessary to identify these attacks in their various categories. To do so, another categorisation will be added to the overall model to differentiate each attack as either a DoS, MitM or an independent standalone attack. This overall proposition is presented in Figure 2 and a brief example of the categorisation applicable to the Network-Layer is presented in Figure 3.

2.1.1. Incident Handling and Response Techniques & Approaches

Where Cyber-Attacks are concerned, there are different means of handling the consequences depending on the impact of the attack. Firstly, we will examine the notion of Incident Handling, as well as different Response Techniques.

In [94], NIST presents a guide to the Cyber-Incident Handling process. This concerns all elements necessary for an IT department to adequately detect, identify, respond, protect and recover. This also includes training users and operatives in the notions of security awareness, thus reducing the risk of attacks resulting from accidental erroneous operations. In [7], Cyber-Incident Handling in a cloud context is examined where it is explained that Incident Handling is part of a larger process called Incident Management [107]. Incident Handling itself contains four steps in order to adequately respond to an incident, presented in Figure 4.

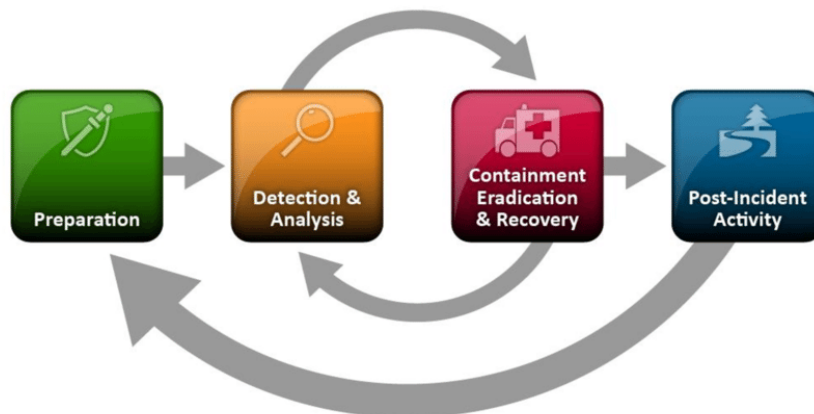


Figure 4: Incident Handling Life Cycle [94]

2.1.1.1. Preparation

The first step in Incident Handling is the Preparation phase. This phase is necessary to create a state of forensic readiness, thus reducing the impact of a security incident and allowing continuous functionality. This preparation assures the system is well prepared for any unforeseen events. A popular approach to pre-incident preparation is the Information Security management, such as training and policy compliance. From a technological perspective, logical security control must be addressed. This is done by implementing certain protection schemes such as firewalls, vulnerability assessments or network monitoring. This is complemented by physical and environmental protection. A Computer Security Incident Response Team (CSIRT) is also

important, as they determine what has happened, what should be done to remedy such happenings and implement the chosen solution.

2.1.1.2. Detection and Analysis

The next phase is called Detection and Analysis and starts when suspicious or unusual events are detected or reported. These events can be anything from an unfamiliar file name to suspicious entries into a network system account and can originate from an automated Intrusion Detection System (IDS) or from manual reporting. After an incident is detected, the resulting data is analysed to determine its validity and the potential impacts to core services. Risk management, containing assessment, mitigation and evaluation, is important to estimate potential damage and determine how to prioritise incident handling in multi-attack scenarios.

2.1.1.3. Incident Response (IR)

The Incident Response (IR) phase occurs soon after the previous phase to mitigate harmful impacts in a quick and efficient way. Since no attack is the same, it is not possible to have a generalised response. The strategy must therefore be adapted from multiple possible criteria such as the potential damage or theft of resources, the necessity of service availability and the duration of the response impacting functionality. This response can be decomposed into three steps: Containment, Eradication and Recovery. Containment and Eradication can often be achieved at the same time, since shutting down a machine, isolating a contamination or blocking all incoming traffic can both isolate and remove a threat. The Containment choice is naturally dependent on the threat perceived, but other factors are also taken into account, such as the availability of the service impacted, the duration and resources needed, but also the need to preserve any evidence. This last element is significantly important as it must follow strict guidelines to be admissible in legal proceedings. Once contained, in depth Eradication can take place to remove any infected software or resources before lifting returning the victim device back into the network. The last step Recovery, emphasises the importance of improved performance techniques and the utilisation of advanced backup technologies, such as online backup or cloud storage.

To react quickly, an automated system capable of responding to an attack by deploying mitigation techniques dependent on the incident scenario is necessary. It is also important for the system to possess a low delay time between the detection and the response, especially in complex multistage attacks. An example is the Automated Intrusion Response System (AIRS) which possesses significant improvement in IR rate. There are three approaches to incident mapping: Static, Dynamic and Cost-Sensitive as presented in [7].

2.1.1.3.1. Static Mapping

Static Mapping uses a pre-defined database, associating a specific incident alert to a specific response. The database is built from previous experience using probabilistic cognitive maps. Although its implementation is relatively simple, it doesn't protect itself entirely from a potential exploitation. Due to its static nature, attackers can circumvent the system by assuming a specific response to their attack. One way to rectify this vulnerability is to render the response strategy dynamic.

2.1.1.3.2. Dynamic Mapping

Using this new dynamic response strategy, Dynamic Mapping is capable of selecting a response based on the context of the incident and not a pre-defined response as before. This allows the system to dynamically adapt to attacks, making it harder to predict and therefore circumvent. However, this solution does not consider the damage or response cost, thus entertaining the possibility of an inappropriate response processing a larger cost than that of the incident itself. The necessity to compare max possible damage costs with those of possible responses increased the interest of cost-sensitive mapping.

2.1.1.3.3. Cost-Sensitive Mapping

A Cost-Sensitive Mapping technique is key to being able to balance both damage and response costs. This allows to reduce the cost of implementation as well as the amount of necessary resources, the temporal effectiveness and the cost of induced modifications. The three major cost factors which are examined are

Damage (amount of damage to target resource), Response (cost of acting on an intrusion) and Operational (cost of processing the IDS).

2.1.1.4. Post-Incident

After an incident has been resolved, Post-Incident processing must be done. It is the final phase where information and results are used as feed-back to improve future incident handling. Using Adaptive Incident Learning, the system and users have the ability to change and learn from past experiences. The information collected from the three previous phases is used to generate a Post- Incident Report explaining the incident as well as possible improvement recommendations in incident handling from both a technical and a managerial perspective. It is the least studied phase of the Incident Handling system.

2.1.1.5. Digital Forensics

Incident Handling focuses mainly on responding to incident breaches without general consideration for evidence collection. This evidence could provide valuable data for current investigations but also the future prosecution of the offender. Using similar security tools as Incident Handling, Digital Forensics is a scientific discipline concerning the collection, analysis and interpretation of digital data connected with a computer security incident. Using legally admissible methods, the recovered data from compromised systems can help reconstruct incident facts but also can be used for risk mitigation in the Post-Incident phase. Integrating Digital Forensic analysis into the Detection and Analysis phase can facilitate the identification of key assets as well as vulnerabilities and threats which could be exploited. Appropriate and effective risk assessment and mitigation strategies help ensure the system is forensic ready, thus when an incident occurs, responding investigators know where potential evidence can be found. This facilitates efficient and timely incident response and forensic examination. A version compatible with Critical Infrastructures (CIs) based on Supervisor Control and Data Acquisition (SCADA) forensics architecture is presented in [8].

2.1.2. Intrusion & Anomaly Detection Techniques & Approaches

Detecting different Cyber events is an active research domain. There are many different techniques for Cyber-Detection, both for a specific attack type or general event detection. Firstly, there are two large categories of Cyber-Attacks where detection techniques differ: Anomalies and Intrusion. Anomalies are abnormal behavioural patterns detected in network traffic and internal IT systems. These patterns indicate something which has changed in the network, either an external attack underway or even an Intrusion. As its name states, in the same way as a thief can enter unauthorised into a building, an Intrusion is the unauthorised access into a computer network or system, allowing unrestricted access.

In [9], Khraisat et al. presented two types of IDS based on two different approaches. The first named Signature-based Intrusion Detection System (SIDS), is a knowledge-based detection system which uses pattern matching techniques from a database containing intrusion signatures. It therefore compares packets in real time to known signatures, raising an alarm if an attack is detected. However, it is incapable of detecting zero-day attacks since no possible signature exists as well as multi-packet attacks due to its packet-by-packet analysis methodology. The other, Anomaly-based Intrusion Detection System (AIDS), uses multiple approaches to compare detected traffic to a “normal” traffic model and can therefore overcome the limitations of SIDS through machine-learning, statistical or knowledge-based methods. Its principal works on assuming that any deviation from the model is an anomaly, based on the assumption that malicious behaviours differ from that of typical users. With this technique, it is capable of detecting zero-day attacks and internal malicious activities such as abnormal users. Although difficult for Cyber-Criminals to recognise, it does generate large quantities of false positives as any new activity is considered an intrusion.

Khraisat et al. also explained two means of data inspection from either a host system or from network traffic. The first, Host-based Intrusion Detection System (HIDS) analyses log files, such as OS, firewall or database logs. It can therefore allow the detection of insider attacks with physical access to a machine. However, it is limited to machines upon which it is deployed, meaning a network wide coverage would need HIDS on every device. On the network side, Network-based Intrusion Detection System (NIDS) extracts traffic through packet

capture and is therefore capable of monitoring all devices on a certain part of the network and can also monitor external malicious activities before they spread to another system. Even with its multi-positional deployment possibilities, the inspection capabilities are highly influenced by data bandwidth as not all traffic can be examined as well as possible encryption technologies.

2.1.2.1. Evolutionary Algorithms

The first of the many different computational analyses is the notion of Evolutionary Algorithms. In [10], Ibor et al. presented the effectiveness of this approach in relation to anomaly detection. Evolutionary calculations, also known as Genetic Algorithms, use natural selection to optimise the analysis for a specific task. Created from training data, the overall results show good performance against various intrusions, however, a more efficient heuristic for chromosomal fitness would prove very valuable for detection techniques. In conjunction with Support Vector Machine (SVM), an average detection rate of 99% can be achieved compared to other approaches, even though fully labelled input data is needed for training. It is also possible to evolve statistical rule-sets, evaluating each rule using a fitness function after each one is evolved with statistical continuous-valued input data. This allows the algorithm to ignore labelled elements in packet headers, as well as keeping the rule-sets small and efficient for detecting attacks.

2.1.2.2. Machine Learning

Mentioned previously, various Machine Learning techniques can be used for attack detection. These techniques need to be trained before they are capable of correctly differentiating target data. However, there are different methods for how classification techniques learn, four of which are presented by Ibor et al. in [10]. Once these techniques have been correctly trained, they can be implemented, a few of which are demonstrated by Ahmed et al. in [11].

2.1.2.2.1. Learning Types

The first of the four paradigms presented in [10] is Supervised Learning. Supervised Learning necessitates the availability of pre-labelled training data, thus teaching the algorithm to differentiate between different categories using pattern recognition. This is the most common type of learning for classification purposes, thus multiple different algorithms exist, from SVM to Artificial Neural Networks.

The second is the complete opposite of the previous. Unsupervised Learning uses the same pattern recognition approach as previously, but uses unlabelled training data to build its own view of the overall problem. The data is first filtered to separate normal data before they are clustered in a specific number of groups, ending with a generated model from the resulting data. However, this approach contains a significant drawback, being the high computational requirements necessary for the classification, which is not always feasible dependent on the available hardware.

The third approach is a mix of the previous two. The Semi-Supervised Learning technique uses both labelled and unlabelled training data. Its first model's normal behaviour from a pre-labelled dataset, thus achieving the same view as the Supervised technique. It then uses an iterative process from the unlabelled data to reduce false alarm rate using similarity distances and dispersion rate of the initial result. The resulting probabilistic model produces overall good results with a high detection rate and low false positives.

Finally, we have the Reinforcement Learning type. As its name states, the model is trained through interaction with the surrounding environment. This allows the pattern recognition model to be specific to the platform on which the interactions with the environment have been taken, being rewarded for the best actions taken. It is suitable for solving sequential problems using a Markov decision process model. Using fuzzy Q-learning techniques, the algorithm can self-learn based on past attacks.

2.1.2.2.2. Implementations

Some of the possible algorithms used for attack detection are presented in [10] and [11].

The first is SVM which can be used to detect anomalous events. It derives hyperplanes from training data which maximises the separation margin between opposing classes. Although a Supervised technique, it can be adapted for Unsupervised functionality as well as Semi-Supervised. It can be used to monitor modifications and query's such as query's to Windows registry where deviation from normal registry access is considered anomalous. Using averaging techniques, SVM can ignore noise thus making the decision surface smoother. Since this approach reduces the number of support vectors, there is a reduced runtime.

The second is the notion of Bayesian Network. Like the previous, this approach can be used with either Supervised or Unsupervised Learning. This approach allows the modelling of domains containing uncertainty in an efficient manner in a tree-like representation, meaning each child-node is dependent on the parent. However, the rate of false positives is elevated, due to the inability to process unusual but legitimate behaviour, such as an increase in CPU usage, or the need to aggregate different outputs for normality deduction when using probability analysis. An example of a Bayesian Network is the Naive Bayes Classifier, which uses the Supervised Learning technique.

Another common occurrence is that of Neural. Although they possess high computational requirements, their efficiency at resolving complex problems explain their use in many domains including image processing and cyber security defence systems. They can also be merged with other techniques from Machine Learning to Statistical Analysis. This combination can be used to create a hierarchical IDS using a K-Nearest Neighbour (KNN) classifier. It is also possible to classify network traffic in real time, where different attacks correspond to different sets of artificial neurons which cover various sizes of area on the neuron map.

The last presented algorithm is the Rule-Based approach, which uses Supervised Learning. It learns the "normal" behaviour of a system and categorises any abnormality as a malicious anomaly. It is possible to train a Rule-Based technique using single or multi-label learning algorithms, the latter being correlated with fuzzy clustering. It can therefore perform in-depth protocol analysis as well as deep packet inspection.

2.1.2.3. Statistical Analysis

Attack detection can also be achieved by using various statistical theories to analyse collected data. Ahmed et al. in [11] explain this approach through two examples extracted from scientific literature. The first, chi-square theory is used for anomaly detection by creating a profile containing only normal events, thus any deviation from these events is deemed anomalous and a possible intrusion. The second is a processing unit capable of detecting rare attacks through network traffic analysis. The developed metric searches automatically for identical characteristics of different service requests, attributing each request an anomaly score. These scores are calculated based on the type of request, the length as well as the payload's distribution, raising an alarm once a customised threshold has been met. Many different types of techniques have been created for anomaly detection based on various statistical principals.

2.1.2.3.1. Mixture Model

The first type presented by Ahmed et al. [11] is based on the concept that anomalies lie within large numbers of normal elements. Mixture Models possess elements which fall into two classes: possessing a small probability of λ or with a majority of elements with the probability $1 - \lambda$. An implementation example of this concept is anomaly detection from noisy data where the assumption resides on a set of system calls with a probability of $1 - \lambda$ being legitimate system use whereas intrusions possess a probability of λ .

2.1.2.3.2. Signal Processing Technique

Another type of statistical processing is Signal Processing Technique. An example of this technique is based on the detection of sudden changes where anomalies are described as either corresponding to network failures and performance problems, or encompassing security-related issues such as DoS attacks. Network health functions are generated which raise alarms when anomalies are detected and are given a degree of abnormality normalised between 0 and 1. This technique is, however, a domain which has hardly been explored.

2.1.2.3.3. Principal Component Analysis (PCA)

Principal Component Analysis (PCA) is an easier method for the analysis of high dimensional network traffic datasets, using linear combinations of a number of random variables. It can be characterised as uncorrelated, with high to low sorted variance or with a total variance equal the that of the original data. The benefits of such an approach is that it is free from the assumption of statistical distribution while being able to reduce dimensions of data without the loss of important information. It also possesses a minimal computational complexity which allows it to be used in real-time anomaly detection.

2.1.2.4. Information Theory

Using Information-Theoretic measurements, it is possible to create appropriate anomaly detection models. Presented in [11], these models use five measurements to explain dataset characteristics:

- Entropy: This is the basic concept of Information Theory, which measures the uncertainty of a collection of data items.
- Conditional Entropy: The entropy measurement of the dataset given the entropy of the probability distribution.
- Relative Entropy: The entropy calculation between two probability distributions defined over the same class.
- Relative Conditional Entropy: The measured entropy of the dataset given the entropy between two probability distributions defined over the same class.
- Information Gain: Measurement of the information gain of an attribute or feature in the dataset.

From these measurement techniques, appropriate anomaly detection models can be designed. Using a supervised anomaly detection approach, these measurements are used to validate new models to determine if they are suitable for testing a new dataset. Information-Theoretic measurements have been determined to have increased performance, thus being suitable to create efficient anomaly detection models.

Using correlation analysis, it is possible to create different functionalities. Nonlinear Correlation Coefficient (NCC) similarity measurement is used to detect malicious network behaviours by extracting both linear and non-linear correlative information between network traffic. Where network traffic is concerned, data sets exist which possess non-linear correlations. Another measurement is Multivariate Correlation Analysis (MCA) which accurately characterises network traffic through the extraction of geometric correlations between network traffic features. Used mainly for DoS detection, this approach uses images converted from characterised network traffic instances. This is done through dissimilarity measurements, such as Earth Mover's Distance (EMD) which considers cross-bin marching and also provides an accurate evaluation on the dissimilarity between different distributions.

2.1.2.5. Clustering

Another algorithm used for anomaly detection is the notion of Clustering. Clustering-Based detection uses unsupervised learning technology to differentiate between data points. The three main assumptions of this method are that (i) the clusters are formed using normal data and any new inputs not corresponding with existing clusters are deemed anomalous. However, when a cluster is formed with both normal and anomalous data (ii), the normal data is considered to lie close to the clusters centroid whereas anomalies reside further away, making them detectable using a distance score. Since clusters vary in size (iii), any cluster whose size is smaller than a given threshold are considered anomalous leaving the thicker clusters to be considered as normal. Many different types of clustering techniques are possible, however only two are presented in [11].

2.1.2.5.1. Regular Clustering

The first and most common clustering technique is Regular Clustering. Using various data processing methodologies, the main standing point of this technique is that clusters are generated from rows extracted from the training dataset. A few existing implementations summarised by Ahmed et al. are K-Means clustering

and a distance-based anomaly detection algorithm. All techniques explored possess varying degrees of accuracy (from 57% to 80%) but with a high false positive rate of approximately 22%.

2.1.2.5.2. Co-Clustering

Unlike Regular Clustering, Co-Clustering uses simultaneous processing of both rows and columns of the dataset to generate two sets of clusters. It also allows the definition of clustering criteria as well as optimisation and simultaneous row or column subset retrieval from the data matrix corresponding to specified criteria. Considered a dimensional reduction technique, the simultaneous grouping of rows and columns allow the preservation of information contained in the original data. There is also a significant reduction in computational complexity compared to other algorithms used in various clustering methods. Experimental results demonstrated that this technique is beneficial in the detection of DoS attacks with an overall 95% accuracy when trained with DoS specific data compared to 75% from generic datasets.

2.1.2.6. Detection Technique Use

All CIs make use of a telecommunication network to transmit data between both critical and non-critical components of their system. The necessity of guaranteeing the proper functionality of such network along with an effective security strategy has been noted in [128]. Their approach was composed of an Intrusion Detection System (IDS) built on top of a customizable flow monitor, capable of monitoring network traffic at different levels of granularity and discovering ongoing attempts of compromise. Imitating IDS methodologies but focusing on Critical infrastructure Supervisory Control and Data Acquisition (SCADA) systems, [125] explored in the near past various ML methodologies optimized for the detection of malicious insider actors. Their work took into consideration multiple learning methods which were evaluated with the use of the Remote Technical Unit communications dataset and involved both normal operations and instances of command data injection attack scenarios. The protection of SCADA systems through machine learning algorithms have been also addressed in [134], where a novel One Class SVM (OCSVM) methodology was implemented to separate outliers (attack data) from the majority (normal data). The proposed methodology was superior in both performance and threat-detection terms compared with the rest of rule-based, Artificial Neural Network (ANN), Hidden Markov Model (HMM), and Support Vector Machine (SVM) techniques.

In [129], Behavioural observations and Big Data analysis techniques were utilized to detect anomalies in CI environments, aiming at providing an additional layer of defence against cyber-attacks. The data used for the purposes of their study was based on normal and “infected” nuclear plant simulation scenarios, so that their feature extraction and data classification results be as realistic as possible. The outcomes of their work regarding the detection capabilities of the proposed solution were satisfactory enough, compared with the already traditionally used solutions. Another study, targeted especially towards the identification of cyber-attacks on CIs like a water distribution system, developed a novel algorithm capable of detecting and localizing such attacks [132]. Their proposal took advantage of a deep learning neural network architecture composed of several autoencoders, which was able to successfully identify all attacks -as well as the compromising of data integrity- of the BATtle of the Attack Detection ALgorithms open source dataset [124].

Over the last few years, a couple of promising proactive detection methodologies have been reported in literature, which require less computational power and outperform prior existing solutions. Among them, [131] proposed the combination of Fuzzy hashing algorithms and clustering methodologies for the efficient detection of emerging ransomware threats, while [130][133] described extensively several reasoning approaches, data mining and pattern matching techniques for the detection of abnormal network behaviour with satisfactory results [126][127].

2.1.2.7. Knowledge and Datasets

One important factor, as presented by Ben-Asher et al. in [12] is that attack detection is strongly influenced by the attacker’s profile, but also the profile of the detection agent. All detection techniques are based on the computational analysis of data, due to our inability to process the thousands of lines of log files and look for various anomalies. However, each analysis was defined, programmed and configured by a human, thus making it dependant on that humans’ abilities. A novice hacker will leave a lot more breadcrumbs than an expert when

intruding into an IT system. On the same principal, a novice defender will find it difficult to detect the novice hacker and practically impossible to detect the expert. The expert defender however, will detect the novice attacker with fewer difficulties and can potentially catch the expert. This principal is also relevant concerning the data used to train the different detection techniques.

Datasets are very important as they are used to train these different methods to recognise “normal” traffic, allowing the system to identify any anomalies. It is therefore important that the data contained in these sets be both clean and up-to-date. In [11], Ahmed et al. presented some available datasets as well as various issues. The main problem is that there are very few public datasets available since privacy is an issue due to the packets being untouched. There is also the risk that the dataset be “corrupted” due to unintended and undetected infected traffic on the network. The DARPA/KDD public datasets, considered the benchmark in network analysis, are unfortunately limited due to the presence of artefacts which influence the detection process. They were also generated on an out of date Solaris-based system, thus creating many important differences with modern systems.

A more modern publicly available set called ADFA-LD12 is also presented. It contains modern attack methodologies and was generated using an Ubuntu 11.04 system from 2011. The attacks target web-based tools on a realistic fully patched server forming an acceptable simulation of the real world, making it a possible successor to the DARPA/KDD dataset. The attacks available include password brute-force on an FTP/SSH connection, a Java-based meterpreter with the TikiWiki vulnerability exploit and a C100 web-shell with PHP remote file inclusion vulnerability. Other public data sets exist and are presented more in detail in [11].

2.1.3. Risk Management Methodologies

Attack-Detection is an important part in the realm of Cyber-Security, but it is only part of protecting assets. Risk Management is a notion which can be applied to any domain where danger is possible, such as a construction site where Risk Management deals with things like falling debris or malfunctioning machines causing bodily harm. In the realm of IT, Threat Modelling techniques help Risk Management, allowing Cyber-Security Specialists to better analyse and manage Cyber-Security Risks.

2.1.3.1. Cyber Risk Management

Cyber Risk Management, explained in [13], is the identification, analysis, evaluation and the focus on potential risks which could have a serious impact to cyber technologies. It begins with a Cyber Risk Assessment, presented in [14], which presents an image of potential security threats of the examined system, helping to ensure that the cyber security controls chosen are adapted to the risks faced. Without such an assessment, time, effort and resources would be wasted as defences would be implemented to counter events that could never happen. It also minimises the possibility to underestimate or overlook certain risks which could cause significant damage to target systems. This assessment is a fundamental requirement of best-practice frameworks, standards and laws, such as the European General Data Protection Regulation (GDPR) from 2016, presented in Section 4.1.2.2, and the UK Data Protection Act (DPA) from 2018. This assessment is conducted in three steps. First, information assets which could be affected by attacks, such as hardware, data or intellectual property, are identified followed by the identification of their predatory risks. Secondly, a risk estimation and evaluation are performed, allowing the identification of controls best adapted to treat the identified risks. Finally, continuous monitoring and review of the risk environment is done, allowing the detection of any changes in context and maintaining an overview of the whole Risk Management process.

The management process then prioritises the different risks by likelihood as well as the amount of impact it could have, thus informing the selection and application of various security control measures. The notion of Risk Management is, like Risk Assessment, an essential requirement of security standards, Frameworks as well as laws such as the Network and Information Systems (NIS) Regulations from 2018 but also once again the GDPR. A few examples of standards that mandate the use of Cyber Risk Management include the Centre for Internet Security (CIS) Controls, which are a set of 20 Critical Security Controls (CSC) for Cyber-Defence, the Payment Card Industry (PCI) Data Security Standard (DSS) which protects digital cardholders data where credit card payments are used, and the International Organisation for Standardisation (ISO) / International Electrotechnical Commission (IEC) 27001 standard from 2013, presented in Section 4.1.1.1. This standard

also provides specifications concerning Cyber Risk Assessment in relation to the entire Risk Management process.

Risk Management has been applied to many different scenarios, such as IoT in [15] and CIs in [16]. In [16], Risk Management applied to the protection of infrastructure is divided into three groups: **Structural**, concerning the composition of hardware or Industrial Control Systems (ICS), **Procedural**, encompassing system management and operation, and **Responsive**, covering responses and damage control post-detection. In [17], the relation between Risk Management and insurance policies are presented. Depending on whether Insurance companies can perceive the level of self-protection, is influenced by the legislations in place of the use of consulting firms to audit security efforts, overall changing the way insurance policies are distributed and maintained. A proposition of a supervised learning technique for Financial Risk Management is presented in [18]. Using Big Data Analysis, they are capable of obtaining unusual behavioural patterns from a target system, by supervising images or examining text. Using a Supervised Learning-Based Secure Information Classification (SEB-SIC) model, potential risks to data sharing can be identified through the use of decision trees, due to its wide adaptability in predictions

2.1.3.2. Threat Modelling

Many different modelling techniques exist in scientific literature, allowing the reliable operation of CPS. These models allow a comprehensive overview of potential attack vectors to new or existent systems. In [111], Threat Modelling is presented as the identification of system vulnerabilities and their potential impact of CPS processes. In this paper, a modelling methodology called STRIDE is presented. Created by Microsoft, this approach focuses on the identification of potential threats in each of the different system subcomponents. Considered a lightweight approach when compared to other methodologies such as HAZOP, OCTAVE or PASTA, STRIDE modelling can be performed either per-element, or per-interaction. STRIDE-per-element possesses a higher complexity as well as identification capabilities, however, STRIDE-per-interaction's protection strategies are still deemed sufficient to protect a CPS since system components generally interact in an anomalous way during attacks.

Another approach is that of the “Open Weakness and Vulnerability Modeler (OVVL)”, presented in [112]. Here, Threat Modelling is presented as being a parallel activity to Risk Assessment and is necessary to create a structured representation of the security properties of a CPS. Modelling and analysing the various elements of a system allow the identification of potential vulnerabilities and threats which exist. Once more, STRIDE is presented along with other various modelling tools such as the Microsoft Threat Modelling Tool (TMT) or OWASP Threat Dragon. Offering various degrees of automatic analysis of report generation, both tools are free to use. However, Schaad and Reski [112] note that Threat Dragon is still limited in its features and functionalities. Comparing their OVVL contribution to that of TMT or Threat Dragon, they notice that OVVL functions similar to TMT with slightly better performance.

2.2. Application to Critical Information Infrastructures (CIIs)

With the expansion of technology in regard to inter-connectivity of various devices, the reach of Critical Information Infrastructures (CIIs) has increased. With the rise in the amount of data being exchanged and processed as well as the added free access to wireless communications, the risk of attack has also escalated. To, therefore, ensure the safety of a country as well as its economy and more importantly its people, increased protection measures in Cyber-Security must be taken.

Although many different approaches to anomaly detection exist, not all are applicable to the same scenario. Due to their computational needs, some are more suited for large servers with limitless processing power whereas others can be applied to IoT applications. It is therefore important to review all existing methods for attack detection to be able to prepare CIIs for possible intrusion. Through risk management and incident handling methodologies, CII operators can be trained to recognise threats as well as learn from past events to efficiently protect their own systems through the use of various available security utilities.

The contents of this section provide a global overview of different threats, as well as detection methods. Although nothing specifically oriented towards CIIs has been presented, many of these notions will be expanded upon in future deliverables. The various threats pertaining to CIIs in particular, will be presented along with their threat model in deliverable 3.1: “Taxonomy of threat landscape for CIIs”.

2.3. Requirements for Critical Information Infrastructures (CIIs)

To collect requirements relevant for CII, end-user questionnaires were devised to collect data. Through the analysis of these results and the identification and prioritisation of user requirements.

For identifying requirements for CIIs this project devised end-user questionnaires and sent them out for partners in the industry to provide their feedback. The identification and prioritisation of user requirements was done through the collection and analysis of these results. This work is presented on **D2.3 User and stakeholders’ requirements and reference scenarios**.

3. Background Solutions Relevant to CyberSANE

In this section, we will describe various solutions, systems and tools, which have already been mentioned in the CyberSANE DoW and will be adapted to work with or could be integrated into the CyberSANE solution. The approaches mentioned in the CyberSANE DoW are the following:

- eMAS SOM (Owner: S2) is a toolchain aimed at Security Operations Centre (SOC) operation in order to monitor an infrastructure, covering both IT and Operational Technology (OT) components.
- SiVi Tool (Owner: SID) is a human-interactive visual-based Anomaly Detection System (ADS) that is capable of monitoring and promptly detecting several devastating forms of security attacks, including wormhole attacks, selective forwarding attacks, Sybil attacks, hello flood attacks and jamming attacks.
- The L-ADS (Owner: ATOS) is a real-time network traffic monitoring and anomaly detection with machine-learning capabilities, which can perform deep-packet inspection using its info for correlation of attacks.
- XL-SIEM (Owner: ATOS) is a Security Information and Event Management (SIEM) solution with added high-performance correlation engine to deal with large volumes of security information.
- CARMEN (Owner: S2) is Europe's first solution for detection Advanced Persistent Threats (APTs). The product focuses on anomaly detection in network traffic. Different modules are in charge of detecting indications of lateral movement or data exfiltration.
- OLISTIC Enterprise Risk Management Suite (Owner: UBI)
- MEDUSA Cyber Intelligence Suite (Owner: UBI)
- MITIGATE (Owner: MAG) is a risk assessment system offering services for Supply Chain (SC) cyber assets, propagation and cascading models' generation engine is provided in the system.
- Metadon SIEM (Owner: PDMFC) is a Log Management solution for dealing with large volumes of information, which can be leveraged by a security analyst to perform fast queries, correlations and historical analysis.
- Chimera (Owner: PDMFC) is a Dataflow tool with focus on privacy primitives, that allows for non-structured information to be anonymised by dynamic rules.
- SPA (Owner: PDMFC) is an Identity Lifecycle management tool, which provides the CRUD for managing an access catalogue and the mechanisms for automatic provisioning, which also incorporates a Single Sign-On (SSO) Provider (both SAML and OAuth supported).

3.1. eMAS SOM

S2 Grupo CERT managed security services rely on emas[®] Security Operations Manager (SOM), a comprehensive software suite developed by S2 Grupo, which is structured around a Configuration Management DataBase (CMDB) (ISO 20000 or Information Technology Infrastructure Library (ITIL) compliant) and provides security events monitoring and collection capabilities, along with a flexible orientation towards network surveillance, including IT for computer network and information systems environments, OT for industrial environments (ICS) and also IoT, advanced intelligence using complex event correlation techniques or the analysis of patterns for the identification of anomalies, as well as service processes management (including Incident Handling process, Quality of Service, configuration or knowledge management).

3.1.1. Key Concepts and kinds of threat managed

emas[®] SOM is strongly related with the family of SEM tools. Nevertheless, emas[®] SOM offers capabilities beyond a traditional SIEM, since it has an intelligence layer provided by a complex correlation engine and is oriented to security events and incidents management.

It is ITIL compliant due to the fact that it requires to focus on Service Level Agreements (SLAs).

D2.1 – Cyber Incident Handling Trend Analysis

The general process is related with the event management lifecycle, in order to manage all possible dependencies and transitions of a Security Event Management (SEM) life-cycle, Figure 5.

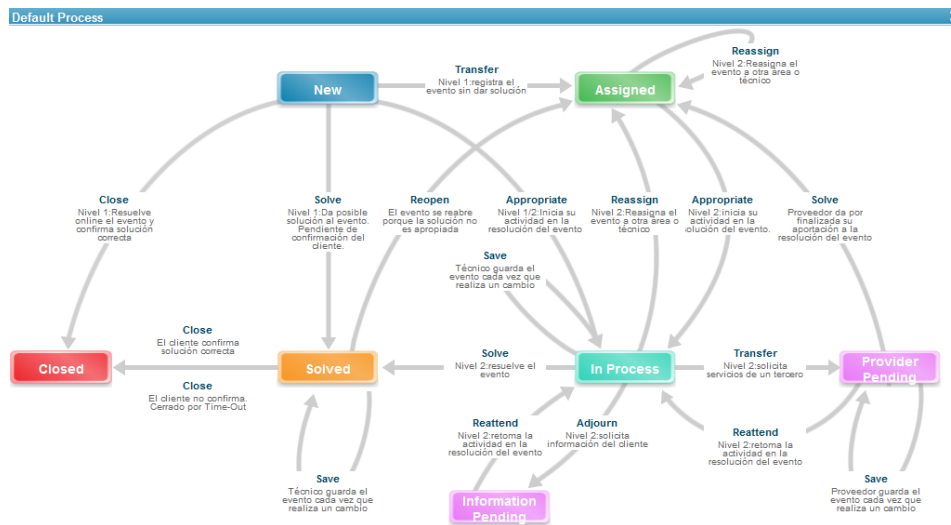


Figure 5: emas® SOM default operational process diagram

As input, it requires logs or relevant data coming from monitored tools or systems (any system or asset that might be target of a security incident). As output, it will report alerts of possible security incidents in real time.

3.1.2. Critics

Strengths	Weaknesses
<ul style="list-style-type: none"> Multi-tenant and multi-tiers Support for hosted deployments Data archiving and back-up Data transformation techniques Customisable dashboards (input logs) Manage host and application logs Network activity monitoring Log search capabilities App store monitoring plugins Scalable log recollection Efficient log indexing Custom rules engine Real-time event correlation Customisable dashboards (incident and alerts) Threshold based alerts OT Intelligence (ICS) Predefined scenarios Incident management lifecycle Asset CMDB Vulnerability Manager integration 	<ul style="list-style-type: none"> Data normalisation techniques Data enrichment Historical correlation Encrypted Network Traffic Analysis Threat intelligence IP reputation feed Fraud detection User and Entity Behaviour Analytics (UEBA) and Profiling Big Data Analytics integration Risk manager integration Incident forensics integration

Strengths	Weaknesses
Full administrative capabilities Manage network and security events Incident Knowledge Base	

Table 1: Strengths and Weaknesses of emas® SOM

emas® SOM is a powerful tool to be oriented as base platform for CIs. This base platform is a good start to build encrypted detection and data normalization on top of it to cover cyber security incidents in real time.

3.1.3. Implications for CyberSANE

emas® SOM (GLORIA) is planned to be used as the base platform of LiveNet, based on the current features and on the development of other features.

3.2. SiVi Tool

SiVi is an innovative visualisation servicer offering an Advanced Programming Interface (API) in order to accept both raw data from sensors and pre-processed data from SIEM software such as the OSSIM AlienVault and present to the end-users an intuitively overview of the network’s status. The API can be modified in order to cooperate and accept data from 3rd party resources. The existing SIEM tools tend to be verbose, carry unnecessary information (noise) and therefore create an environment that does not offer any added value to the security administrator (or SIEM operator).

After the installation of the SiVi tool, the security operator of the system integrates on its daily working routine the visualisation capabilities in order to get a quick overview of the system and if decides that an incoming traffic is a potential threat to the system, she/he can proceed to further actions using the installed SIEM in the system.

The input of the software is the incoming traffic flows and the output are the visualisation graphs. The input is received through the SiVi’s API, which can be modified based on the needs of its client. Figure 6 presents an overview of SiVi Tool’s user interface.

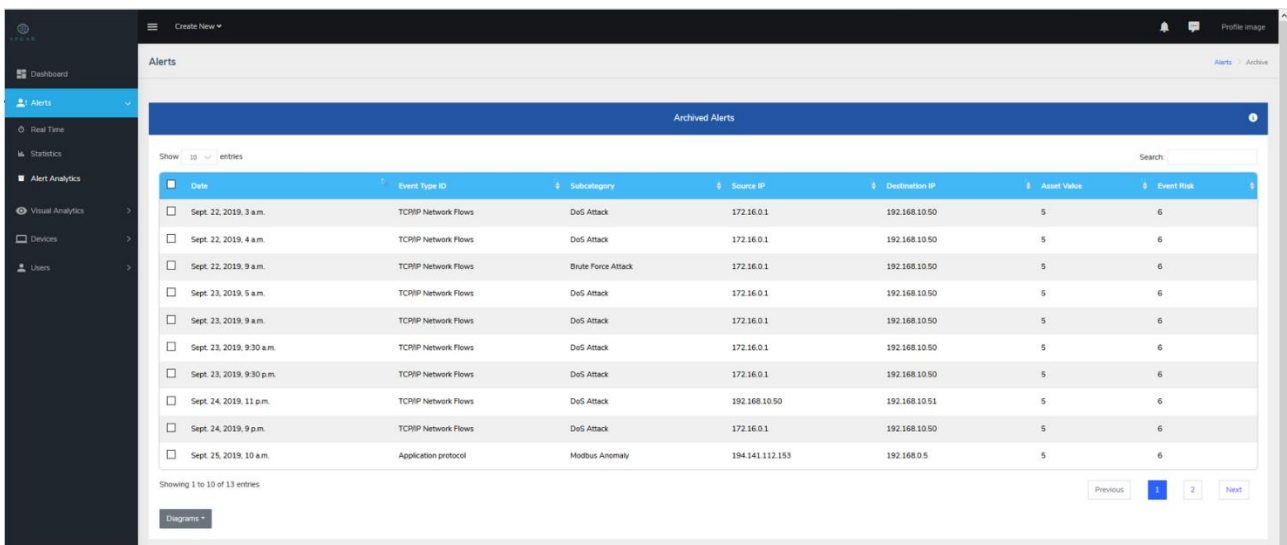


Figure 6: SiVi Tool User Interface

3.2.1. Critics

CyberSANE combines different cybersecurity tools that will form the CyberSANE ecosystem providing extra functionalities to the network administrators to detect and analyse anomalies on time before the occurrence of any devastating situations. The tool integration phase of such a system, as CyberSANE, would be a demanding process since different tools should exchange information and orchestrates to work as a whole. This process might create an overhead on the technical partners, but eventually, CyberSANE users will benefit from the added value coming from the usage of multiple cyber-security tools.

From the User Experience (UX) point of view, the SiVi tool is a lightweight software with a friendly user environment offering easily interpretable graphs without adding any significant overhead to its users.

3.2.2. Implications for CyberSANE

SiVi Tool will be used in CyberSANE to recognise familiar threats as well as identify threats that have not been experienced before (anomaly detection). SiVi Tool does not require vigilant human oversight, while supports the reasoning ability that is crucial for making decisions about anomalous data that may or may not be a threat. Based on a rigorous radial visualisation design, SiVi Tool may expose adversaries conducting one or multiple concurrent attacks against IoT enabled infrastructure.

SID's SiVi Tool will be integrated in the CyberSANE ecosystem via the provided APIs. Since the SiVi Tool does not support SIEM functionalities, in the context of data extraction, a SIEM tool (probably the one supported by ATOS – L-ADS) should be used to feed the SiVi Tool with network data. Regarding the SiVi Tool output, in the unified dashboard that will be created, the SiVi Tool will be provided as an option to the network administrator.

3.3. L-ADS

In a world where data traffic is increasingly encapsulated either through Virtual Private Networks (VPNs) or through TLS/SSL (traffic encryption layer), it is increasingly difficult to monitor these data flows to detect malicious traffic that may exist. In response to this situation, the L-ADS tool aims to provide a solution that can solve these challenges.

The Live Anomaly Detection System (L-ADS) collects traffic with different data flows and uses unsupervised algorithms based on patterns. It can extract all the events that match with some kind of suspicious behaviour. Particularly, L-ADS is based on one class SVM algorithm. This algorithm looks for the hyperplane that has the maximum distance with points that are closest to it. Therefore, SVMs are sometimes known as maximum margin classifiers. In this way, the points of the vector that are labelled with one category will be on one side of the hyperplane and the cases that are in the other category will be on the other side. This analysis is used for identifying malicious behaviour in the system. The tool has also a training component for improving the identification and results of the analysis according to the specific functionality of each system.

3.3.1. Key Concepts and kinds of threat managed

The input data that L-ADS uses is related to the connections and data exchange between systems. It is obtained from the network and uses mainly header data of exchanged packets. This includes, among others:

- Number of incoming/outgoing connections.
- Size of the packets sent/received.
- Duration of the connections established by clients and servers.
- IP addresses and ports, Source/destination
- Information of the protocols or applications to be modelled.

Based on this data the tool is able to generate reliable patterns for training. This is required due to the specific characteristics and behaviour of each system. The training process improves the accuracy of the ADS, reducing false negatives and positives. A high-level presentation of the solution and components is shown in Figure 7. As we can see, the solution provides the following functionalities:

- Unsupervised learning processes used on unlabelled traffic.
- Learn and train decisions based in new detections and processing of events
- Training process is initially performed using legitimate data.
- The evaluation is done using a valid dataset that is generated during the training process.

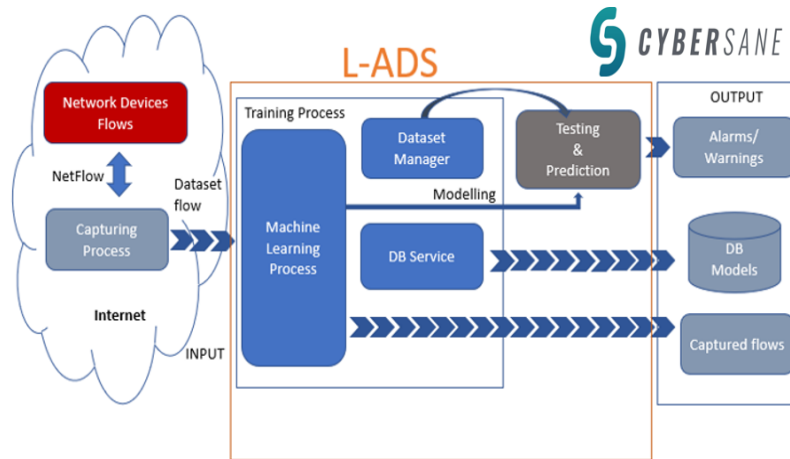


Figure 7: L-ADS concepts chart

The system generates alarms and information about the anomalous data exchanged identified in the system. This data is provided as a structured format and as graphical information. The structured format is used for sharing with other monitoring tools so it can be used for correlation and as input for system risk assessment.

3.3.2. Critics

Strengths	Weaknesses
Anticipate possible risks Improve communication processes in different scenarios Easy to incorporate into architecture Output easily exchanged with other monitoring tools Good functionality	Not all attack vectors covered Cannot analyse encrypted network data Initial training needed for identification

Table 2: Strengths and Weaknesses of L-ADS

3.3.3. Implications for CyberSANE

Due to the importance and risk of CIs we think the tool could be expanded for integrating with other monitoring and detection tools of the project in order to give a better understanding of the situation of the system and recommendations to better secure the system or react to alarms using the correlated data. The tool could provide risk analysis based on learning models that could be complemented using the output of other monitoring and detection tools.

Also, the information provided by the tool is currently provided as direct output and it could be integrated in a common framework together with alarms and events for the user. This could include the possibility for the users to define alarms for the anomalies detected. The information could be shown in a cybersecurity dashboard or sent as alerts to a user.

3.4. XL-SIEM

CyberSANE needs to provide a robust Cyber-Security infrastructure for the HybridNet so the data coming from the live analysis and deep web can be correlated. In this regard, it should be noted that monitoring is a

fundamental pillar to cover on CyberSANE, helping with early Cyber-Threats detection and warnings. The XL-SIEM is a SIEM solution that can integrate different security solutions in a single framework, allowing a clearer vision of the Cyber-Security status of IT/IoT/OT systems. The events used for monitoring can be obtained through either sensors (in the form of agents) that compile system logs from where they are deployed, or as an input of other monitoring tools. This is easily achieved and extended to other solutions by setting up a policy and formatting in the event management engine that allows a good interpretation of the provided data.

XL-SIEM is a software instance capable of processing and analysing information and finally producing a useful output. Sensors can collect information from different methods:

- On the network layer, information about the network activity.
- On the application layer, data in transit of the applications that run on the monitored machine.

Depending on the method used, sensors can obtain a top level of aggregation with a calculated process after that they send their logs to the Cyber Agent. The agent module translates input data coming from the different sources to the format of the event management. The logs received by plugins are processed and only the types of events needed are normalised before being sent to XL-SIEM.

3.4.1. Key Concepts and kinds of threat managed

One positive point of the XL-SIEM is that it can integrate and correlate events coming from different monitoring and detection systems such as IDS, HIDS, antivirus and ADS. As abovementioned for the functionality of the solution, Figure 8 shows a high-level diagram of its inputs, outputs and communications. More in detail, we identify and describe some of its more important components:

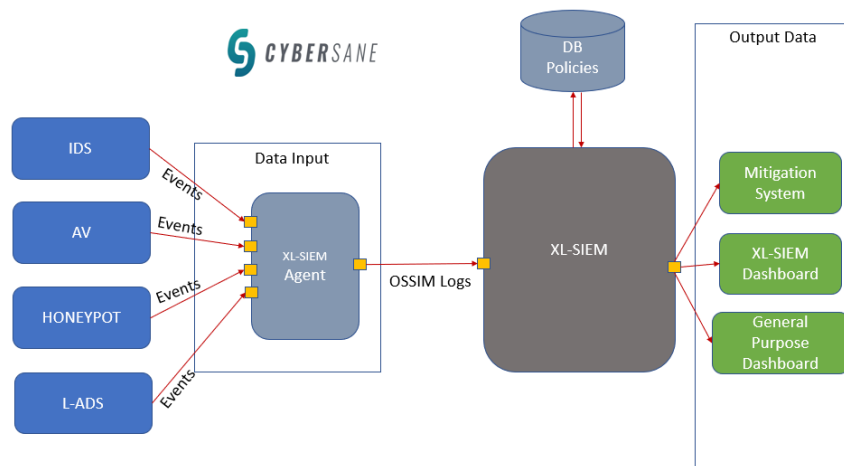


Figure 8: XL-SIEM concept chart

Logs Collection

The XL-SIEM allows the collection of logs from different sources or systems, centralising them for unified correlation and management.

- Logs are standardised for further treatment using regular expression techniques to generate a regular internal log;
- Different logs are grouped by labels according to, among others, the source, type of event, and criticality;
- It allows having a distributed storage, which improves the efficiency and scalability of the system being monitored (e.g. problems of disk space of the system under-surveillance).

Policies Management

The security policy module integrated in the tool can perform different actions associated with events or groups of events.

- Setting rules according to the topology of the type of events;

- Supports predefined rules and customisation of filtering rules;
- Definition of retention policies for obtaining data of a specific event due to a regulatory or compliance policy;
- Policy Filtering.

Security Alerts

The solution can select a wide range of alerts that allows for informing about different types of threats. Among others the more basic threats that can be monitored for alarms are:

- DoS
- Distributed-DoS.
- Port Scanning.
- Brute Force Attack.
- SQL injection.
- Suspicious files.
- USB detection.
- Rootkits.
- Arp attacks.

3.4.2. Critics

Strengths	Weaknesses
Integrate and correlate events coming from different monitoring/detection systems Fast and clear identification of threats Response and mitigation actions Either manual input or correlation of several monitoring tools Reduces amount of exchanged/stored information Generating customised reports efficiently	Needs large amounts of log information Could slow down internal processes Could impact LiveNet and HybridNet infrastructures

Table 3: Strengths and Weaknesses of XL-SIEM

3.4.3. Implications for CyberSANE

Due to the needs of CyberSANE some initial ways for integrating the tool in the general framework could be for managing the event monitoring that is provided by other Cyber-Security tools or platforms in the scope of the project such as SiVi, L-ADS, etc. Therefore, the applicability of this tool would allow to have more understanding and information of the systems Cyber-Security status and what is happening in the network infrastructure. Also, we could improve the alarm system for providing better recommendations and, if possible, reaction capabilities to critical attacks that require a more direct solution. Another innovation for the deployment could be to identify normal behaviour patterns, using machine learning techniques to be mapped with suspicious patterns, avoiding false positive during monitoring.

3.5. CARMEN

CARMEN, Centre of Log Analysis and Mining of Events, is a tool developed by the National Cryptologic Centre and the company S2 Grupo to identify compromises by Advanced Persistent Threats (APTs), and is the first tool based on Spanish technology and know-how.

3.5.1. Key Concepts and kinds of threat managed

CARMEN is a tool that collects, processes and analyses information to generate intelligence mainly from the network traffic. It is made up of agents that compile traffic flows (collection elements), a database engine where information is inserted and a web application that allows representing and checking the collected information so that analysts can work on it and make decisions based on the results provided by the tool.

The data sources which CARMEN is able to work with are listed below:

- Proxy logs
- Passive HTTP
- Passive DNS
- Passive SMTP
- Monitoring and storage of Inter-Process Communication (IPC) data

CARMEN allows applying predefined rules to every data source to detect undue use and, particularly, to detect significant anomalies (statistics, text chains, temporary series and based on knowledge) that may indicate that the organisation has been compromised, and to define and integrate know-how in the tool, ranging from Indicator of Compromise (IOC) to conditions of the anomaly.

As input, it requires logs or relevant data coming from monitored tools or systems (any system or asset that might be target of a security incident). As output, it will report alerts of possible security incidents.

3.5.2. Critics

Strengths	Weaknesses
Misuse detection Behaviour analysis Statistical anomaly detection Time series anomaly detection Anomaly detection Improper use at the endpoint Lateral movement detection Knowledge based anomaly detection URL anomaly detection Alerts triggered by rule-set Intrusion detection through sandboxing and static analysis Integration with honeypots.	Requires full security skills and expertise to be used.

Table 4: Strengths and Weaknesses of CARMEN

3.5.3. Implications for CyberSANE

This tool can be applied in CyberSANE to cover anomaly detection features as part of the HybridNet.

3.6. OLISTIC Enterprise Risk Management Suite

OLISTIC Enterprise Risk Management Suite features innovative smart automations that simplify time consuming tasks and allow to focus on the risk management aspects, where expert thinking is required. OLISTIC upon initialisation, it scans devices connected to the network of a CI in order to produce meaningful risk assessments and alternative risk mitigation strategies. OLISTIC collects and continuously updates a state-

of-the-art built-in knowledge base of threats, vulnerabilities, controls, risk scenarios, propagation rules, risk assessment methodologies, reports and dashboards according to international standards, databases, best practices and worldwide experience.

One of the innovative aspects of OLISTIC is its ability to perform risk calculations based on the relationship of the CI assets. In CyberSANE there will be three types of risks which will be calculated. These risks are the Individual Risk Level (IRL), the Cumulative Risk Level (CRL) and the Propagated Risk Level (PRL).

- The IRL quantifies the risk of an asset taking under consideration all the associated vulnerabilities (disclosed or zero day) and all the enforced controls ignoring the asset's dependencies and relationships.
- The CRL quantifies the risk that is caused on a single asset using the vulnerability profiles of the adjacent assets. This approach takes under consideration all the possible attack paths that are generated towards this specific asset from neighbouring assets.
- The PRL quantifies the maximum pivoting depth that can be occurred by one exploited asset taking under consideration the vulnerability profiles of the adjacent assets along with all the possible attack paths that are generated from this specific asset.

The OLISTIC Suite facilitates risk assessment at the operational level by identifying assets within an organisation which are outdated or about to be exposed to threats in line with the business guiding principles in order to ensure that software, hardware and equipment are functioning appropriately.

Also, it facilitates risk assessment at tactical level in line with the project management processes for key approved actions. Tactical risk analysis requires that the organisation has the means, the people and plans that provide the competence and the guidelines to identify, quantify, qualify and control potential risks.

Finally, it provides insights to assist decision making at strategic level. These insights can facilitate strategic planning elements, cultural risk attitude, governance, measured approaches for risk identification, response and control. On a regular basis, OLISITC assists to set up an enterprise risk environmental scan to ensure that the business and services are operating as intended.

3.6.1. Key Concepts and kinds of threat managed

Risk is a factor in every business that requires high consideration. It entails the understanding, analysing, and minimising the threats that have the potential to severely impact a business. By identifying, quantifying and qualifying through the OLISTIC the cyber risks, it enables to assess the likelihood of their occurrence and take targeted actions to address them. OLISTIC enables risk assessment under standard methodologies which in turn permits to obtain a holistic view across all entities and operational units of an organisation. As a result, without this unified, objective and measurable input, management cannot understand the total risk exposure and proceed with focused actions.

The processes supported by OLISTIC include the population of an organisation's assets inventory, the classification of assets to groups of software, hardware and networking components, the creation of hierarchies to facilitate group actions and filter risks, the correlation of assets within organisational units, to enable propagated risk assessment and management. As far as the vulnerabilities addressed are concerned, OLISTIC features an intelligent engine which enables the automated assignment of threats and vulnerabilities to assets based on their type. It is constantly updated via the US National Vulnerability Database with the latest Common Vulnerabilities and Exposures (CVE) and the scheme for IT systems, software and packages (Common Platform Enumeration (CPE) Dictionary). It also features a subscription-based risk feed, which is regularly updated according to risks events, new regulatory and legislative requirements and other reference sources for each risk management domain. OLISTIC has a rich library of risk scenarios, tailored to each asset type, which enables the fast and efficient population of the risk assessment. It finally suggests controls which may already be in place in order to mitigate each risk based on international best practices. The output of OLISTIC is visualised through graph analysis which demonstrates the Personally Identifiable Information (PII) processing, IT systems, organisational units, processing operations, data owners and data processors enabling to predict how a proposed change in data governance may influence compliance.

3.6.2. Critics

OLISTIC is delivered through a web-based software solution designed to enable organisations to easily and effectively implement an enterprise risk management process. It has a friendly and intuitive user interface which supports multiple risk management processes and enables the participation of different user groups.

Its rich risk scenario library, is available out of the box for each risk domain, and it enables to be easily configured by business process owners. This offers significant time to value and reduced total cost of ownership over bespoke and toolkit-based solutions. It is available as both an in-house deployable solution where data control, security and integration are important, or as a hosted Software as a Service (SaaS) based solution.

OLISTIC proves the value of risk management allowing an organisation to track the health of its risk management process through intuitive dashboards, in different areas and over time on organisation-wide objectives and Key Risk Indicators. It delivers an evidence-based risk management process, producing a full audit trail of system activity and stores all the evidence required so that someone can produce on-demand the risks, controls, treatment actions and incidents in a top-down, bottom-up and cross organisational manner. It lets record, score, assess and mitigate risks at all levels in a business via a single, secure and auditable system.

OLISTIC reduces the workload and potential errors that are inherent when using spreadsheets to manage risk, by allowing users from different locations, departments, sites or even companies to enter data into the same software solution. It also increases transparency of critical future business performance information and provides a single source of truth for risk by the central storage of information in organised structures that are configured according to the business objectives. Finally, OLISTIC gets user adoption quickly because it offers a full system out of the box, is quick to install and configure and can be rolled out getting users managing their risks within days - an unbeatable “time to value” and reduced total cost of ownership versus other software systems.

3.6.3. Implications for CyberSANE

OLISTIC can be applied as a means to assess the risk in the different CIs of the CyberSANE project. It covers computer security, information security (compliance with ISO 27001, 27002 and 27005), PII, business continuity (compliance with ISO 22301), environmental management (compliance with ISO 14001), occupational health and safety (compliance with OHSAS 1800).

3.7. MEDUSA Cyber Intelligence Suite

MEDUSA Cyber Intelligence Suite constitutes a sophisticated, modular, highly-configurable and scalable web mining and cyber intelligence platform that benefits from Artificial Intelligence (AI) and Big Data technologies so as to provide intelligence and real-time insights to non-IT domain experts, satisfying the multi-disciplinary needs of end-user organisations that require advanced web crawling, processing and analytics services. The software can be exploited at operational, tactical and strategic level and covers features which are related with scalable web crawling functionalities, multi-level processing pipelines, evidence collection, intuitive analytics, built-in AI support and trained models for image processing and objects detection, Natural Language Processing (NLP), Named Entity Recognition (NER) and graph mining, integrated network tools, multi-modal alerting and reporting capabilities and interoperability with 3rd party tools.

At operational level, the identified incidents are related to events and activities and provide insights that can guide and support response operations. At tactical level, the events and evidences collected in real-time provide day-to-day operational support. Finally, at strategic level similarities, differences and correlations enable to assess disparate bits of information to form integrated views through graph analysis. Notifications can be provided through alerts or email in order to inform decision and policy makers on broad or long-term issues.

3.7.1. Key Concepts and kinds of threat managed

MEDUSA Cyber Intelligence Suite acts as a web cyber intelligence platform, with abilities to crawl web sites and dark web, collect important information and evidences, index and correlate findings related with text, images and social media posts by identifying and performing a set of intuitive analytics over the collected data sets. The analytics supported concern web search based on free text, with results categorised by a specific entity, with results correlated or not with a specific entity and with complex search expressions along with the combination of all the aforementioned search types. An unsupervised neural network model is used for encoding individual words into a common vector space through Word2Vec model to produce word embeddings. The latter enables to identify words that occur in similar contexts, which are also similar in meaning, enabling to naturally represent analogies with "human-like" semantic awareness. The processes of MEDUSA enable companies have an in-depth discovery and understanding of cyber threats (i.e. illegal activities, leaked data, brand abuse, trafficking in goods and services, etc..) coming from the dark web, social platforms, forums and devise a plan to protect their business. The results of the web crawling and social mining are further analysed and can be demonstrated highlighted, with differential capabilities (i.e. previous vs. current web content), or aligned over a semantic graph and can be exported in multiple formats (i.e. XML, JSON, CSV, binary).

MEDUSA relates to familiar tools in the frame of a collection of common processes including data collection, evaluation and analysis through rigorous and structured techniques. However, its built-in AI capabilities enable to extract knowledge and correlations in an automatic way after having performed a structured initialisation with respect to the examined web content, its links to other sites and classification of the information according to semantic interpretation and understanding. Its architecture is highly modular, scalable asynchronous and is based on microservices.

3.7.2. Critics

MEDUSA has been developed as a modular collection of processes which are asynchronous where evidences are made available upon the first sufficient iteration of the cyber intelligence cycle. This cycle includes the data collection from the web and dark web through web crawling, data alignment, indexing and semantic annotation and results analysis through intuitive analytics to produce intelligence. The results can be enriched in the context of new information and end-user feedback. The analysis is based on sophisticated algorithms in the support of text mining, objects detection over images and graph analysis and relies on a rigorous way of associating information, finding correlations, identifying similarities and differences and detecting abnormal activities in an accurate, timely and relevant manner. Some advantages include its architectural approach which is based on asynchronous microservices enabling for making available the produced evidences upon a sufficient collection, extraction and analysis of occurrences coming from the web and dark web. In the context of CyberSANE, specific scenarios should be defined in order to focus on CIs.

3.7.3. Implications for CyberSANE

In the context of the CyberSANE project, MEDUSA may act as a component which is able to provide context and relevance to a large amount of data collected over the web, to empower the stakeholders develop a proactive cybersecurity posture and to bolster overall risk management policies and to drive improved detection of advanced threats and illegal activities/occurrences.

3.8. Evidence-driven Maritime Supply Chain Risk Assessment (MITIGATE) System

MITIGATE [19], [20], [21], [59] targets to contribute to the effective protection of the Information Communication Technologies (ICT)-based ports SCs that arise from the ICT interconnections and interdependencies of a set of maritime entities (e.g. port authorities, ministries, maritime companies, ship industry, customs agencies, maritime insurance companies other transport CIIs (e.g. airports) and other CIIs (e.g. transport networks, energy networks, telco networks)). This is achieved by treating the resolution of the

ICT maritime SC risks as a dynamic experimental environment that can be optimised involving all relevant maritime actors. MITIGATE approach based on simulations facilitates the identification, analysis, assessment and mitigation of the organisation-wise and interdependent cyber threats, vulnerabilities and risks.

In the literature, the analysis and evaluation of the cyber risks are based on a straightforward approach that combines a set of parameters and features such as the likelihood of a security event and the consequences of the event itself, the exploitation level of a vulnerability etc. MITIGATE aims to support this approach with rational decision making. The pursuit of MITIGATE is to support risk analysis with security-related information obtained from online repositories strengthening the rational analysis. MITIGATE's objective is to promote a more rigorous, rational approach that gathers, critically appraises and uses high quality research information either produced by well-defined simulation experiments or are available online to enhance the risk assessment process.

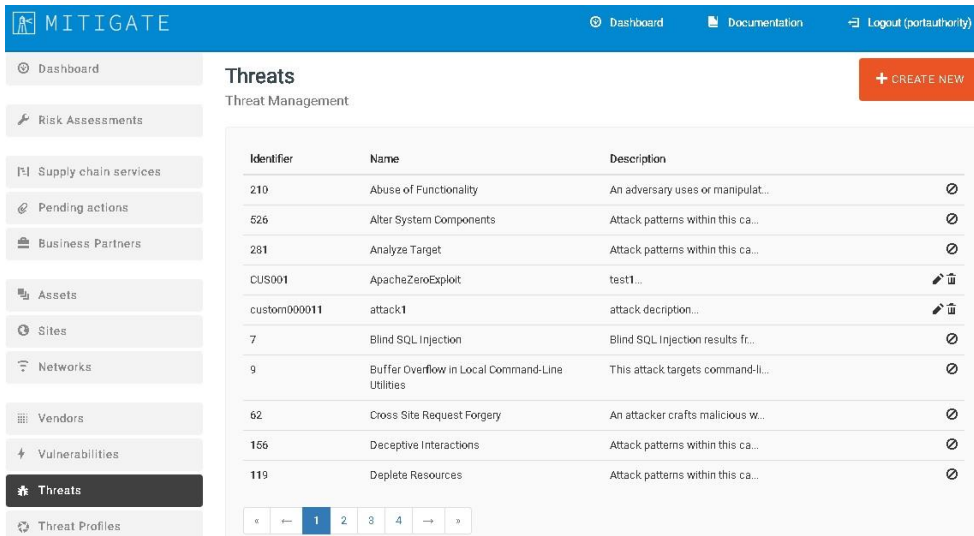
In particular, MITIGATE shares the view that process of evaluation and mitigation of the cyber issues is neither objective nor neutral; it should be an inherently rational process that relies on well-defined and widely acceptable security-related data and not only upon highly personalised experience, expertise and judgment of individuals.

3.8.1. MITIGATE System

MITIGATE (Figure 9) aims at realising a radical shift in risk management for the maritime sector towards a collaborative evidence-driven Maritime Supply Chain Risk Assessment approach. To this end, MITIGATE has integrated an effective, collaborative, standards-based risk management system for port's CIIs, which shall consider all threats arising from the SC, including threats associated with port-CIIs interdependencies and associated cascading effects. The proposed system enables port operators to manage their security in a holistic, integrated and cost-effective manner, while at the same time producing and sharing knowledge associated with the identification, assessment and quantification of cascading effects from the ports' SC. In this way, port operators are able to predict potential security risks, but also to mitigate and minimise the consequences of divergent security threats and their cascading effects in the most cost-effective way i.e. based on information associated with simulation scenarios and data acquired from online sources and repositories (e.g. National Institute of Standards and Technology (NIST) Repositories).

In order for the system to meet its objectives has been empowered by: (i) a range of reasoning, data mining, crowd-sourcing and Big Data analytics techniques that incorporate and leverage a variety of data sources and data types, enabling efficient handling of data that are incomplete, uncertain, and probabilistic; (ii) pioneering mathematical techniques for predicting and analysing threats patterns; and innovative visualisation and simulation techniques, which optimise the automatic analysis of diverse data. These ICT solutions/technologies and mathematical instruments provide a basis for implementing a variety of mechanisms and processes that facilitates collaboration between the various maritime agents enabling them to:

- Identify and model assets, processes, risks, stakeholders' relationships/interactions and dependencies.
- Analyse threats, vulnerabilities and countermeasures accumulated in various online sources and repositories.
- Identify, evaluate and classify various ICT-based risks, while at the same time facilitating the risk resolution.
- Design, execute and analyse risks and threat simulation experiments in order to discover viable attack paths in the SCs. These attack paths consist of vulnerability chains that can be exploited by attackers in order to accomplish their malicious goals.
- Exploit the simulation results towards formulating effective evidence-based mitigation plans.
- Support continual Webs' vast reserve of open, distributed data uptake, integration, state assessment, decision analysis, and action assignment based on large-scale high- performance open computing infrastructures so that all agents may access and analyse a plethora of collected data and information.



Identifier	Name	Description
210	Abuse of Functionality	An adversary uses or manipulat...
526	Alter System Components	Attack patterns within this ca...
281	Analyze Target	Attack patterns within this ca...
CUS001	ApacheZeroExploit	test1...
custom000011	attack1	attack description...
7	Blind SQL Injection	Blind SQL Injection results fr...
9	Buffer Overflow in Local Command-Line Utilities	This attack targets command-li...
62	Cross Site Request Forgery	An attacker crafts malicious w...
156	Deceptive Interactions	Attack patterns within this ca...
119	Deplete Resources	Attack patterns within this ca...

Figure 9: Evidence-driven Maritime Supply Chain Risk Assessment (MITIGATE) System

3.8.2. MITIGATE Overall Architecture

As already mentioned, MITIGATE system aims to provide a holistic solution regarding risk management in the frame of port Supply Chain Services (SCS). To this end, specific set of services need to be developed and integrated in a seamless manner. Such services include assessment of risk in a collaborative manner among business partners, advanced simulation and visualisation of potential attacks and advanced reports from open intelligence analysis services. In order to achieve the goal of developing a unified system, a high-level architecture has been defined and presented in Figure 10.

As it is depicted, there are the following eight components that comprise the MITIGATE system:

- The **Asset Modelling & Visualisation** component allows business partners to declare their assets along with the cyber relationships. The creation of a valid asset cartography within the frame of an organisation is the first step towards the realisation of a collaborative risk assessment. Each organisation that participates in a SCS will use this component in order to create its own cartography. The cartography will be automatically linked to available vulnerabilities and attack-types that are relevant to the individual assets that are declared. The cartography along with the linked information will be intuitively visualised by a graph rendering subcomponent of this component.
- The **Supply Chain Service (SCS) Modelling** component allows the modelling of the examined SCSs. More specifically, these SCSs consist of various business processes that are performed in a synergetic way among different business partners. Each business partner has a predefined role in the SCS which requires the ‘participation’ of specific cyber assets. Towards these lines, this component relies on the output of the Asset Modelling component since it allows mapping assets that are already defined in the asset cartography of each organisation with the processes that these assets are involved. This ‘mapping’ plays a significant role during the calculation of risks.
- The **Simulation & Game Theory** component has a twofold goal. On the one hand it is responsible for the discovery of attack paths given a specific asset cartography and a specific SCS and on the other hand it is responsible to propose the best defensive strategy regarding the protection of a specific asset based on game theoretical principles. Both of these features provide significant added value to the final solution.
- The **Collaborative Risk Assessment** component is responsible to provide guidance for the conduction of a risk assessment for a specific SCS. More specifically, MITIGATE introduced a detailed multi-step process [60], in order to calculate the SCS-related risks. This component offers all supportive features and mechanisms that are required for an error-free execution of the proposed risk assessment methodology.
- The **Open Intelligence and Big-Data Analytics** component is responsible to provide near real-time notifications regarding potential vulnerabilities that are related to the assets that exist in the asset cartography of one organisation. These notifications will be generated based on the text-processing of open

sources. However, such mining techniques are extremely computationally intensive; thus, the component will rely on a big-data framework (SPARK) in order to achieve linear scalability.

- The **Notification and Reporting** component is responsible to provide push notifications to the business partners regarding any type of messages that are published in the pub/sub queue. Since MITIGATE involves many time-consuming operations (e.g. the conduction of a vulnerability assessment, the calculation of risks, the processing of open information sources) every time that such an operation is completed a specific message is placed in a predefined topic of the pub/sub queue. The specific component consumes all messages that relate to notification topics and presents them in a structured way to the user.
- The **Administration** component is responsible for the management and the consistency of the various ‘enumerations’ that are required by all the other components. Such enumerations include mainly vulnerabilities, attack-types and business partners. This component also implements the semi-automated update of these enumerations from open sources.
- The **Access Control and Privacy** component provides security guarantees in a horizontal manner to all the other components. More specifically, since the information that is provided and processed (e.g., asset cartography, attack paths, risk calculations etc..) is extremely sensitive, the specific component undertakes the responsibility of implementing the appropriate authentication, authorisation and encryption schemes that are required in order to protect MITIGATE services and data end-to-end.

Finally, it should be noted that the architecture is complemented by a persistency layer and a pub/sub system which are totally supportive. In particular, it should be noted that the persistency layer consists of two types of databases; one relational (MySQL) and one NoSQL (MongoDB). The relational database is used in order to store fully structured data that change rarely (e.g. credentials, business partners) while the NoSQL is used in order to store semi-structured data that change frequently (e.g. Vulnerability reports). The pub/sub system (ActiveMQ) is used in order to decouple the communication of the components and more specifically to eliminate any blocking communication that may be required. Elimination of blocking communication is a prerequisite for the creation of scalable system.

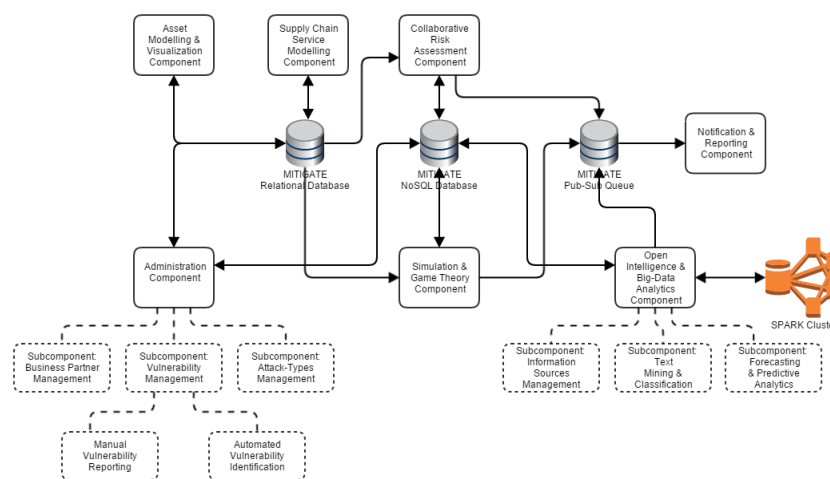


Figure 10: MITIGATE High Level Architecture

3.8.2.1. MITIGATE Security Assessment Services

This Section provides details regarding the main services that have been integrated in the MITIGATE system. These services include:

- The Risk Assessment and the Visualisation functionalities aim to quantify the risks that derive from the various vulnerabilities associated to specific assets that participate in a Supply Chain Service (SCS). According to the proposed approach, three different qualitative risk levels are evaluated and derived. The individual risk refers to the impact of potential exploitation of several vulnerabilities at the asset-individual

level. On the other hand, the cumulative and the propagated risks quantify the effect of an exploitation at a vulnerability chain level, taking under consideration that the assets which participate in a risk assessment are interconnected to each other. Cumulative risk quantifies the effect of incoming attacks to a specific asset while propagated risk quantifies the effect of an exploitation towards the adjacent network. The two latter types of functionalities raise some visualisation requirements that have to be tackled.

- The Risk Management functionalities aim the generation of an optimal mitigation strategy given a specific SCS. The generation of the optimal strategy is performed using a game-theoretic approach that takes into consideration several offensive and defensive strategies that an attacker/defender can perform on a given set of assets within an SCS.
- The Simulation functionalities facilitate the design, execution and analysis of risk and threats simulation experiments that rely on a rule-based reasoning approach in order to generate the chain of sequential vulnerabilities on different assets that arise from consequential multi-steps attacks.
- The open intelligence functionalities relate to the dynamic aggregation and indexing of content that relates to cyber-security. This aggregation is achieved using crawling techniques in order to extract information from various web sources and social media regarding cyber-security aspects. The extraction and the indexing employ big-data techniques in multiple stages since the involved processes are both computationally and storage intensive.
- The prediction and forecasting functionalities provide automated identification of potential vulnerabilities and attacks in the maritime supply chain. More specifically, the indexed dataset that is crawled by the open intelligence functionalities is automatically queried based on specific keywords that are automatically extracted by the profile of assets that are registered by security officers. The automatic correlation of news with the existing assets will provide the risk assessor the possibility to register zero-day exploits and re-run the risk assessments that have been already prepared.

3.8.3. Critics

MITIGATE, funded under the Horizon 2020 Programme of the European Union for Risk Assessment and Assurance models, has introduced an integrated framework for identifying, classifying, assessing, simulating and mitigating risks associated with port CIIs and cybersecurity incidents.

In particular, the MITIGATE system enables the involvement and participation of all stakeholders (e.g., port security operators, port facility operators, and SC participants) in the Cyber-Security management. In order to meet its objective, this system has been empowered by a range of: (i) reasoning, data mining, crowd-sourcing and Big Data analytics techniques that incorporate and leverage a variety of data sources and data types (e.g. vulnerabilities) retrieved from online repositories; (ii) pioneering mathematical techniques for predicting and analysing threats patterns; (iii) innovative visualisation and simulation techniques, which will optimise the automatic analysis of diverse data; and (iv) innovative game theory techniques in order to link optimisation and simulation. All these technologies and techniques have been combined for implementing a variety of services (Collaborative Risk Assessment and Mitigation Services, Open Simulation Environment (ORASE) and Simulation Services, Risk and Vulnerability Visualisation Services and Prediction, Forecasting, Social Engineering and Open Intelligence Services) as part of the project's risk assessment system that enable maritime agents to:

- Design, execute, analyse and optimise risks and threat simulation experiments that will produce the appropriate evidence, information, indicators, factors and parameters.
- Exploit the simulation results towards formulate of effective evidence-based mitigation plans.

However, it should be noted that the complicated nature of the ports' SCs' environment raises a set of additional issues concerning the effective and efficient handling of their security issues. In this context, taking into account the MITIGATE experience, there is a set of research challenges and issues (e.g. usage of machine learning methods such as Naïve Bayes, Random Forests or Neural Networks for the classification of the predicted attack paths, usage of use of distributed computation methods, such as multi-agent systems for more effective cyber-attack path discovery), regarding the distributed and interconnected nature of complex, interrelated SCs' physical and cyber components, network and operating environments, that need to be covered.

3.8.4. Implications for CyberSANE

In CyberSANE, MITIGATE may be used as an analysis tool to completely assess the assets, threats and vulnerabilities associated with the CIIs.

The MITIGATE system incorporates a bundle of automated processes and routines and integrates a wide range of ICT tools which enable port operators in structuring, organising and managing assets and threats, as well as in executing simulation scenarios and deriving evidence based knowledge that will be used for the identification, classification, assessment, simulation and mitigation of risks associated with port CIIs. Hence, these concepts can also be used for CyberSANE to facilitate the analysis and propagation of a threat, risk or incident from in a structured and well-defined way.

MITIGATE is a good candidate tool to be used in Task 5.6 (Data Fusion, Risk Evaluation and Event Management (HybridNet) Component Integration) under WP 5 (Data Fusion, Risk Evaluation and Event Management (HybridNet)) to design and develop the Data Fusion, Risk Evaluation and Event Management (HybridNet) Component.

3.9. Metadon SIEM

Metadon is a SIEM component and provides the following features:

- Security Information Management (SIM);
- SEM;
- A common taxonomy for security events and incidents;
- A common information model leveraged on the industry and government published standards.

It provides connectors for multiple forms of ingesting data, might they be syslog, TCP, HTTP or file based. The input formats can be transformed by a domain specific language and normalised into a common event and field taxonomy.

Currently leverages Elastic Search as a back-end for data storage and provides a web interface where the security analytics can query the data in a high level google like language.

Metadon implements a query interface where other components or users are able to distinguish between normal and abnormal operations. To complement the data search, visual analytics methods are made available to visually depict characteristics that assist the human operator in discovering attacks and their causes.

Using the query language 20 correlation use cases are provided by default. These use cases assume a set of common logs ingested into Metadon.

3.9.1. Key Concepts and kinds of threat managed

The tool is composed by the following major concepts:

Log Collection

- Ingestion, Parsing, Labelling, Field Extraction and Normalization
- A few hundred standard formats are supported natively, others can be added through customisation

Log storage

- Distributed Storage
- Retention Policies

Query Language

- Metadon Query Language (MQL) allows users to query data in a high-level language, inspired in the stream processing tech.

Log Correlation and Enrichment

- Has the ability to correlate multiple sources of data on a common field. Resulting data can be enriched multiple times. For instance, it can do GeoIP location for a given field, or malware domain lookup for another.

Standard security use cases and Alerts

Out of the box, Metadon comes with the following use cases:

- Brute force attempt
- Multiple failed sign-ins to different accounts by same IP
- Accesses to the same account from different IPs
- Password change after new IP access
- Access from/to blacklisted IP
- Possible MitM
- Too many errors 404, 403, 500, 501
- Exposed endpoints used from public IP
- Detection of accesses to sensitive protocols
- Anomalous traffic detection
- Commonly abused URLs
- Distributed brute force attempt
- Attempt of log tampering
- Sensitive file permissions change
- Sensitive group change
- Suspicious user elevation
- Suspicious number of VM/docker activity
- High NXDomain count
- High reverse DNS count
- Failed access to host but successful access to system
- Multiple users email forwarding to same destination
- Anomalous sensitive service execution
- User created and deleted within 10m
- Process executed from binary hidden in Base64 encoded file

Metadon currently leverages ElasticSearch [22] (Open Source version) for log storage, but for the other components uses tools developed by PDMFC. It's more lightweight on the collection front, the log collection agents are written in a language that compiles to binary with performance approaching what you would get from C/C++ code. The frontend aims to be as user friendly as possible and privileges use of access for existing functionalities (search, filtering, aggregation, reporting, correlation) over features.

Metadon is similar in concept to Splunk, presented in 3.12.3.1, using ElasticSearch as a storage engine, but with MQL which is closer to Splunk Query Language and Microsoft KQL.

The tool follows a distributed approach, where the solution is the composition of multiple smaller tools, and not a monolith. Can be deployed in cluster mode and scale horizontally.

A normal use case would be, having a security appliance like a firewall generating logs, a collector retrieving those logs, parsing them into a common schema and then shipping them to a storage engine (ElasticSearch). Afterwards a user can through a domain specific language query those logs and perform correlations with external or internal data. Alerts can be setup to notify users by email, web-service or shell script when a condition is met.

Any log source can be used as input, audit logs, firewall logs, router logs, DNS traffic, traffic flow. For correlation CSV files can be dynamically loaded and used for data enrichment, or web-services that can be parsed with json_path.

As outputs multiple formats are supported, the most relevant should be CSV, JSON and RAW.

Summing up, the tools receives text and outputs text.

3.9.2. Critics

Strengths	Weaknesses
Easily customised Very flexible design Easy deployment without single points of failure; Immediate value Dynamic data correlation and has real-time data streaming capabilities	Dependency on ElasticSearch which requires a significant amount of resources for good performance some important features from their payed tier are not available, like LDAP authentication Requires someone from PDMFC to setup and configure Non existing documentation

Table 5: Strengths and Weaknesses of Metadon

3.9.3. Implications for CyberSANE

The software can be used as log storage for CyberSANE and as a SIEM. It can be used by third parties' components through web-service APIs to consume the stored information, or through an analyst to analyse historical and / or forensic data.

3.10. Chimera

Chimera is a dataflow tool that has high throughput for processing large text datasets in unstructured formats and perform user-defined transformations to clean, bake, structure, anonymise and or encrypt. Since formats change greatly and often, the tool needs to be customisable and support a dynamic language to define which fields should be transformed.

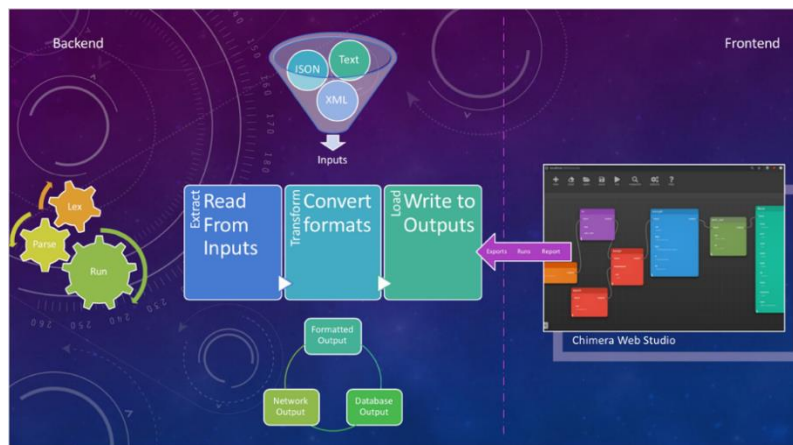


Figure 11: Chimera Diagram

Chimera provides a backend written in a language that compiles to binary format (elf / exe) for performance reasons. This backend has a hand-written parser and lexer that creates an Abstract Syntax Tree (AST) for the CAL language. Further, a tree walker interpreter provides the runtime for CAL. Message passing between AST nodes is performed through shared memory and all nodes follow the same specifications for accessing data and creating new data.

To ease the usage of the domain specific language, a web frontend with a single page application is available to help operators design workflows visually. Workflows can then be exported, including the respective rules in CAL.

Exported workflows follow a standard format that can be processed by the backend runtime.

The anonymisation module provides an API that is able to remotely transform data, by either performing encryption/decryption or by applying anonymisation techniques such as one-way hashing combined with k-anonymity/t-closeness/p-sensitive.

Multiple formats are supported and the most relevant are presented bellow in Figure 12.



Figure 12: Chimera Supported Connectors

3.10.1. Key Concepts and kinds of threat managed

Chimera aims to be a swiss army knife to deal with unstructured information, allowing for operators to use schema on read approaches, and define which fields should be extracted dynamically from the information they need to process. A normal workflow includes the following steps:

1. Read input data (either from files, URLs, or databases)
2. Define rules to extract dynamic fields
 - a. Either through regular expressions or custom-made parsers (key=value, csv, xml, json, etc)
3. Define the rules to transform fields (either add, remove or mutate in place)
 - a. Can anonymise, encrypt, decrypt, refactor data
4. Write output data (either to files, URLs or databases)

On the structured information side, a few well known formats are supported as inputs, such as Excel, Word, PDF, CSV. Out of the box Chimera parses these formats using third party libraries, converts them into the memory data structure representation of their textual values and from there they can be dealt with as if they were extracted from plain text files.

Common operations on these types are provided to ease the setup of new workflows, such as converting PDF to text, performing redaction on PDFs image layers, detecting PII and redacting PII.

3.10.2. Critics

Strengths	Weaknesses
<p>Easy integration with common formats</p> <p>Supports unstructured data formats</p> <p>High performance engine</p> <p>Easy to deploy (single binary and respective workflow configuration files)</p>	<p>GUI can be too focused on simple workflows</p> <p>Doesn't deal with image or video formats</p> <p>Custom DSL can be hard on new users</p> <p>No orchestrator to manage workflows, each workflow must be deployed on its own</p> <p>Key management needs to be delegated to an HSM such as Hashicorp vault to be secure</p>

Table 6: Strengths and Weaknesses of Chimera

3.10.3. Implications for CyberSANE

The Chimera Anonymisation Language (CAL) can be leveraged by the CyberSANE Project as a way to formally define how personal data at rest should be handled, transformed, anonymised, encrypted or decrypted, to keep relevant data protected from prying eyes.

As an example, below are a few simple redactions and anonymization types that are possible.

```

A) Raw event, 157 chars
<134>Dez 12 23:59:59 alfr04dnsvs named[28633]:
12-Dez-2015 23:59:59.849 queries: client 87.103.90.XXX#52442: query: www.facebook.com
IN A + (87.103.113.XXX)

B) Filtered, 68 chars
1436808722,87.103.90.XXX,52442,87.103.113.XXX,www.facebook.com,A,+

C) SHA1 + salt, 120 chars [SHA1 always 40 chars – License problem]
1436808722,8e28b667a35fdfa32512ea07ff810746e030487,52442,
8659e321f3e032929ade0e19e5b790d1034df91d,www.facebook.com,A,+

D) AES 128 + salt + Base64, 85 chars [Size linear with input & block size]
1436808722,AvlMiH9j+NQbvUOnljDzlg==,52442,fPxTwK6Cupx6TXxFCg==,
www.facebook.com,A,+
    
```

Figure 13: Example of Data Anonymisation with Hashing

Incident report data to be shared with third parties can contain sensitive data, which needs to be scrubbed before its ready to be shared. Chimera can help CyberSANE by providing custom workflows to deal with the datatypes and taxonomies defined to be used for security incident data sharing.

3.11. SPA

Smart Profiling Application (SPA) is an Identity and Access Management (IAM) software. This software combines a web interface, both for management and for user self-service functionality and background processes that ease the integration among several systems.

The software architecture comprises a set of modules, that when combined are able to address several security concerns and compliance measures. Such modules are:

- Identity Management: Supports multiple identity sources and merges identities in a centralized database

- Access Management: Publishes a catalogue of access and profiles for all the applications provided by a certain company, that can be assigned to our users, either by self-request, exception or pre-configuration of a list of accesses per user role(s) in the company
- Workflow Management: enables customisation of the workflow for each access request, depending on internal or external factors, that together will decide which path the access request will follow (e.g. approved by a manager, approved by IT, etc.)
- Compliance: A set of reports that may be filtered by an auditor using multiple filters to audit any user, access, request, application or risk classification
- Governance: Highly configurable interface, that allows our Backoffice to configure how the application handles certain events, such as role changes, contract changes, or any other event that may occur.

3.11.1. Key Concepts and kinds of threat managed

SPA aims to manage all the user and access lifecycle within a context (e.g. one company, a set of clients, etc.).

The top known IAM software has the same structure and main functionality, mostly providing web interfaces where users can see and/or request their access to several other systems and a powerful Backoffice where the operators can configure a set of settings that allow the software to be useful depending on each company needs in terms of process, policies and other factors.

Similar commercial tools are Oracle Identity Management and SailPoint.

SPA is both a competitor for other IAM tools in the market, and also complements them. From our experience using other IAMs, we’ve experienced the lack of these competitors to be flexible enough to address some of the processes required by the company. Our tool is mainly focused on giving our clients a flexible and highly configurable framework, where they can make their own configurations, both process wise, and even when integrating new systems. This means that our clients are not dependent on us to integrate with new software or to align with new policies in the companies, and we see this as a critical factor for any IAM process, therefore it’s one of our strengths.

Our application is constantly monitoring Human Resources (HR) databases for any contract changes, and managing user access according to their roles and/or requests, while providing a BUS with connectors (i.e. integrations) to grant or revoke user accesses to any system in a certain context (such as databases, LDAP, or any other).

Depending on our customer needs, we may operate with no inputs nor outputs, or in a hybrid way. In a typical scenario, our inputs would be the HR contractor database(s) and the access catalogues; while our outputs would be the grant/revoke of user access to external systems, as well as remediation on any access that is not certified in our database, among others.

3.11.2. Critics

Strengths	Weaknesses
Easy integration with external systems Highly flexible and configurable set of accesses per role(s) Modular SSO mechanisms using SAML and OAuth, working as an Identity Provided and/or Service Provider	The governance module has to have a set of out of the box process to align with standard policies and security standards, instead of being configured per customer Integration with external system should have a “solution oriented” set of connectors, instead of all of them configured in a low-level fashion Setup process should be able to be achieved by our customers

Table 7: Strengths and Weaknesses of SPA

3.11.3. Implications for CyberSANE

SPA is the piece of software that can bring to CyberSANE the sense of risk that each identity and/or device brings to the overall picture, by providing a centralized database of users, devices and access.

3.12. Other Solutions

3.12.1. Security Information and Event Management (SIEM)

SIEM is a platform for managing security incidents. It combines SIM and SEM to enable the collection of system logs and data from across data-centres for detecting and real-time reporting of suspicious activity. SIEMs are designed to provide a view of an organisation's IT security environment by supporting the analysis of security alerts generated by network hardware and applications in real-time. Many types of SIEM solutions and vendors that specialise in the provision of SIEM exist in today's market, and irrespective of the type and vendor, SIEMs provide basic functionalities that include (i) IR capabilities that allow organisations to aggregate information related to a potential incident; (ii) threat identification capabilities for effective identification and response to threats; (iii) threat reporting functionalities; and (iv) threat intelligence abilities for identifying threat information from different IT environments and their possible relation to an organisations assets. Below, we describe some known commercial or free SIEM tools found in the market.

3.12.1.1. Splunk

Splunk [23] is a commercial SIEM product that collects all machine data from various sources, including physical, virtual and cloud environments. It enables users to search, monitor and analyse the data from one place in real-time, to troubleshoot problems and investigate security incidents in minutes, to monitor the end-to-end infrastructure to avoid service degradation or outages, and to gain operational intelligence with real-time visibility and critical insights. Splunk supports several features like Data Model, Pivot, Distributed Search, and Apps. In particular:

- **Indexing:** Splunk indexes machine data. This includes data streaming from packaged and custom applications, application servers, web servers, databases, networks, virtual machines, telecoms equipment, operating systems, sensors, and so on that make up your IT infrastructure.
- **Data model:** A data model is a hierarchically-structured search-time mapping of semantic knowledge about one or more datasets. It encodes the domain knowledge necessary to build a variety of specialised searches of those datasets. These specialised searches are used by Splunk to generate reports for Pivot users. Data model objects represent different datasets within the larger set of data indexed by Splunk.
- **Pivot:** Pivot refers to the table, chart, or data visualisation you create using the Pivot Editor. The Pivot Editor lets users map attributes defined by data model objects to a table or chart data visualisation without having to write the searches to generate them. Pivots can be saved as reports and added to dashboards.
- **Search:** Search is the primary way users navigate data in Splunk. It can be used to write a search for retrieving events from an index, use statistical commands to calculate metrics and generate reports, search for specific conditions within a rolling time window, identify patterns in your data, predict future trends, and so on. Searches can be saved as reports and used to power dashboard panels.
- **Alerts:** Alerts are triggered when conditions are met by search results for both historical and real-time searches. Alerts can be configured to trigger actions such as sending alert information to designated email addresses, post alert information to an RSS feed, and run a custom script, such as one that posts an alert event to syslog.
- **Reports:** Reports are saved as searches and pivots. Reports can be run on an ad hoc basis, schedule them to run on a regular interval, and set a scheduled report to generate alerts when the result of a run meet particular conditions. Also, reports can be added to dashboards as dashboard panels.
- **Dashboards:** Dashboards are made up of panels that contain modules such as search boxes, fields, charts, tables, forms, and so on. Dashboard panels are usually connected to saved searches or pivots. They can display the results of completed searches as well as data from real-time searches that run in the background.

- **Apps:** Apps are a collection of configurations, knowledge objects, and customer designed views and dashboards. Apps extend the Splunk environment to fit the specific needs of organisational teams such as Unix or Windows system administrators, network security specialists, website managers, business analysts, and so on. A single Splunk Enterprise or Splunk Cloud installation can run multiple apps simultaneously.
- **Distributed Search:** A distributed search provides a way to scale deployment by separating the search management and presentation layer from the indexing and search retrieval layer. It can be used to facilitate horizontal scaling for enhanced performance, to control access to indexed data, and to manage geographically dispersed data.

3.12.1.2. Graylog

Graylog [24] is an open-source and free log analyser tool that enables log collection, visualisation, and trigger processes. However, a more advanced paid version of the product is provided with extra features like archiving, audit log, and user support. The following are the main features of Graylog:

- **Collect and process:** It parses and enriches logs, wire data, and event data from any data source. Graylog also provides centralized configuration management for 3rd party collectors such as beats, fluentd and nxlog. The processing pipelines allow for greater flexibility in routing, blacklisting, modifying and enriching messages in real-time as they enter Graylog.
- **Analyse and search:** It searches through terabytes of log data to discover and analyses important information. It uses powerful search syntax to find what the user is looking for. It saves search queries to share.
- **Visualisation:** It creates dashboards to visualise metrics and observes trends in one central location. It uses field statistics, quick values, and charts from the search results page to dive in for deeper analysis of your data. The simple user interface enables team members to access the wealth of information and add new charts easily.
- **Alert and Trigger:** It triggers actions or notifies users when something needs attention, such as failed login attempts, exceptions or performance degradation.
- **Central Management:** Graylog gives the team access to runtime configuration and the log data they need without touching the Graylog servers. No need to restart the system. **DevOps:** It lets developers set up parsing of their messages, to configure streams on the fly and route messages to their workstation for debugging.
- **Users and Roles:** It groups users into roles to simplify permission management. The administrator can also restrict what kind of log messages certain users are allowed to access, using real-time categorisation functionality.
- **LDAP:** Graylog can be integrated with the existing LDAP user directories.
- **Archiving:** It automatically archives the data that the user does not search through very often. It stores this data on more cost-effective, slower hard disks and makes it available for search in Graylog only when there is such a need.
- **Audit log:** Audit Log records and stores actions taken by a user or administrator that make changes in the Graylog system.

3.12.1.3. Elastic SIEM

Elastic SIEM [135] is an open source solution by Elastic Co, which is built on top of the ELK stack (Elastic, Logstash, Kibana). The SIEM is an app in Kibana where the security analytics can perform log analysis, create interactive dashboards, and do run of mill event triage or security incident investigations. Additionally, machine learning anomaly detection jobs and detection engine rules provide ways to automatically detect suspicious activity across your entire fleet of servers and workstations.

Elastic SIEM requires the following Elastic Stack components:

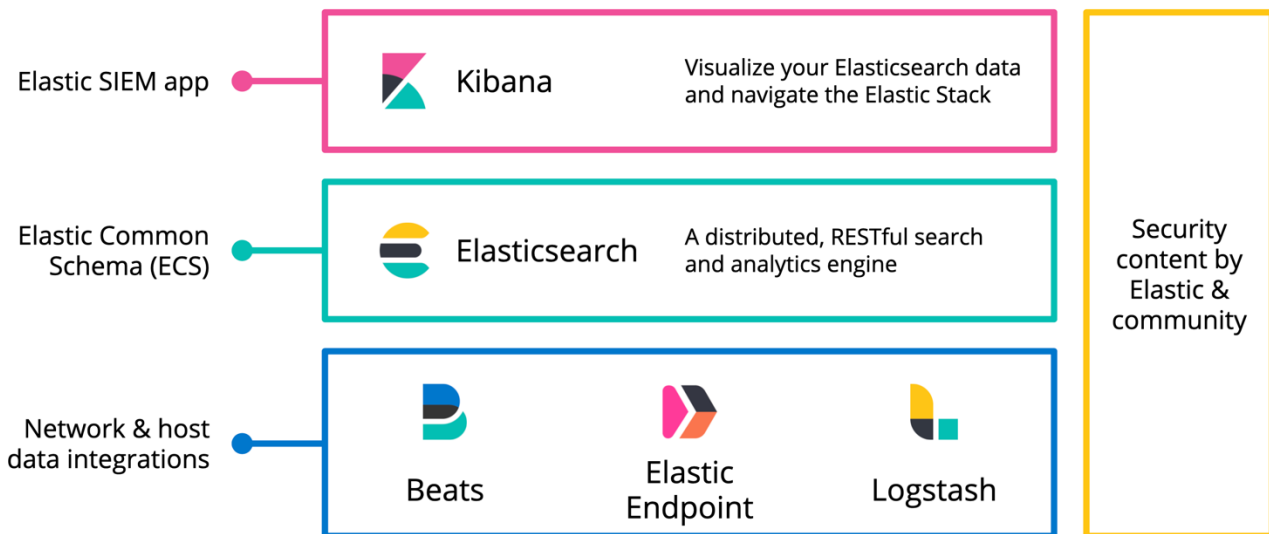


Figure 14: Elastic SIEM Stack

ElasticSearch [22] - is used as the database providing the distributed storage, search, and analytics engine. It's based on the opensource text indexing tool Lucene, a Java library that provides indexing and search features, as well as spellchecking and advanced analysis/tokenization capabilities.

Beats and Logstash – are open source data shippers that are installed as agents on the relevant systems, they send security events and other data to Elasticsearch. They are the main data collectors and can-do initial parsing of the logs, creating a schema-on-write by extracting fields with regular expressions or grok rules.

Elastic Endpoint – is the endpoint security platform and agent that provides prevention, detection, and response capabilities. It ships events and security alerts directly to Elasticsearch.

Kibana - is the frontend web application that can perform analytics and custom visualizations, it was designed from the ground up to work with Elasticsearch. Kibana can search, view, and interact with data stored in Elasticsearch indices. Can perform advanced data analysis and visualize data in a variety of charts, tables, and maps.

3.12.1.4. IBM QRadar SIEM

QRadar SIEM is a commercial, highly scalable, enterprise solution that consolidates log source event data from thousands of devices distributed across a network, storing every activity in its database, and then performing immediate correlation and application of analytics to distinguish real threats from false positives. It also captures Layer 4 network flow data and, more uniquely, Layer 7 application payloads, using deep packet inspection technology. An intuitive user interface shared across all QRadar family components helps IT personnel quickly identify and remediate network attacks based on priority, ranking hundreds of alerts and patterns of anomalous activity into a drastically reduced number of offences warranting further investigation [25].

IBM Security QRadar SIEM provides enterprise visibility and threat intelligence for Systems, Applications and Products for data processing (SAP) environments. It provides capabilities for real-time analysis, threat detection, and incident management with sophisticated correlation using data from the SAP environment. The following list describes the SAP integration features [26]:

QRadar Log Manager functionality includes:

- Real-time analysis, threat detection, and incident management based on data from the SAP environment.
- Sophisticated correlation, incorporating diverse data sets collected from the SAP environment (event, flow, asset, vulnerability, and external intelligence).
- Managing flows for full network behaviour analysis.

- Asset profile creation and management for all assets in the SAP environment.
- Incident management for problems found in the SAP environment.

QRadar SIEM collects information that includes:

- Security events: From firewalls, VPN, IDS, intrusion prevention systems, databases and more.
- Network events: From switches, routers, servers, hosts and more.
- Network activity context: Layer 7 application context from network and application traffic.
- User or asset context: Contextual data from IAM products and vulnerability scanners.
- Operating system information: Vendor name and version number specifics for network assets.
- Application logs: Enterprise Resource Planning (ERP), workflow, application databases, management platforms and more.
- Threat Intelligence: From sources such as IBM X-Force.

QRadar SIEM contains a variety of **anomaly detection** capabilities to identify changes in behaviour that could be indications of an insider threat. QRadar SIEM can detect off-hours or excessive usage of an application or cloud-based service, or network activity patterns that are inconsistent with historical, moving-average profiles and seasonal usage patterns. QRadar SIEM learns to recognise these daily and weekly usage profiles, helping IT personnel to quickly identify significant deviations. The QRadar SIEM centralised database stores log source events and network flow traffic together, helping to correlate discrete events with bidirectional network flow activity emanating from the same IP source. It also can group network flow traffic and record operations occurring within a narrow time period as a single database entry to help reduce storage consumption and conserve license requirements. The capabilities of QRadar SIEM can be expanded further by downloading apps from the IBM Security App Exchange. This exchange allows customers, developers, business partners, and clients to collaborate and share applications, dashboards, custom rules, reports, and other enhancements to QRadar SIEM. Solutions can be found here to help address the latest security threats, without having to wait until the next product release.

3.12.2. Incident Response Systems and SOAR

Incident Response systems (IRs) and platforms provide automated processes for preparing, detecting, reporting, assessing and responding to security breaches. IRs are mostly utilised by companies to monitor the IT environment (such as networks, infrastructure and endpoints) for intrusion and anomaly detections, as well as real-time threat response. An important benefit of IR systems and platforms is that they can detect a variety of known threats or incident types in accordance with a company's policy or SLA, and can be used to escalate a threat level after threats have bypassed security mechanisms particularly if critical information assets are affected. Generally, IRs offer automated functions such as best practice response plans, attack behaviour analytics, real-time detection and forensics, anomaly detection, automated response to security alerts, timeline analysis to identify threats, automated escalation of security incidents and reporting of a breach to privacy policies. SOAR is the class of solutions that help security response teams respond to the multitude of event, alarms and alerts that arrive at lightspeed from the sensors, anti-virus, probes, network security devices and all the other appliances used to protect organizations computers. They are designed to enable combining comprehensive data gathering, case management, standardization, workflow and analytics to provide organizations the ability to implement sophisticated defence-in-depth capabilities.

They usually consolidate alarm data from each deployed platform and place them in a single location to give security analysts a single point of interaction. SOAR's follow a case by case approach where they allow users to research, investigate, explore relevant data for a single case. This segregation of data is a strong foundation to support larger teams with different abilities and responsibilities.

Dealing with high volume of alarms means in SOAR multiple integrations exist, mainly to ensure security incident response workflows can be as automated as possible and provide a clean and clear automatic defence. An instantiation of this process is to have a set of playbooks that deal with specific threats, then each step is automated to what is deemed relevant by the organization, trying to reduce the human interaction requirements, and maximize the throughput of incident response. Integrations with third-party solutions are often required, for covering the full lifecycle of incident response.

SOAR's main benefit to a SOC is that it automates and orchestrates time-consuming, manual tasks, including opening a ticket in a tracking system, such as Jira, without requiring any human intervention which allows engineers and analysts to better use their specialized skills.

Some of the IR and SOAR systems are discussed in this section:

3.12.2.1. Resolve

Resolve [103] is a solution that focuses on incident detection and prevention in IT infrastructure systems. The platform was initially designed to focus on IR and management but has expanded preventive measure capabilities such as secure provisioning, patch management and audit trails. It enables the capture of all incident-related activities for compliance, forensics, evidence preservation and reporting. The platform also provides an integrated environment that ensures incident responders across an organisation follow standard-based process guidance, play-books and options for a human-guided and fully-automated security IR process based on the recommendations of NIST Special Publication (SP) 800-61 (Computer Security Incident Handling Guide).

3.12.2.2. RTIR

Request Tracker for Incident Response (RTIR) [148] is an opensource incident response solution, that brings pre-configured queues and workflows designed for incident response teams. RTIR was built to fulfil the specific needs of CERT teams. It's first release is from 1999 but in 2006 it was expanded and upgraded thanks to the funding from several CSIRTs from Europe. Having been born in this environment it is not surprise that it is still today a tool of choice for many CERT and CSIRT teams.

As main functionalities, it can correlate key data from incident reports, both from people and automated tools, to find patterns and link multiple incident reports with a common root cause incident. Security incidents lifecycles can be managed fully in RTIR where it manages communication to multiple interested parties including counterparts at other security teams collaborating on responses, and other internal teams coordinating countermeasures.

3.12.2.3. IBM Resilient

IBM resilient is an Enterprise licensed incident response platform. It does not enable quicker detection of malicious activity; this is a function of the existing security infrastructure. Likewise, Resilient does not perform the remediation. Instead, the Resilient solution accelerates the incident response workflow once an incident has been detected, leading to a significantly reduced time to enact the remediation and containment procedures otherwise explained as the period of time between mean-time-to-detect (MTTD) and mean-time-to-contain (MTTC).

IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform is a platform for orchestrating and automating incident response processes. IBM Resilient SOAR Platform integrates with the organization's existing security and IT solutions. It aims to make security alerts actionable, and provides intelligence and incident context, finally it enables adaptive response to cyber threats.

The orchestration includes:

- **Dynamic Playbooks:** Provides the agility, intelligence, and sophistication needed to contend with complex attacks. Dynamic Playbooks automatically adapts to real-time incident conditions and ensures repetitive, initial triage steps are complete before an analyst even opens the incident.
- **Visual Workflows:** Enables analysts to orchestrate incident response with visually built, complex workflows based on tasks and technical integrations.
- **Incident Visualisation:** Graphically displays the relationships between incident artefacts or IOCs and incidents in an organisation's environment. [102]

D2.1 – Cyber Incident Handling Trend Analysis

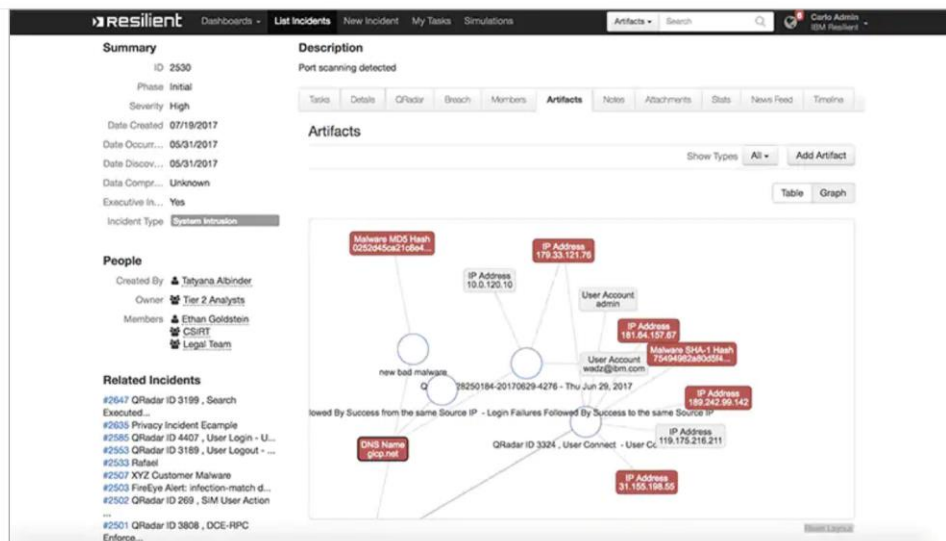


Figure 15: IBM Resilient

3.12.2.4. Splunk Phantom

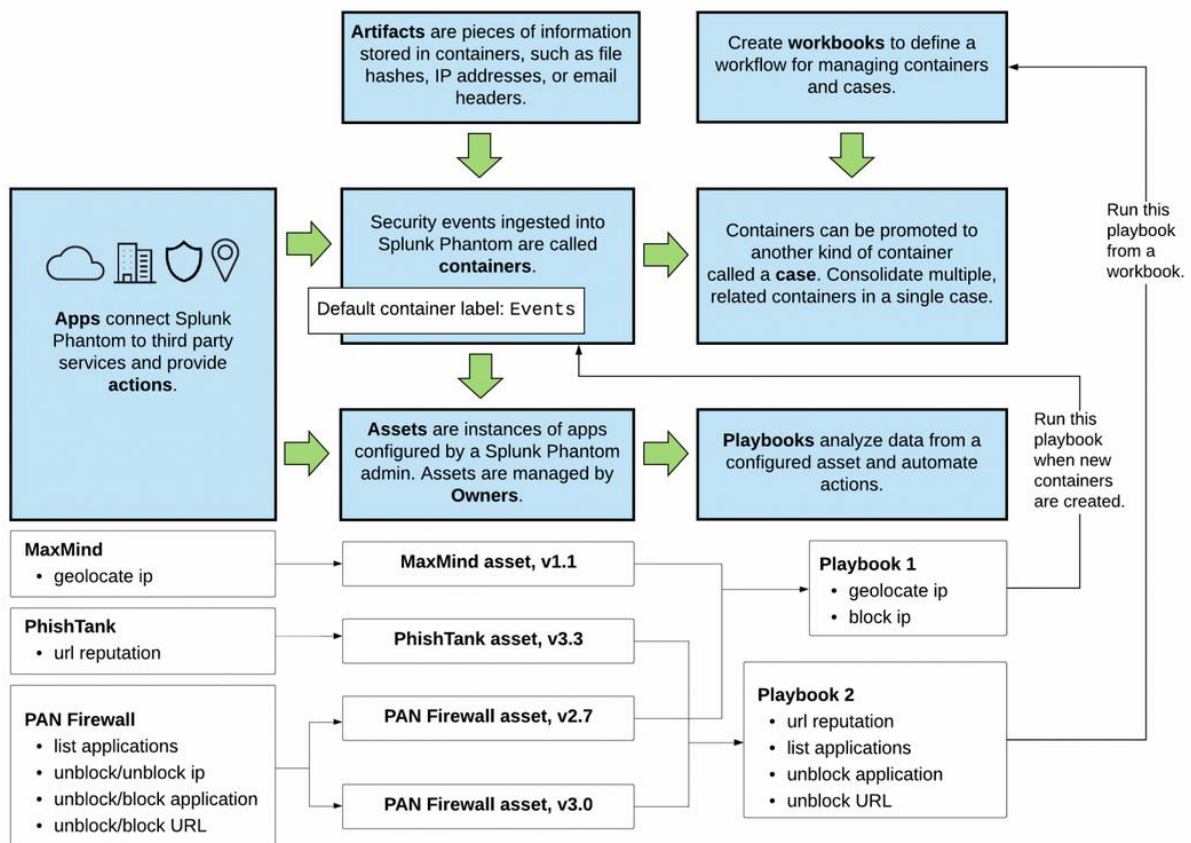


Figure 16: Splunk Phantom Example [138]

Splunk Phantom is a SOAR platform built on top of the Splunk log management solution. Phantom started as an independent company and was acquired by Splunk in 2018. The product was then rebranded Splunk Phantom and has seen continuous improvement and investment since then. The Splunk Phantom platform

combines security infrastructure orchestration, playbook automation and case management capabilities to integrate your team, processes, and tools together.

It's highly integrated into the existing Splunk Platform and provided out of the box a set of integrations with third parties such as phistank or maxmind databases. This enhances the natural abilities of Splunk to provide good event correlation with relevant external sources that can be used in playbook actions. These actions are at the core of the automation capabilities for Phantom.

The playbooks can be visually defined and configured, and are usually provided with good defaults, enabling administrators that might not be too familiar SOAR concepts to be productive. Below in Figure 17 we can see an example of the type of playbook and respective actions available.

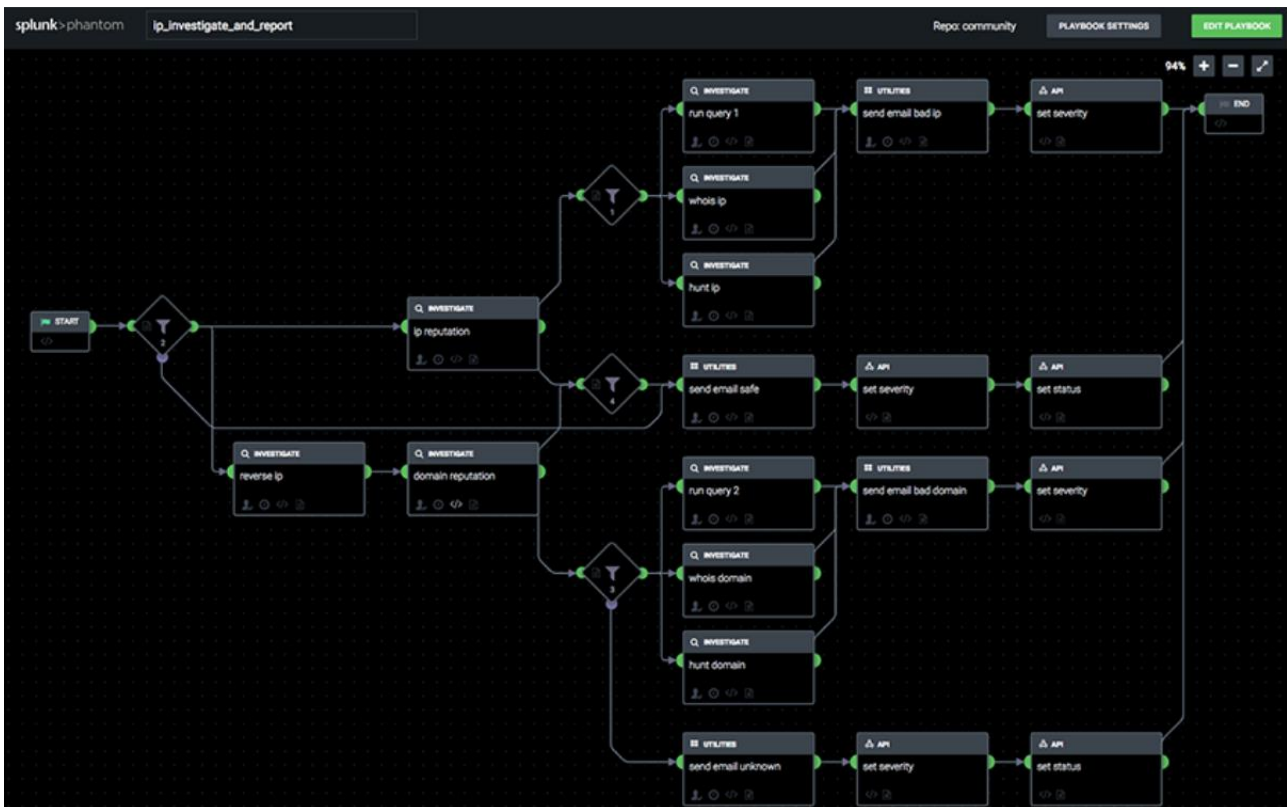


Figure 17: Splunk Phantom Playbook Example

3.12.3. Digital Forensics Tools

Digital forensics is the collection and examination of digital evidence residing on electronic devices and the subsequent response to threats and attacks. Digital forensics can be used for various purposes such as cybercrime investigation, IR and analysis, policy violation etc. Various tools have been developed in recent years to accomplish digital investigation process and support the ability to acquire data from a wide variety of IT infrastructure, including systems and networks, provide visibility into processes and actions that occurred across systems, and support a comprehensive and forensically-sound investigation. Many commercial and free source forensic tools have been developed to provide specific features such as evidence acquisition, analysis, documentation and reporting, data recovery and carving, file analysis, and log file analysis. A brief description of some of these tools is provided.

3.12.3.1. EnCase Forensic

EnCase [104] is a digital forensic solution developed to enhance efficiency, forensically-sound data collection, identification, and reporting in a repeatable process. EnCase is one of the most widely used digital forensics tools across the industry as well as the court of laws around the globe for digital media analysis. It is available

within many products, currently, including EnCase Forensics Endpoint Security, EnCase Security, EnCase eDiscovery, and EnCase Portable. The EnCase Forensics is the de-facto digital forensic tool that offers the capabilities for the preservation of crime-related digital evidence and allows a forensic examiner to acquire data from a wide range of volatile or non-volatile devices, discover potential evidence and the creation of comprehensive reports while also maintain the integrity of evidence. Some of the key features supported by EnCase Forensic include:

- **Evidence Acquisition:** EnCase Forensic tool can be used to acquire data from myriad device types and various sources such as networks, documents, disk, RAM, images, email, cache, compressed files, backup files, encrypted files, RAID5, workstations, servers, smartphones etc. Another important feature of the tool is the capability to acquire data from cloud services, which is particularly important for mobile devices that use data stored in the cloud. Currently, EnCase supports cloud services such as Google Drive, Amazon Alexa, Gmail and Facebook
- **Advanced Inspection and Analysis:** the tool can be used for the inspection and analysis of evidence in relevant files such as deleted files, file slack and unallocated space, as well as for evidence management of large quantities of files by parsing event logs, file signature analysis, and hash analysis, even within compounded files or unallocated disk space.
- **Automated de-NISTing Capabilities:** The National Software Reference Library (NSRL) is provided in the EnCase hash library format, allowing the user to easily de-NIST their evidence, eliminating thousands of known files from their evidence set, which significantly reduces the time and amount of data that needs to be analysed.
- **Automatic Reports:** EnCase supports the features for generating reports containing a list of lists of all files and folders along with a detailed list of URLs, with dates and time of visits. Provide hard drive information and details related to the acquisition, drive geometry, folder structure, etc.
- **Actionable Data:** another important feature of EnCase is that allows digital forensic investigators to create a comprehensive report that can be admissible in the court of law.

3.12.3.2. Forensic Toolkit (FTK)

Similar to EnCase, Forensic Toolkit (FTK) [63] is another widely used forensics investigation solution that helps law enforcement and cybersecurity professionals to access and forensically evaluate the evidentiary value of files, folders, and computers. It provides integrated features to support in-depth data processing integrity, imaging, indexing and analysis, in addition to filtering and search functionality, and access to remote systems on a network. Some of the major capabilities of FTK include:

- **File Decryption:** file decryption is one of the important features of FTK that is used for decrypting entire files and recovering passwords, including creating images, conducting an investigation and building a report.
- **Email Analytics:** FTK provides capabilities for forensic email analysis, including the ability to parse emails for certain words, header analysis for the source IP address, the social network of an email custodian for determining strength/frequency of communication, peak email communication periods etc.
- **Optical Character Recognition (OCR):** FTK provides the OCR engine that allows the conversion of images to readable texts such as PDFs and TIFFs, which enhances forensic examiners ability to pull text out of graphics files found on hard drives.
- **Cerberus:** Cerberus is another analytics feature that provides automated malware detection capabilities. It allows forensic examiners to perform malware analysis on executable binaries on a disk, network or system memory. The Cerberus consists of threat analysis, which aims to identify potentially malicious code on general file and metadata, and static analysis that mainly examines the elements of the code.

3.12.3.3. SleuthKit & Autopsy

Autopsy and Sleuth Kit are arguably the best known opensource toolkit for performing digital forensics, they complement each other, with Autopsy being the front end with a new GUI that allows users to analyse hard drives, mobile devices and smart card raw images. They both provide an extensible API for third party plug-

ins; several python and java add-ons are available to offer complementary services. Such as file carving, hidden image detection, file hasher, virus total checkers and many others.

The Sleuth Kit is a collection of command line tools and a C library that allows you to analyse disk images and recover files from them. It is used behind the scenes in Autopsy and many other open source and commercial forensics tools.

3.12.3.4. ProDiscover Forensic tool

ProDiscover [64] is another forensic product that combines the features for digital forensic and IR. It supports most of the basic digital forensics' capabilities such as disk imaging, the discovery of hidden data, and file metadata information and ensures that both capturing and analysis processes are performed according to forensically-sound processes. Also, it provides other network-based digital forensic functions such as the ability to access computers over the network for enabling media analysis, image acquisition, recovery of deleted files, and analyse network behaviour. Other capabilities supported by the tool include remote analysis of running processes, open files, open ports and services and other network-based functions. Some of the key features of ProDiscover are as follows:

- Incident Discovery: ProDiscover enables the identification of systems and network devices that have been compromised as well as enabling the gathering of digital evidence.
- Remote forensics: the tool supports the remote forensic examination of live systems to uncover Trojans, rootkits, including kernel mode Trojans.
- Utilises remote agent to read the cybercrime suspect's disk at bit level, enabling a forensic examiner to examine all the contents of the disk, including Host Protected Area (HPA) and Windows Alternate Data Streams.
- Integration: The tool is integrated with a full-text search engine, set of embedded viewers and hash comparison methods, for providing a powerful toolkit to forensic investigators.
- Automatically creates and records MD5, SHA1 and SHA256 hashes of evidence files to prove data integrity.
- Preview and search cyberattack suspect's files to find evidence quickly and without altering any data or metadata.
- Capture volatile state information such as open ports with connected IP addresses, route tables, ARP cache, logged-on users, etc. to investigate an incident.

3.12.4. Network Behaviour Anomaly Detection Systems (NBADS) tools

3.12.4.1. Anodot Anomaly Detection

Anodot Anomaly Detection [27] is a real time business incident detection system providing real-time analytics using online machine learning algorithms, offering a scalable platform for visualising, alerting and searching [28]. Key aspects of its technologies are automation, scaling and creation of own, highly adaptive algorithms. Anodot's flow includes: i) learning the normal behaviour of its metric separately, ii) detecting (single) anomalies, iii) trying to combine single metrics and iv) trying to interpret combined metrics.

Anodot uses a hybrid approach of learning method, semi supervised learning [29], which uses both labelled and unlabelled data to perform an otherwise supervised or unsupervised learning task. The learning implementation of Anodot includes: i) Using a few labelled examples to improve unsupervised methods ii) Using unsupervised detection for unknown cases and supervised for known.

It Monitors time series and Identifies deviations (anomalies) from metrics normal behaviour patterns. Two of the most important properties that Anodot focuses in order to achieve this are automatic determination of the proper model and seasonality detection.

In Anodot, every dataset gets automatically classified to a model type [30] that it may fit best. Model types include: Smooth, Irregular Sampling, Multi Modal, Sparse, Discrete, Step and other. This task is a rather complex one and it gets even more demanding taking account that data may include a changing behaviour over

time. So, approaching the appropriate model is one challenge and adapting to the changing nature of it is another that Anodot faces and offers solutions.

In order to enhance the interpretation of normal behaviour, an analyst should also look for seasonality in data. Anodot is patenting its own algorithm to detect this seasonal data variation, called Vivaldi, which is based on serial correlation [31] but also uses smart subsampling to reduce computational complexity [32].

In addition, Anodot performs cloud based real time processing, using large scale data from any software, either using an API or small relay. For real-time decision making and adapting to changes in datasets Anodot [30] employs online machine learning algorithms. This family of algorithms start from an initial guess model which gets updated with every data point. In other words, “the machine learns as the data come in piece by piece”. According to Anodot research team, online machine learning algorithms scale easier to metrics additions and larger datasets than batch learning algorithms (which accept training data to train a model).

Moreover, the algorithms need to be highly adaptive in order to confront frequently changed patterns. On the stage of normal behaviour learning process, a time window is set where an average value of this period for a metrics are calculated and then compared to the new values. If there is a big deviation then an anomaly might have occurred. In the matter of defining the Learning Rate, which refers to the time period mentioned before, Anodot uses auto-tuning of the parameters. When an anomaly is spotted model learning rate is adapted by giving anomalous data a lower weight. If it appears again a higher weight is applied. This way anomalies get handled but their impact does not exceed the level it should be [32].

In addition to being adaptive in algorithms, Anodot supports creation of composite metrics using a rich set of analytic functions. It follows a hybrid approach to number of metrics used to detect an anomaly. Combines Univariate detection, meaning examining every metric by itself, to Multivariate Anomaly Detection (MAD) which takes input from all the signals together as one. This approach seems to be scalable, but requires additional work.

In the stage of Anomaly Behaviour learning Anodot offers an anomaly scoring statistical model. The input of the model is a set of statistics (like deviation, duration and other) related to each anomaly and the output is a score (0 to 100) of significant the anomaly is. This leads to filtering anomalies based on their importance. To calculate the anomaly score, Anodot does not use an absolute value, but a value relevant to past anomalies on that metric. To achieve that Anodot uses probabilistic Bayesian models [30].

Finally, Anodot uses Abnormal Based Similarity processes to create metrics relations. The combination of metrics gives a better understanding of the incident. These processes are implemented using Latent Dirichlet Allocation Algorithm (LDA) [33] with some enhancements. LDA performs “soft clustering”, allowing a metric to belong to more than one group and also allows partial similarity for a metric to still belong to a group [30].

Other features which most refer to user interface include:

Providing a configurable graphic dashboard for metrics display and grouping.

Providing support for easy metrics configuration.

Isolating and zooming on an identified anomaly.

Configuring alerts according to the significance of the anomaly.

3.12.4.2. WEKA

Weka is a collection of machine learning algorithms and visualisation tools for data mining tasks like reprocessing, Classification, Regression, Clustering, Associating, Visualisation and Features Selection as well as Big Data analysis. Weka provides support for experimental data mining, like preparing input, evaluating, learning, visualising input and results [34, 35, 36].

Weka consists of four main interfaces:

- **Explorer.** Provides the main interface which is user friendly and helpful. Explorer’s subcomponents include:

- **Pre-process:** This component is responsible for importing data and modifying it. Its tools are called filters and typical methods are: Discretisation, Normalisation, Resampling, Attribute Selection, attributes transformation and combination.
- **Classify:** Classification and regression. Offers Bayesian, Trees, rules, functions, lazy classifiers and a miscellaneous category.
- **Cluster:** Weka offers the use and configuration of Cobweb, SimpleKMeans, Expectation–Maximisation (EM), HierarchicalClusterer, FarthestFirst and Canopy clustering algorithms. Users can define parameters such as the number of clusters to be generated, the maximum number of iterations and the minimum allowable standard deviation for normal density calculation [65].
- **Associate:** Weka offers three association rule learners, Apriori, FPGrowth and FilteredAssociator.
- **Select attributes:** Weka is compatible with both common strategies: Dividing first into subsets or evaluating each attribute individually from the beginning discarding those whose value is below a certain threshold.
- **Visualise:** Visualisation panel embodies a two-dimensional scatter plot matrix to visualise a dataset. Scatter plots can be enlarged and analysed through selection operators. The matrix is highly configurable and assists in understanding data and their relations.
- **Experimentation:** Examines the machine learning algorithms on a collection of datasets in order to decide what’s best for each use case and setting up automated tasks. This feature also is helpful in distributing the work load to multiple machines.
- **Knowledge flow:** Through the dragging of boxes, a user can design stream procedures so to create a data stream. Boxes represent learning algorithms. This feature also allows incremental learning.
- **Workbench:** Combines everything else in one interface, even adding plugins the user may have installed.

3.12.4.3. Scikit Learn

Scikit-learn (formerly scikit.learn) [66] is a free software machine learning library for the Python programming language. It features various classification, regression and clustering algorithms and it is designed to interoperate with the Python numerical and scientific libraries.

The vision for the library is a level of robustness and support required for use in production systems. This means a deep focus on concerns such as ease of use, code quality, collaboration, documentation and performance.

Scikit-learn provides a range of supervised and unsupervised learning algorithms via a consistent interface in Python, such as:

- KNN
- K-Means
- Linear Models
- Naive Bayes Classifiers
- Decision Trees
- Random Forests
- Gradient Boosted Decision Trees
- Kernelized SVMs
- Neural Networks
- Density-Based Spatial Clustering of Applications with Noise (DBSCAN)

In addition to these machine learning algorithms, scikit-learn also provides a set of tools for carrying out a Principal Components Analysis, as well as for data pre-processing (scaling, normalisation, etc..).

The scikit-learn project is constantly being developed and improved and has a very active user community. It contains a number of state-of-the-art machine learning algorithms, as well as comprehensive documentation about each algorithm on their website. Since scikit-learn is very popular and one of the most prominent Python libraries for machine learning, it is widely used in industry and academia. Thus, in addition to all the official documentation, there is a wealth of tutorials and code snippets about scikit-learn available online.

3.12.4.4. TensorFlow

TensorFlow is an open source software library for machine learning across a range of tasks, developed by Google to meet their needs for systems capable of building and training neural networks to detect and decipher patterns and correlations, analogous to the learning and reasoning which humans use.

TensorFlow is Google Brain's second-generation machine learning system, released as open source software. While the reference implementation runs on single devices, TensorFlow can run on multiple CPUs and GPUs (with optional CUDA extensions for general-purpose computing on graphics processing units).

TensorFlow is an open source software library for numerical computation using data flow graphs. Nodes in the graph represent mathematical operations, while the graph edges represent the multi-dimensional data arrays (tensors) communicated between them. The flexible architecture allows for the deployment of computation to one or more CPUs or GPUs in a desktop, server, or mobile device with a single API.

Although it was originally developed within Google's Machine Intelligence research organisation for the purposes of conducting machine learning and deep neural networks research, the system is general enough to be applicable in a wide variety of other domains as well.

Getting started with TensorFlow is not as easy as with other libraries, such as scikit-learn. However, there is plenty of online documentation in its web site, provided by the Google development team. In addition to that, since TensorFlow became free access in 2015, there is an active worldwide community contributing to the project itself. This community also provides support for developers of applications using TensorFlow. As a consequence, there is a lot of online tutorials, code snippets and forums.

3.12.4.5. Keras

Keras [67] is a high level, open source neural network library written in Python. It is capable of running on top of MXNet, Deeplearning4j, TensorFlow, CNTK or Theano.

Keras has been designed to enable fast experimentation with deep neural networks. In particular, it supports both convolutional and recurrent neural networks, as well as combinations of the two. It was developed to run either on CPU or GPU systems, when available, which makes it more versatile.

Keras' API is simple and consistent, developed to be user friendly, not only in order to make users' learning curve faster, but also to minimise the number of user actions required for common use cases and to provide a clear and actionable feedback upon user error.

Keras was also designed to be modular. A model is understood as a sequence or a graph of stand-alone, fully configurable modules that can be plugged together with as little restrictions as possible. In particular, neural layers, cost functions, optimisers, initialisation schemes, activation functions, regularisation schemes are all stand-alone modules that you can combine to create new models.

Models are described in Python code, which is compact, easier to debug, and allows for ease of extensibility. New modules are simple to add (as new classes and functions), and existing modules provide ample examples. To be able to easily create new modules allows for total expressiveness, making Keras suitable for advanced research.

3.12.5. Honeypots

A honeypot [37] is a tool set to detect, gather and analyse the attack trends setting a false environment with apparently sensitive information. It's generally used as a set of services and data accessible through internet that appears to be legit, however these deployments are isolated from the real network and monitored. The attacker is baited, and all actions are logged for future analysis with the main goal to prevent them. This will be achieved through the creation of new detection and prevention rules. Service and network flaws can be detected as well as exploits being used. As a trend detector, for instance, an increment of attacker's activity through a specific port or service could raise the awareness level.

Honeypots can be classified as production or research based on their deployment. Production ones are deployed inside production network, are easy to use but capture only limited information, they are usually low-interaction honeypots. Research honeypots are used to research about the threats and to learn how to improve protection against them. Research ones are often more difficult to maintain and deploy due to the large amounts of information gathered.

Honeypots can also be classified based on design criteria and attacker interaction level. Low interaction honeypots run a fake service, application or operative system and lack capabilities to gather high amount of information. HoneyC, HoneyD, Dionaea, Hontel, Honeytrap, RDPy Glastopf, Conpot are examples of low interaction honeypots. Medium interaction honeypots run services capable of responding the attacker such an FTP server or SSH connection. However, if the attacker is used to, he can easily understand that is a simulated service. Kippo, Cowrie and Shiva, are examples of medium interaction honeypots. High interaction level honeypots are true applications with false data, designed to log all attacker activities. Hihat, HonewBow, Sebek and Capture-HPC are some examples of high interaction honeypots.

Below you can find some widely used honeypots:

3.12.5.1. Conpot

Conpot is a low interaction open source honeypot oriented to industrial control systems (ICS / SCADA). This tool provides a range of common industrial protocols like s7comm, capable to emulate complex infrastructures and so on to convince and deceive the attacker that he is targeting a huge industrial complex. Furthermore, Conpot can even deploy a human machine interface to enhance the attack surface.

3.12.5.2. Dionaea

Dionaea (previously known as Nephentes) is a low interaction honeypot and its intention is to trap malware exploiting vulnerabilities exposed by services offered to a network. It's designed to emulate vulnerabilities in order to intercept the code of the malicious software like worms who use them to propagate. This honeypot can launch different services like FTP, HTTP, MSSQL, SMB, etc. The tool is able to capture and log the binary files used by attackers. For instance, shell-codes used in HTTP or payloads in SMB. A web interface, DionaeaFR is available to analyse the gathered information.

3.12.5.3. Cowrie

Cowrie (Kippo fork) is a medium interaction SSH and Telnet honeypot designed to log brute force attacks and the shell interaction performed by the attacker based on python. It's able to emulate a fake filesystem resembling a Debian 5.0 installation. Files can be monitored and session logs stored in UML compatible format and can also capture binaries.

3.12.5.4. SHIVA

SHIVA (Spam Honeypot with Intelligent Virtual Analyser) is a medium interaction SMTP honeypot. It's is an open but controlled relay Spam Honeypot (SpamPot), built on top of Lamson Python framework, with capability of collecting and analysing all spam thrown at it. Analysis of data captured can be used to get information of phishing attacks, scamming campaigns, malware campaigns, spam botnets, etc. Shiva is the reference point of SMTP honeypots; the main advantage is the full email log. It can gather information regarding IP source, email destination address, email source address, email headers, subject, message content, URLs in content and attached files.

3.12.5.5. RDPy

RDPy is a low interaction Remote Desktop Protocol honeypot. This tool emulates a host with this protocol enabled and accepts RDP connections. It's used to gather and log the attacker interaction with the service. RDPy is python based, and is capable to log date time, login and password used as well as the source IP.

3.12.5.6. Glastopf

Glastopf is a web application low/medium interaction honeypot. Vulnerability type-based emulation instead of vulnerability emulation. Once a vulnerability type is emulated, Glastopf can handle unknown attacks of the same type. As advantage, it has a modular design that enhances the addition of new logging capabilities or attack type handlers. Various database capabilities are already in place. HPFeeds logging is supported for centralized data collection. Popular attack type emulation is already in place: Remote File Inclusion via a build-in PHP sandbox, Local File Inclusion providing files from a virtual file system and HTML injection via POST requests. It also supports Docker deployment.

3.12.6. Network Access Control Tools

Network Access Control (NAC) solutions are necessary to maintain the security of the network and ensure the resilience of the infrastructure. In order to meet their objectives, the NAC includes four main functionalities: **authentication**, **authorisation**, **evaluation** and **remediation**.

First of all, a NAC system will **authenticate** devices and users who want to access to the network no matter how the connection is made, wired, wireless or even remote via VPN. The device who wants access, will first try to authenticate with the communications device using their protocols (open or closed) who will redirect the request to the NAC to grant the authorisation. As an authentication process is a back-end process, it provides a database with users, passwords and cryptographic certificates. In addition, NAC devices often integrate RADIUS and Active Directory functionalities.

Once the device or host is authenticated, NAC will apply specific **authorisation** policies regarding the device type and the user. Policies can involve user role types for instance a guest user will have limited access. This tool is integrated in the communications infrastructure and through the use of Access Control Lists (ACLs) can isolate devices moving them to a specific more restricted Virtual LAN (VLAN).

Regarding the **evaluation** functionality a NAC can check if the device is configured according to their policies. If the corporate environment makes use of an antivirus software and an agent must be installed, NACs are able to check and raise an issue accordingly. Everything that is defined by the policies, is constantly evaluated. If the device does not meet the requirements established, actions can be programmed as an active response.

Remediation actions can be executed from NAC devices to meet the security requirements needed. As an example, if a Windows host is not updated with the latest patches, internet navigation can be restricted to Windows Update servers and a message can be displayed to warn the user. Furthermore, some NAC tools deploy their own agents to have a widest range of actions, giving them the possibility to execute updates, scripts, etc.

3.12.6.1. OpenNAC

OpenNAC [68] is an open source NAC that provides secure access for LAN/WAN. It allows the application of flexible access policies based on rules. It works with a wide range of clients (Windows, Mac, and Linux) and network devices (Extreme Networks, Cisco, Alcatel and 3Com). It is based on well proven open source components like FreeRadius, iTop and Icinga. Extensible and very flexible, it is easy to add new functionalities. It is open to be integrated with current platforms like accounting, asset management, authentication and NIDS.

Apart from core NAC, OpenNAC has value added services like network configuration and discovery, network device configuration backup and network monitoring.

OpenNAC is divided into components with different functionalities called, onNAC, onNETCONF, etc. In particular, it integrates the following components:

- **Multiple Deployment Modes:** All OpenNAC services are packaged in a virtual appliance that can be run on a VMware or a KVM environment. For cloud environment, a VPN connection can be made between the customer infrastructure and the OpenNAC private cloud.

- **Web based management:** All services can be managed by a web frontend, with 24x7 monitoring and support service available on demand.
- **onNAC:** OnNac is a core NAC service. It allows enforcing authentication and authorisation policies over corporate networks. From the Management Console, an administrator can find and manage a user based on username, IP, MAC, network switch, or physical location (if a physical asset management system is integrated). Audit and reporting are available in order to review network activities.
- **onNETCONF:** The Network Configuration module allows to configure network devices from a comfortable web Graphical User Interface (GUI), based on templates that can-do bulk configuration of hundreds or thousands of devices or Based on stateful queue that allows programming when and how to push configurations. An API is available to extend functionality.
- **onNETBACKUP:** Automatically backup and archive network device configurations.
- **onNETDISCO:** Network Discovery module that allows to provision network devices automatically and maintain inventory.
- **onCMDB:** Network CMDB module that is the back-end for all information about inventory, allowing to share information with other platforms in an easy way.
- **onMON:** Network Monitor module: it allows monitoring network health and is the alarm administrator if some part of the network is not working properly. From CMDB, monitoring is auto provisioned.

3.12.6.2. Cisco ISE

Cisco Identity Service Engine (ISE) [69] is a solution that allows enterprises to gather real-time contextual information from networks, users, and devices. The administrator can use that information to make proactive governance decisions by tying identity to various network elements including access switches, Wireless LAN Controllers (WLCs), VPN gateways, and data centre switches.

Cisco ISE is software-based NAC that supports several features, including:

Centralised management: Helps administrators centrally configure and manage profiler, posture, guest, authentication, and authorisation services in a single web-based GUI console. Simplifies administration by providing integrated management services from a single pane of glass.

- **Business-policy enforcement:** Provides a rule-based, attribute-driven policy model for flexible and business-relevant access control policies. Provides the ability to create detailed policies by pulling attributes from predefined dictionaries.
- **Access control:** Provides a range of access control options, including Downloadable Access Control Lists (dACLs), VLAN assignments, URL redirections, named ACLs, and Security Groups (SGs) with Cisco TrustSec technology.
- **Secure supplicant-less network access with Easy Connect:** Provides the ability to swiftly roll out highly secure network access without configuring endpoints for 802.1X authentication. Derives authentication and authorisation from login information across application layers, allowing user access without requiring an 802.1X supplicant to exist on the endpoint.
- **Security group tag eXchange Protocol (SXP) support:** Uses SXP as a control protocol for propagating IP-to-Security Group Tags (SGTs) binding information across network devices that do not have the capability to tag packets with SGT. Allows security services on switches, routers, or firewalls to learn identity information from access devices.
- **Device profiling:** Ships with predefined device templates for many types of endpoints, such as IP phones, printers, IP cameras, smartphones, tablets, and more than 250 medical devices. Creates custom device templates to automatically detect, classify, and associate administration-defined identities when endpoints connect to the network. Associates endpoint-specific authorisation policies based on device type. Collects endpoint attribute data with passive network monitoring and telemetry.
- **Device administration access control and auditing:** Supports the Terminal Access Controller Access-Control System Plus (TACAS+) protocol. Grants users access based on credentials, group, location, and executable commands. Provides access to device configuration on a need-to-know and need-to-act basis while keeping audit trails for every change in the network.

- **Monitoring and troubleshooting:** Offers a built-in help desk web console for monitoring, reporting, and troubleshooting. Provides robust historical and real-time reporting for all services. Logs all activity and offers real-time dashboard metrics of all users and endpoints connecting to the network.

3.12.6.2.1. Forescout

Despite other companies, Forescout [105] focuses on NAC solutions, being a reference as a commercial solution available, Forescout CounterACT is the flagship product. CounterACT main capabilities are its wide visibility and detection without agents, but posture assessment and remediation capabilities are improved with their use. Authentication process is made through a captive portal when a new connection is established. Like competitors it offers layer 2 security with 802.1x protocol in order to validate credentials against back-end servers like RADIUS, Active Directory and LDAP. When authentication is made, user host is moved to a VLAN to grant resource access to authorised ones. With ACLs, filtering actions can be done and applied to network devices such as switches or firewalls. For evaluation purposes, if the agent is not installed, the check is made with a web browser add-on. Once is evaluated, a report is sent to CounterACT server deciding to grant or deny access. For remediation functionality, this solution can isolate the host to a quarantine VLAN. If an agent is deployed, remediation is done without the user interaction.

- **Agent-less Visibility:** Agent-less approach to device visibility. As physical or virtual solution, it lets you instantly identify devices with IP addresses, including network infrastructure, Bring-Your-Own-Device (BYOD) systems, non-traditional IoT devices (handhelds, sensors and machines) and rogue endpoints (unauthorised switches, routers and wireless Access Point (AP)s)—without requiring management agents or previous device knowledge.
- **Open interoperability:** Forescout includes a wide variety of integrations with network and IT infrastructure (switches, wireless controllers, VPN, routers, directories), endpoints (Windows®, Mac, Linux, iOS, Android, printers and other devices), and endpoint software (antivirus, instant messaging, Windows Management Interface (WMI) and more). These integrations give you tremendous power through visibility of your full network and let you take action on discovered security gaps.
- **Security orchestration:** Extended Modules expand the see and control capabilities of Forescout CounterACT®. The organisation can share contextual device data with third-party systems, automate policy enforcement across disparate solutions, bridge previously siloed IT processes, accelerate system-wide response and more rapidly mitigate risks. Here is an extract: Advanced Threat Detection, Enterprise Mobility Management, Endpoint Protection, IT Service Management, Next-Generation Firewall, Vulnerability assessment and a very interesting one, Open Integration Module for custom integrations.
- **802.1X authentication, or not:** 802.1X or other authentication technologies such as LDAP, Active Directory®, RADIUS®, Oracle® and Sun are supported. Hybrid mode lets you use multiple technologies concurrently.

3.12.6.2.2. Inverse PacketFence

Inverse [106] is a company founded in 1998 and is the author of an interesting NAC open source solutions: PacketFence. It is an open source (license) utility for NAC. Additionally, Inverse can provide commercial and technical assistance if it's required as an additional service for the configuration, RADIUS integration, Active Directory, etc.

Features

Being open source, this NAC tool is able to integrate in the same server other services as DHCP, FreeRADIUS, DNS, etc. The main features are:

- **Integration:** Open source solution with integration with other services and good community support.
- **Multiple configuration modes:** This server can be configured in two modes, inline and out-of-band. For inline mode is a must to have two network interfaces and for out-of-band three of them (using two for VLAN assignation).

- **802.1X Support:** Wireless and wired 802.1X is supported through a FreeRADIUS module which is included in PacketFence. PEAP-TLS, EAP-PEAP and many more Extensible Authentication Protocol (EAP) mechanisms can be used.
- **Wireless Integration:** PacketFence integrates perfectly with wireless networks through a FreeRADIUS module. This allows you to secure your wired and wireless networks the same way using the same user database and using the same captive portal, providing a consistent user experience. Mixing AP vendors and wireless controllers is supported.
- **Registration of Devices:** PacketFence supports an optional registration mechanism similar to "captive portal" solutions. Contrary to most captive portal solutions, PacketFence remembers users who previously registered and will automatically give them access without another authentication. Of course, this is configurable. An Acceptable Use Policy can be specified such that users cannot enable network access without first accepting it.
- **Detection of Abnormal Network Activities:** Abnormal network activities (computer virus, worms, spyware, traffic denied by establishment policy, etc..) can be detected using local and remote Snort, Suricata or commercial sensors. Content inspection is also possible with Suricata and can be combined with malware hash databases such as OPSWAT Metadefender. Beyond simple detection, PacketFence layers its own alerting and suppression mechanism on each alert type.
- **Isolation of Problematic Devices:** PacketFence supports several isolation techniques, including VLAN isolation with VoIP support (even in heterogeneous environments) for multiple switch vendors.
- **Command-line and Web-based Management:** Web-based and command-line interfaces for all management tasks. Web-based administration supports different permission-levels for users and authentication against LDAP or Microsoft AD.

3.12.7. Endpoint Detection and Response Systems (EDR)

EDR is an emergent approach (the term was coined in 2013) primarily focusing on detecting, investigating and mitigating attacks on endpoints terminals (as opposed to servers). It generally relies on light-agent technology, and scales to large enterprise system.

EDR stems from the consensus in security that endpoints are the main weakness of today systems. Because of the quickly evolving nature attacks (both malware-based or not), this issue is difficult to address beforehand. Detection & response is hence a needed solution. In order to do so, three technological challenges must be addressed:

- **Detection:** too many alerts overload security teams
- **Investigation:** lack of information (either historical or up-to-date) on endpoint states
- **Remediation:** first issue stemming from lacking investigation. Second from the lack of ability to quickly apply counter-measures on all concerned endpoints (scalability problem).

Thus, EDRs main innovation is about *smart visibility*, the capacity to have a broad yet selective understanding of the system state, both at current-time and through history.

As opposed to Endpoint Protection Platform (EPP), they do not focus on preventing a *priori* attacks by removing vulnerabilities (although most of the solutions in market also offer this capability), but in an a *posteriori* responding to attack, both at short-term (using quarantines and likes) and long-term (with forensics on the endpoint to perform root cause analysis). The latter is the most innovative one, involving capacities to remotely investigate the endpoints data state both at current-time and through history, and advanced visualisation techniques, and allowing experts to reduce forensic time from weeks to minutes or even seconds.

Most EDRs also allow designing complete workflows in after the first detection-investigation-remediation loop, allowing decreasing the further load for security teams.

3.12.7.1. Cynet 360

Cynet 360 [61] is a commercial threat detection and response platform that uses sensor fusion technology for enabling an autonomous breach protection platform. The system integrates automation of monitoring and

control, attack prevention and detection, and response orchestration across the entire IT environment of a company. The sensor fusion in Cynet 360 enables continuous collection and analysis of data across the IT environment, including user account activity and access, network traffic behaviour etc. Furthermore, the platform provides enterprise security by correlating indicators, thus increasing visibility and accuracy of detection, proactive discovery, monitoring and control of exposed attack surface in the entire environment. Once deployed, Cynet 360 platform begins analysing and correlating indicators across files, endpoints and user activities to issue risk rankings for potentially anomalous behaviour. The main capabilities supported by the platform include:

- **Endpoint Detection and Response (EDR):** Cynet 360 Advanced Threat Detection and Response platform provides visibility to endpoints, servers and networks to detect threats with near-zero false positives. By deploying continuous monitoring of endpoints for behavioural and interaction indicators, in-memory attacks and suspicious network communications, the platform applies threat intelligence feeds driven from IOC to predict adversary activities and give a complete picture of an attack operation.
- **User and Entity Behaviour Analytics:** this is another feature that combines other various Cynet 360 capabilities such as EDR, forensics, deception and more to provide comprehensive detection of insider threats, malicious users, and enable prioritisation of alerts across systems and initiative rapid response. The capabilities provided by this feature include quick detection of suspicious activities, identification of compromised devices and machines, verification for user identity and protection of networks and servers.

3.12.7.2. EnCase Endpoint Security

Guidance Software EnCase Endpoint Security [38] is an EDR platform with an emphasis on MMI and threat visualisation.

It can scale up to 100'000 nodes and provides agents for Windows, Linux and Mac OS X endpoints. Smartphones & tablets are explicitly supported.

Detection:

- Can detect similarities in code base between different types of malware, thus mitigating the ability of polymorphic/metamorphic code to be detected.
- Centralised storage of logs allows a quicker detection of security events.
- Schedulable scans against past threats.

Response:

- Use sets of heuristic to compute a “threat score”, thus reducing the operator burden and allow quicker response.
- After APT identification, a “snapshot” of the system is performed, and further evolution are recorded and displayed.
- Rich high-level visualisation allows fast analysis.
- Threat intelligence allows attacker profiling.
- Event history helps performing a root cause analysis.

3.12.7.3. TANIUM

Tanium Endpoint Platform [39] is a platform for EDR, with a strong emphasis on timing, scalability and analysis helping features. It claims to address any enterprise network in tightly bounded time (1 sec for queries and visualisation, 15 sec for actions/counter-measures) through a peer-to-peer communication pattern that allows scaling up to millions of endpoints. It provides agents running on Windows, Mac OS X or Linux in endpoints.

It provides the SOAP API for custom interaction and integrates a large number of third-party systems.

Discover:

- Network scan with millions of nodes;
- Unmanaged asset discovering and surveillance;
- Access network and system information as well as connection logs Integrity.

Monitor:

- Continuous monitoring of critical systems, applications and log files;
- File integrity monitoring;
- Schedulable scans.

Protect:

- Threat detection: through anomaly detection in behaviour and automated scan, search both types of malware and non-malware-based breaches;
- Enforcement: allows continuous and schedulable updates.

Threat Response:

- Continuous, proactive and real-time alerts from endpoints;
- Focus in answer speed, using a partially peer-to-peer communication pattern;
- Advanced visualisation and investigation tools, including “natural” query language;
- Support for current-time and historical data;
- Remote forensics investigation capabilities;
- Responses including process killing, file capture and quarantine, registry key repairing, update applications, connections shutdown, user management;
- Current-state and historical data display;
- Creating IOC on-the-fly.

3.12.7.4. CARBON BLACK Response

Carbon Black Response [40] is an EDR platform with emphasis on forensics. It is consistently cited by multiple sources as a reference for EDR. Potential users should be wary of links between the company executive board and the US securities agencies.

It provides an agent for endpoints running on windows, Mac OS X or Linux systems. It also scales up to 150000 endpoints by cluster, with an unlimited number of clusters.

Detection:

- Continuous recording of (critical) data, and their relationship/causality, can define customised thread detection;
- Use of event streams to detect new threats (by looking at evolution);
- The records are centralised in a single server or cloud-hosted;
- Alter filtering reduces the number of false positive or non-priority alerts.

Threat Response:

- Up-to-date threat intelligence (provided by a dedicated cloud) allows to perform attacker profiling;
- Automatic blocking of attacks;
- Protection: malware history (intrusion time and method, replication across the system, executions) can be followed and understood.

3.12.7.5. Symantec Endpoint Security

NortonLifeLock Inc. -formerly known as Symantec Corporation- is one of the leading companies which provide software security solutions and services. Among them, their Symantec Endpoint [115] is able to detect, isolate and eliminate cyber-intrusion attempts across all endpoints of an enterprise. It takes advantage of

Targeted Attack Analytics (TAA) to combine local and global telemetry, AI and threat intelligence techniques for a 24/7 threat hunting based on custom-made investigation flows. It also promotes the automated repetition of manual tasks without authoring complex scripts and encapsulates the streamlining of all core Security Operations Center (SOC) processes using a single only agent and console. Symantec's endpoint protection suite can be deployed either as a virtual or as a physical solution, offering the following features:

- Both legacy and next-generation antivirus (NGAV) with emulator capabilities for the efficient detection of hidden malicious activity and deception technologies, as well as the prevention of memory exploits and network intrusions
- Detection of advanced threats thanks to a predefined set of behavioural policies which are updated on a regular basis by Symantec itself
- Identification of compromised endpoints and application of rapid response by interlocking them on device, app and/or network level
- Provides integration capabilities with pre-existing security tools and APIs, assisting in this way the security experts to efficiently analyse cyber-attacks using on-premises or cloud-based sandboxes

The aforementioned characteristics stem from the combination of vendor's EPP and EDR products, where the overall response, management and ease-of-use have been found to be satisfactory enough, attributing Symantec's platform as a leading product in the endpoint protection market [119]. However, it is worth mentioning that there are a few additional features which come at great cost like the full-disk encryption, web content monitoring and threat intelligence feed integration, while on the other hand a rollback mechanism is not provided at all within their subscription plans.

3.12.7.6. CrowdStrike Falcon

CrowdStrike has developed an extensible cloud-based platform with a lightweight agent, capable of capturing and recording all endpoint activity of an enterprise [116]. The modular design of their product offers critical capabilities in the form of separate modules. Amongst them, NGAV protects the system against malware attacks, Integrated Threat Intelligence aims at detecting faster any malicious activities, and Managed Threat Hunting is deployed for proactive defence purposes. Their EDR module covers all features expected from a leading product in the EDR area, with its key benefits focus on the:

- Application of Behavioural analytics to detect suspicious activity and uncover stealthy threat-actors, followed by real-time remediation and response mechanisms capable of either isolating the infected endpoint, or running user-execution commands remotely
- Real-time historical visibility of the recorded security incidents regarding processes' creation, drivers' loading, system's registry modifications, disk and memory access control, as well as network activity
- Provision of several information collectors which monitor and gather information relevant with the file system, running processes, event logs etc.
- Display of threat graphs based on Big Data and AI techniques that assist security experts to analyse and remediate a threat faster and more efficiently than before

The prior mentioned real-time detection and response capabilities of the CrowdStrike platform nearly eliminate the possibility of silent failures, where its biggest advantage lies to its built-in scalability with the at-request addition of additional high-level monitoring and forensic capabilities. Despite the fact that it lacks the ability to filter web content and does not provide a VPN service, it still managed to be named a Leader in [118], gathering the highest possible score in 11 criteria of this extensive and well-grounded report.

3.12.7.7. SentinelOne

SentinelOne provides an autonomous AI platform capable of efficiently preventing, detecting and responding to cyber-security threats, which also incorporates a real-time endpoint protection approach [123]. It makes use of multiple patented AI algorithms to thwart not only known threats, but also unknown and emerging threats in the context of critical corporate assets. The application of such techniques differentiates with the traditionally used protection techniques since the latter have been periodically proved insufficient against the compromise of a system's endpoints. Therefore, SentinelOne operates on three distinct but interconnected

layers to protect against all possible threat vectors, namely the Pre-Execution, On-Execution, and Post-Execution, respectively. The Static AI engine is deployed on the first layer of the platform which is responsible for the pre-execution protection of the system. Then follows the On-Execution layer where a Behavioural AI engine tracks devices and processes, maps their interrelations and applies a set of dynamic policies for enhanced discovery and control. Finally, the Post-Execution layer of the EDR provides various automated response mechanisms along with a rich set of forensic data. The main features shipped with the SentinelOne are summarized below:

- Lightweight, real-time and high-performance holistic platform for any PC, Mac, Linux, or VDI
- Scalable and cloud-based solution with on-premises management capabilities, able to serve as a standalone platform or as an integrator for other EDR solutions
- Provides a deep file inspection mechanism and a strong protection against modern ransomware attacks
- Offers automated EDR features which include the automatic mitigation of threats, network isolation, and auto-immunization of endpoints to newly unknown threats

The automated response feature is maybe the one that makes SentinelOne to stand out compared to its competitors. This lies to the fact that small-sized organizations which do not possess an incident response team, or large-sized enterprises with limited background knowledge in the cyber-security domain, are able to efficiently deal with security incidents towards their endpoints without any human intervention. On the other hand, SentinelOne's main drawbacks include the lack of a couple of features found on other EDR platforms like the full-disk encryption, provision of VPN services, support of mobile devices, and its inability to whitelist applications or allow suspicious files' execution in a sandbox mode. However, Gartner and NSS Labs still distinguished it as an innovative product which managed to come out on top during the second round of MITRE's testing [122].

3.12.7.8. Cybereason

Cybereason's EDR [117] is a next generation layered endpoint security platform capable of protecting an organization's endpoints from ransomware attacks in real-time, as well as analysing and mitigating any security threat before causing harm to the system. Attack patterns and malicious activities are identified by an AI-based hunting engine which makes use of custom built-in memory graphs to inquire any endpoint directly, millions of times per second. The platform is delivered with a single agent and a suite of managed monitoring and detection services, especially designed to provide as complete as possible security awareness:

- Provides NGAV and cross-correlating data capabilities from different endpoints, which enable the timely identification of emerging threats with a high degree of accuracy, reducing many time-consuming and resourceful false positives
- Threat feed integration with third-party components like firewalls, SIEM tools, and other threat intelligence resources to prevent file less attacks and malicious encryption
- Threat remediation is feasible by either accessing remotely the platform's tools, or enabling its rapid automated detection and response mechanisms
- Visualization of attacks through a user dashboard which contains all the necessary information regarding a threat in detail, using rich analytics to view process trees and timelines for each network's endpoint

The deployment of Cybereason's EDR solution requires minimum effort from the personnel, it does not impact the organization's functionality and the detection of attacks takes place within 24 to 48 hours. Moreover, instead of manually authoring a monitoring rule for every endpoint of the infrastructure, an end-to-end context of attack campaigns is provided to identify any malicious attempts that could potentially compromise critical assets. Even though it is a relatively new product with an efficient centralized management approach for security incidents and a nice-to-have user interface, it scored quite well in the first round of MITRE ATT&CK® EVALUATIONS [120], standing out with the rest of platforms.

3.12.7.9. Kaspersky EDR

Kaspersky EDR [113] is a specialized, unified cybersecurity solution for the protection of enterprise infrastructures by providing endpoint detection and response capabilities to their SOC teams. It implements a

full endpoint protection cycle which includes deep visibility across all endpoints of a corporation, as well as automated routine tasks for prioritization, discovery and neutralization of advanced threats and future attacks. Its main features focus on the:

- Provision of a single but powerful agent with abnormal behaviour detection capabilities for the automated identification and protection against targeted attacks (e.g. evasive ransomware and file less threats)
- Deep analysis of any file on any endpoint in an isolated and safe sandbox environment, which lies exclusively within the organization’s in-house premises
- Dramatic reduction of the response time needed for a security incident, by utilizing evidence collection and telemetry analysis capabilities, as well as adapting the automation of its EDR and remediation processes

According to [114][121], Kaspersky EDR managed to provide 100% visibility across several attack techniques that covered a variety of situations, while at the same time demonstrated high-quality detection capabilities against Advanced Persistent Threat (APT) attacks. However, it is worth noticing that its detection methodologies (e.g. sandboxes, events’ correlation, AI and Deep Learning techniques) proved to be quite resource-intensive for the system, which resulted to a lower than average score during the second round of MITRE ATT&CK® EVALUATIONS. Finally, the lack of support for MAC or mobile devices, as well as the reported complexity of its user interface, may discourage some cybersecurity experts from choosing Kaspersky’s single agent solution.

3.12.8. Pros and Cons

After the previously presented solutions, we subjectively evaluated them based on personal experience and online information available, either from customer reviews or user manuals, the sources are too many to cite individually. And are mostly the ones already presented on the solution summary.

The approach to select the tools in each category, followed the reasoning of looking for the 1 or 2 commercial best in class for each category and a at least one opensource friendly solution (when available).

It’s hard to compare different solution from different categories under the same criteria, as such we don’t follow a specific rule book for the comparison, and they to depict the 3 most prominent positive facts and the 3 lest satisfying ones. Generally, we view a product being open source a very strong plus, since it favors transparency, openness and accountability. Not all is great, because in some cases being opensource limits the ability of a project to finance itself and threatens it’s longevity and up-to-date existence. Tools are evaluated on performance, scalability, feature set, price, ease of use and maintainability, these end up being the most prevelant criterias.

3.12.8.1. SIEM

Tool	Pros	Cons	License
Splunk	Easy Correlation Flexibility in data to be ingested Performance & Schema on Read flexibility	Requires additional license for Splunk Security Enterprise App Requires a team to manage large installations Expensive for large volumes	Commercial
Graylog	Scalability Cloud Integration Support Good performance	No correlation engine on the community edition Expensive on the Enterprise License Hard to do data retention properly	Community & Commercial

Tool	Pros	Cons	License
Elastic SIEM	Speed Powerful REST API Mostly OpenSource	Requires good infrastructure and resources to work well Correlations with third parties aren't easy to do Requires a lot of menial work to setup	Community & Enterprise
QRadar	Very good threat intelligence Feed Offer many correlations out of the box More than 400 built in sources types	Configuring log sources with unregular formats is hard to do Requires good infrastructure and resources to work well Can be expensive when large volumes are involved	Enterprise

Table 8: SIEM Pros and Cons

3.12.8.2. SOAR

Tool	Pros	Cons	License
Resolve	Easy to Use Follows NIST best practice recommendations Good auditing capabilities	Slow Performance Unpredictable at times Requires menial repetitive work when dealing with duplicates	Commercial
RTIR	OpenSource Built by people familiar with IR Requires few resources to run	Weak SOAR features, mostly focused on IR Old-school look and feel Doesn't run on windows	GPL2, Commercial support available
IBM Resilient	Easy to Use Great step of workflows and playbooks High level of automation	Customization can be hard to grasp Weak report scheduling Requires high-level tech skills to understand the details of the tool	Enterprise
Splunk Phantom	Flexibility to integrate with 3rd parties Good Documentation Good IAM controls	Support level was reported to be subpar before the Splunk acquisition Full integration with Splunk Enterprise Security APP hasn't happened yet Pricey for high number of daily actions	Enterprise

Table 9: SOAR Pros and Cons

3.12.8.3. Forensics

Tool	Pros	Cons	License
EnCase	User Friendly Good Reporting Won best forensics tool prize 10 years in a row!	Very Expensive Slow to process large mailboxes Weak on mobile	Enterprise
Sleuth Kit / Autopsy	Flexibility to integrate with 3rd parties Open Source User Friendly	Weaker features compared to EnCase and FTK Weak on mobile extractions Can be hard to setup properly when the disc raw images are encrypted	OpenSource
FTK	User Friendly FTK Imager is free (Image acquisition) Good auditing capabilities	Weak extensibility Slow on big volumes Timeline is lacking	Free & Commercial
ProDiscover	Forensics focused IR instead of criminal investigation File previews Heuristic Searches	Less well known than direct alternatives UX is lacking compared to alternatives Lack of focus, trying to be good and IR and Forensics at the same time	Commercial

Table 10: Forensics Pros and Cons

3.12.8.4. NBADS

Tool	Pros	Cons	License
Anodot	Real time support Responsive Dashboards Good forecast abilities	Complex to master Requires time to configure in a way that can avoid being overwhelmed by false positives Flaky ETL refreshes	Commercial
WEKA	Strong integration features Powerful GUI Good support for multiple ML techniques	Can't handle large datasets well Slow performance Generic tool, not focused on NBADS	OpenSource
SciKit	Flexibility and ease of use Excellent Documentation Multiple models publicly available	Generic tool, not focused on NBADS Slow performance Scalability	OpenSource

Tool	Pros	Cons	License
TensorFlow	Excellent performance Good documentation Excellent development GUI	Generic tool, not focused on NBADS Data ingestion can be hard Error messages are difficult or impossible for non-programmers	OpenSource
Keras	Good set of ML techniques out of the box Good Documentation Excellent API	Generic tool, not focused on NBADS Only a wrapper, can't easily change the backend Errors are impossible to deal with for the non-experts	OpenSource

Table 11: NBADS Pros and Cons

3.12.8.5. Honey Pots

Tool	Pros	Cons	License
Conpot	Well-designed API Supports HoneyNet Project Industrial Grade	Few support protocols Inconsistent Maintainability Unfrequently updated project	GPL2
Dionaea	Supports fail2ban and HoneyNet project Several protocols supported	Inconsistent Maintainability Unfrequently updated project	GPL
Cowrie	High interaction SSH + Telnet Frequently updated Well maintained	Dependent on third parties to support continuous development (like GSOC) Poor defaults Easily detected by attackers	OpenSource
SHIVA	Supports HoneyNet Project Support Email protocol	Unmaintained project Not really production ready	OpenSource
RDPy	MiMT RDP HoneyPot Supports VNC and RDP session recording Multiple OSs supported	Limited feature set and capabilities Poor architecture	OpenSource
Glastopf	Web HoneyPot with meta features Support HoneyNet Project Extensibility	Poorly updated Easy to detect Not widely used	OpenSource

Table 12: Honey Pots Pros and Cons

3.12.8.6. NAC

Tool	Pros	Cons	License
OpenNAC	Support AAA policies OpenSource Easy to extend	Does not track bandwidth utilization Not broadly supported by vendors Lackluster documentation	OpenSource
Cisco ISE	Best in class Good integration with existing Radius Servers & commercial vendors Good device profiling	Can be expensive Required deep expertise to setup Complex to operate	Commercial
Forescout	Very good device visibility and profiling Good integration with patch management Good Guest support	Thick client UI feels dated Configuration is complex Aesthetics are lacking	Commercial
Inverse	Good community Good posture analysis Good feature set and 3rd party integration	Configurations can be complex Hard to master	OpenSource with optional Commercial Support

Table 13: NAC Pros and Cons

3.12.8.7. EDR

Tool	Pros	Cons	License
EnCase Endpoint	User Friendly Good Reporting Streamlined Forensics with EDR	Performance can be slow at times Memory based learning curve Features can be found without previous experience	Commercial
Tanium	Good visibility and discovery Multi OS Support Stability	3rd party integrations Mobile devices aren't supported Historical reports lacking	Commercial
Carbon Black	Low resource usage Good value / price ratio Good feature set	Can be chatty on the network Mobile devices aren't supported Can be tough to automate deployment	Commercial
SEP	Best in class AV detection Reduced false positive ratio Easy to setup and deploy	Resource usage can be an issue with systems with databases installed Significant impact on the machine performance Is known to have issues with other	Commercial

D2.1 – Cyber Incident Handling Trend Analysis

Tool	Pros	Cons	License
		software running on the same machine	
CrowdStrike Falcon	Good dashboards Good detection rates Good Ransomware protection	Lack of OnDemand scanning Host management is lacking Can be pricey	Commercial
SentinelOne	Very good neighbour (works well with others) Low resource consumption Good threat detection	Deep analysis can be hard Lacking dashboards Auto update features of client apps	Commercial
Cybereason	Good dashboards Good and detailed timelines Good threat hunting capabilities	Discovery mode can be hard on existing systems Support can be slow to respond Threat detection is subpar compared to other tools	Commercial
Kaspersky EDR	Very good thread detection Good behavioural Analytics Good threat intelligence	Mobile is lacking support Being from Russian based company, trust is an issue High resource consumption	Commercial
Cynet360	Easy to setup and deploy Easy to learn Good and easy to use GUI	Too many false positive Week log correlation capabilities Lack/Weak AI/ML capabilities	OpenSource

Table 14: EDR Pros and Cons

4. Standards, guidelines and best practices

In this section, we want to give a short overview on existing standards and guidelines for prevention, detection, response and mitigation of threats, which might be interesting/applicable in the CyberSANE project. We identified the following standards and reference documents:

- NIST SP800-61 Computer Security Incident Handling Guide;
- ISO / IEC 27035:2016+ — Information technology — Security techniques — Information security incident management;
- More available in [41].

4.1. Security Management Standards

CyberSANE should be applicable worldwide and thus will have to comply with various privacy and cybersecurity standards. This section gives an overview of standards from ISO/IEC, European Committee for Standardisation (CEN)/CENELEC and NIST that are relevant to the CyberSANE topic.

4.1.1. International overview

4.1.1.1. The standard ISO 27000

ISO / IEC 27000 is the family of international standards that define the requirements for setting up and managing the Management System of Information Security. It provides good practice recommendations on Information Security Management Systems (ISMS). The series of ISO / IEC 27000 is broad in scope and can be used by organisations of all types and sizes. The latest version of the standard is the ISO / IEC 27001:2017 [70], which replaces the 2013 version and comprises more than fifty standards. In the sections that follow, an overview of the ISO / IEC 27001:2017 is given, which is aimed at providing a better understanding of the role of the standards in CyberSANE in conforming to legal requirements, best practice and globally accepted security principles. Hence, the group of ISO 27000, valid today, can be grouped into the following areas:

Terminology

ISO / IEC 27009 [71] – “IT - Security techniques - ISMS - Overview and vocabulary”. It provides guidance and defines requirements for the use of ISO / IEC 27001 in any specific sector, field or application area.

General Requirements

ISO / IEC 27001 – “ISMS – Requirements” is the normative document to which an organisation that wishes to be certified must refer. It describes the necessary steps needed for managing information security in an organisation. It consists of 10 clauses and more than 110 security controls grouped into 14 different sections. The standard primarily provides guidance to help organisations define, implement, operate, control and improve information security based on a risk management approach.

ISO / IEC 27006 – “IT - Security techniques - Requirements for bodies providing audit and certification of information security management systems” is the gold standard for certification bodies [72]. ISO / IEC 27006 is mostly designed for organisations that provide ISMS certification by supporting them to meet the requirements contained within ISO / IEC 27001 and ISO / IEC 17021 [73].

General Guidelines

ISO / IEC 27002 – “IT - Security techniques - Code of practice for information security management” [74] provides guidance not prescriptive to protect the information assets of a company. It provides recommendations for ensuring information security against risks to the confidentiality, integrity and availability of information. Also, the guidelines in ISO / IEC 27002 focus on ensuring the security of all forms of IT systems, networks, including data, and intellectual property. The standard is tailored to the specific information risks and needs of any organisation, irrespective of size or type and offers recommendations on standard security practices that enable an organisation to meet audit, regulatory and legal requirements.

Therefore, by adopting ISO / IEC 27002, an organisation can be able to assess its information risks, define control objectives and apply appropriate controls (e.g. asset management, compliance, operations security, communications security etc.)

ISO / IEC 27003 – “IT - Security techniques – ISMS” [75] provides guidelines for the implementation of a management system of information security in accordance with ISO 27001. The goal of this standard focuses on the crucial aspects needed for the successful design and implementation of ISMS within an organisation. In particular, it guides the process of obtaining management approval to implement ISMS, defining ISMS project from planning, inception and design and final implementation phases. Mostly, ISMS’ comprise a set of activities for the management of information security risks by which an organisation identifies, analyses and addresses risks. ISMS ensures that an organisation’s security processes are fine-tuned to address the ever-dynamic security threats and vulnerabilities.

ISO / IEC 27004 – “IT - Security techniques - Information security management – Measurement” [76] provides the procedures and examples of construction for defining and measuring the effectiveness of the Management System for Information Security adopted by the organisation and related controls of Annex A. In other words, the standard intends to help organisations evaluate the effectiveness and efficiency of ISMS, and where necessary, systematically improve the overall ISMS. Hence, it provides pragmatic guidance on the development and use of specific measures and measurement that can be used to assess the effectiveness of implemented ISMS.

ISO / IEC 27005 – “IT - Security techniques - Information security risk management” [77] focuses on security risk management. This standard, in the 2011 version, has been aligned with ISO / IEC 31000 "Risk management - Principles and guidelines" [78]. It is designed to support the suitable implementation of a risk management-based approach to information security. Specifically, it provides guidance on the necessary steps needed for a sufficient assessment of business risks, particularly the risk inherent to information security that could compromise the assets of an organisation. Even though this standard does not recommend a specific risk management methodology, it does, however, recommend a structured sequence of activities that establish the risk management context (e.g. the scope and an organisation’s risk tolerance), risk identification and analysis (e.g. incident scenarios and predicted business consequences), risk treatment (using information security controls, risk sharing and avoidance), the responsibilities of stakeholders for risk management activities, and lastly, the monitoring and review of risks and treatment plans on continuous basis.

ISO / IEC 27007 – “IT - Security techniques - Guidelines for information security management systems auditing” [79] is a guideline for Certification Bodies (CBs) accredited for internal auditors, external auditors / third parties to verify compliance with the requirements of a Management System for Information Security. The standard focuses on the specific aspects of a compliance audit of ISMS, and in particular, provides guidance on managing ISMS audit programme (in terms of determining what to audit, delegating auditors, managing audit risks and maintaining audit records), performing an ISMS audit (e.g. planning, fieldwork, analysis and reporting), and managing auditors (such as auditor competencies and skills). It could, therefore, be said that the standard is tailored specifically to support organisations needing to conduct internal or external audits or to manage an ISMS audit programme.

ISO / IEC Technical Report (TR) 27008 – “IT - Security techniques - Guidelines for auditors on information security controls” [80] supports the planning and execution of ISMS audits adding further value by closing the gap between the system and the revision, if necessary, implementing verification tests of the controls provided from Annex A of ISO / IEC 27001. Although not intended for ISMS audits, it provides guidance to organisations on how to review and assess the implementation and operation of security controls in order to provide the assurance that controls are effective and efficient or to identify the need for changes.

Specific Guidelines for Industry

ISO / IEC 27010 – “IT - Security techniques - Information security management for inter-sector and inter-organisational communications” [81]. ISO / IEC 27010 primarily focuses on the information exchange and sharing regarding the maintenance and protection of an organisation’s CI. It aims at providing general guiding principles for communicating and information sharing about security incidents, threats, vulnerabilities and controls, between organisations in the same or different sectors to protect CI, meet legal, regulatory or

contractual agreements. In addition, it provides the basis and guidance on methods, models, policies, processes, protocols, and controls, for the sharing of information securely with trusted counterparties under all circumstances

ISO / IEC 27011 – “IT - Security techniques - Information security management guidelines for telecommunications Organisations based on ISO / IEC 27002” [82]. This standard provides a set of telecommunications sector-specific security controls that must be met by any organisation within telecommunications sector for ensuring the confidentiality, integrity and availability of telecommunications facilities, services, including information handled, processed or stored by the facilities and services. The standard also establishes general principles for implementing, maintaining and improving information security controls.

ISO / IEC 27013 – “IT - Security techniques - Guidance on the integrated implementation of ISO / IEC 27001 and ISO / IEC 20000-1” [83]. The standard helps organisations to develop a better understanding of the characteristics, similarities and differences of ISO / IEC 27001 and ISO / IEC 2000. It provides guidance on the processes and documentation required for the implementation of an integrated management system. It proposes a set of recommendations by which organisations can follow to plan, organise and prioritise activities on the implementation of integrated information security and IT service management systems based on ISO / IEC 27001:2005 (ISMS) and ISO / IEC 20000-1:2011.

ISO / IEC 27014 – “IT - Security techniques - Governance of information security” [84]. The standard “provides guidance on principles and processes for the governance of information security, by which organisations can evaluate, direct and monitor the management of information security”. It provides a structure by which the objectives of an organisation are set, the means of attaining those objectives, and how performance monitoring can be achieved. In general, the standard assists organisations to make informed and timely decisions about information security issues in support of its strategic objectives by aligning security objectives with business strategy, effective investment decisions on information security, ensuring transparency on information security status, as well as achieving compliance with regulatory, contractual and legal requirements.

ISO / IEC TR 27015 – “Information technology - Security techniques - Information security management guidelines for financial services” [85]. The standard provides “information security guidance complementing and in addition to information security controls defined in ISO / IEC 27002:2005 for initiating, implementing, maintaining, and improving information security within organisations providing financial services”.

ISO / IEC 27031 – “IT - Security techniques - Guidelines for information and communication technology readiness for business continuity” [86]. The standard focuses on resilience and recovery for business continuity. Essentially, it specifies crucial aspects for ensuring business continuity by identifying the relevant design, performance measurements and implementation of techniques to efficiently enhance an organisation’s readiness to survive a disaster. By considering various aspects of incidents and events likely to affect the operations of an organisation or impact IT systems and infrastructure, the standard extends guidance on the practices of information security incident handling and management.

ISO / IEC 27032 – “IT - Security techniques - Guidelines for cybersecurity” [87]. The standard consists of two focal areas. The first part deals with control measures for addressing cybersecurity issues associated with the Internet, with a particular focus on providing technical guidance for addressing common cybersecurity risks such as social engineering, hacking and malicious software. The standard also provides recommendations with regards to the crucial measures for addressing these risks, including preparing, detecting and monitoring, and responding to attacks. The second area of the standard provides a framework for efficient and effective information sharing, collaboration, coordination and incident handling amongst organisations. It includes key elements for establishing digital trust and processes for information interchange.

ISO / IEC 27033-1 – “IT - Security techniques - Network security - Part 1: Overview and concepts” [88]. In essence, the standard provides the fundamental description and overview of the concepts and principles that underpin the remaining parts of ISO / IEC 27033 series. It focuses mainly on the provision of detailed guidance regarding “the security aspects of the management, operation and use of information system networks, and their interconnections.” It aims to support network security architects, designers, and managers with guidance

for ensuring the protection and security management of networked devices, network applications, services and end-users.

ISO / IEC 27033-2 – “IT - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security.” This standard focuses on the planning, designing, implementing and document network security. It complements *ISO / IEC 27033-1* by “providing guidelines for organisations to plan, design, implement and document network security.” It also provides detailed technical recommendations to organisations on how to achieve network security using a consistent approach to the planning, design and implementation of network security relevant to their business environments.

ISO / IEC 27033-3 – “IT - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues.” In addition to the preceding *ISO / IEC 27033* series, this standard elaborates the “threats, design techniques and control issues associated with typical network scenarios.” It provides detailed guidance on implementing *ISO / IEC 27002* network security controls, including the security of information being transmitted through communication networks. It also provides guidance on security threats, design techniques and the necessary controls needed to control the associated risks. Moreover, the critical element of the standard is to provide a comprehensive definition and implementation of an organisation’s network environment by supporting the review of technical security design options, documentation of preferred security architecture and related controls.

ISO / IEC 27034-1 – “IT - Security techniques - Application security - Part 1: Overview and concepts.” [88] This is another multi-part standard consisting of six documents. Guidance for application security is the focal scope of this standard. It is made to support organisations that deal with mission-critical software in terms of specifying, designing, selecting and implementing information security controls throughout an organisation’s Systems Development Life Cycle (SDLC). Specifically, the standard assists organisations to easily integrate concepts, principles, components and processes for ensuring security throughout the life cycle of in-house developed applications. Also, it provides guidance on how security requirements should be adequately addressed and managed constantly by defining and analysing security considerations at every stage of an application’s life cycle.

ISO / IEC 27035 – “IT - Security techniques - Information security incident management.” [89] *ISO / IEC 27035* is another crucial standard that focuses on information security incident management. It aims to complement other ISO standards that guide the investigation of, and preparation to investigate security incidents. The also provides a basic definition of concepts and phases for information security incident management, including a structured guideline for planning and preparing incident management activities such as detecting, reporting, assessing and responding to incidents. The guidelines consist of phases for planning and preparing security incident management policies, security policies, establishing incident response team, incident management awareness training, and incident management plan testing.

ISO / IEC 27036-3 – “IT - Security techniques - Information security for supplier relationships - Part 3: Guidelines for information and communication technology Supply Chain Security (SCSs).” [90] The standard focuses on managing the information security risks caused by today’s complex ITC SCs. It provides the guideline to reduce or manage information security risks associated with acquiring and supplying ITC products and services. The defines the “business case for ICT SCSs, specific risks and relationship types as well as how to develop an organisational capability to manage information security aspects and incorporate a lifecycle approach to managing risks supported by specific controls and practices.” In particular, the guidance in this standard, centres around areas such as ITC outsourcing, transparency on managing the information security risks of multi-layered ICT SCs, and compliance obligations in relation to acquiring ICT-related products.

ISO / IEC 27037 – “IT - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence” [91]. The *ISO / IEC 27037* standard provides “guidelines for identification, collection, acquisition and preservation of digital evidence”. Fundamentally, it provides guidance on specific activities in the handling of digital evidence of potential digital forensic evidence that can be of evidential value i.e. “digital data that may be of value for use in court”. The principal aim of this standard is to promote good practise methods and processes for a forensic investigation of digital evidence. It provides guidelines that

assist organisations in the exchange of potential digital evidence between jurisdictions, and in general, incident handling process.

ISO / IEC 27042 - “Guidelines for the analysis and interpretation of digital evidence” [92]. ISO / IEC 27042 aims at promoting “good practise methods and processes for forensic capture and investigation of digital evidence.” It provides detailed guidance to individuals responsible for handling digital evidence (such as incident response specialists and forensics examiners) with a specific set of activities for the identification, collection, acquisition and preservation of potential digital evidence. These activities are requisite in an investigation for ensuring the integrity of the digital evidence that will contribute to its admissibility in legal and disciplinary actions. Additionally, the standard provides “general guidelines for the collection of non-digital evidence that may be helpful in the analysis stage of the potential digital evidence”.

ISO 27799 – “Health informatics - Information security management in health using ISO / IEC 27002” [93]. Deals with information security management and information security controls in the healthcare industry. The standard provides detailed guidance on how best to protect the confidentiality, integrity and availability of personal health data for anyone working in the health sector or its unique operating environments. Additionally, it “gives guidelines for organisational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organisation's information security risk environment.”

4.1.1.2. NIST Special Publication

National Institute of Standards and Technology, Joint Task Force Transformation Initiative (NIST JTFTI) is an interagency working group in the United States that works towards producing a Unified Information Security Framework for the federal government. NIST has partnered with various agencies to develop and maintain an extensive collection of standards, guidelines, recommendations, and research on the security and privacy of information and information system. “It also focuses our security initiatives to operate effectively in the face of changing threats and vulnerabilities. The unified framework standardises the information security process that will also produce significant cost savings through standardised risk management policies, procedures, technologies, tools and techniques.” Recommended security controls for federal information systems and organisations (NIST Special Publication (SP) 800-53, revision 3). The major NIST guidelines and standards relevant for CyberSANE are provided.

NIST SP 800-61 Revision 1 - “Computer Security Incident Handling Guide” [94] is an incident response guideline that aims at providing practical guidance to organisations for effective and efficient response to cybersecurity incidents. The guideline comprises detailed recommendations for establishing an incident response program with a particular focus on the structure of an incident response team, the necessary steps for performing incident handling (such as incident detection and analysis), and incident response coordination and information sharing.

NIST SP Version 1.1 - Framework for Improving CI. This publication is developed to help organisations have a common language and shared understanding of the ever-evolving cybersecurity threats landscape, and managing and expressing cybersecurity risks (threats, vulnerabilities, and impacts) to both internal and external stakeholders. It also supports organisations to identify and prioritise a customised set of controls for reducing cybersecurity risks by aligning policy, business and technological approaches to managing risks. The framework focuses on the CI within an organisation; however, it can be used to manage cybersecurity risks across entire organisations. Also, the framework consists of five core functions for addressing and managing dynamic cybersecurity risks in critical infrastructure, which include identification, protection, detection, response, and recovery.

NIST SP 800-30 Rev. 1 - “Guide for Conducting Risk Assessments” [95]. This publication provides guidance on the essential steps for conducting risk assessment process such as preparation, conducting the assessment, communication assessment results, and maintaining the assessment. It also guides determining appropriate courses of action in response to identified risks, as well as identifying specific risk factors that are continuously monitored so that an organisation can decide if risks have exceeded organisational risk tolerance and the different courses of actions that should be taken. Generally, the guideline articulates the fundamental concepts

associated with assessing security risks within an organisation and an overview of the risk management process.

NIST SP 800-39 - “Managing Information Security Risk” [96]. The purpose of this publication is to provide guidance for an integrated program for managing information security risks across all levels of organisational operations including reputation, mission, functions, assets, and individuals. It aims to provide complementary enterprise risk management program that supports existing risk-related activities or programs of organisations by providing a structured and flexible approach for managing risks with specific details of assessing, responding to, and monitoring risks continuously.

NIST SP 800-64, Revision 2 - “Security Considerations in the SDLC.” The purpose of this publication is to provide guidelines to assist organisations in incorporating security into the IT systems development process for ensuring a more cost-effective, risk-appropriate security control. It describes the key security roles and responsibilities needed in the development of information systems, as well as the basic understanding of the relationship that exists between information security and SDLC. Overall, the guidance focuses on the security aspects of SDLC.

NIST SP 800-82 - “Guide to ICS Security.” This publication focuses on providing guidance for ensuring the protection and security of systems that perform control functions such as ICS, SCADA systems, and Distributed Control Systems (DCS). It elaborates the typical overview of ICS, identifies the common threats and vulnerabilities to these systems, and provides different methods, techniques and recommendation for mitigating the associated risks and security ICS.

NIST SP 800-83 - “Guide to Malware Incident Prevention and Handling” [97]. This publication aims to support organisations to build an understanding of the threat posed by malware, including the necessary control actions for mitigating the risks associated with malware incidents. It defines and compares the various categories of malware, malware incident response processes, and practical strategies for detecting, containment, eradication of malware, in addition to responding to malware incidents.

NIST SP 800-53 Revision 4 - “Security and Privacy Controls for Federal Information Systems and Organisations” [98]. This version of NIST Publication provides guidelines for specifying necessary security controls for information systems that process, store or transmit sensitive information. The guidelines aim to provide recommendations for secure information systems by facilitating a consistent approach for selecting and specifying security controls, providing a flexible catalogue of security controls to meet current information protection needs, and a foundation for the development of assessment methods for determining the effectiveness of security controls. The publication also establishes the relationship between privacy and security controls for purposes of enforcing respective privacy and security requirements which often overlap in concept and implementation within systems, programs and organisations.

NIST SP 800-66 - “Guide to Integrating Forensic Techniques into Incident Response” [99]. This publication provides practical guidance for investigating computer security incidents and performing computer and network forensics. In particular, the publication offers a set of processes and activities for performing practical forensics (such as data collection, examination, analysis and reporting), including advice about different data sources (such as files, operating systems, network traffic and applications).

NIST SP 800-150 - “Guide to Cyber Threat Information Sharing” [100]. This publication intends to provide guidance to organisations on gathering, exchange, and sharing information on cyber threats to CI. It addresses the process for sharing of cyber threat information within an organisation, for using cyber threat information received from external sources, as well as for producing threat information that can be shared with other organisations. The publication provides the basic concepts of threat information sharing, the benefits of sharing, challenges associated with sharing capabilities, including important considerations for active participation and sharing relationship between organisations.

NIST SP-184 - “Guide for Cybersecurity Event Recovery” [101]. The purpose of this publication is to support organisations in improving their cyber event recovery plans, processes, and procedures to resume normal operations in times of a disaster. The publication aims to extend existing NIST guidelines regarding incident response by providing more detailed and actionable information guidelines on planning, preparing and

recovering from a cyber event, achieving continuous improvement of recovery capabilities as well as integrating these processes into an organisation’s risk management plan.

4.1.2. European Committee for Standardisation (CEN)

A number of Standards issued by the ISO are currently under approval by CEN. Examples are the following of the work programme “CEN / SS F12 - Information Processing Systems”:

- *Daft European Standard for formal vote (FprEN) ISO / IEC 27037 - “IT - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO / IEC 27037:2012)”*
- *FprEN ISO / IEC 27038 - “IT - Security techniques - Specification for digital redaction (ISO / IEC 27038:2014)”*
- *FprEN ISO / IEC 27040 - “IT - Security techniques - Storage security (ISO / IEC 27040:2015)”*
- *FprEN ISO / IEC 27041 - “IT - Security techniques - Guidance on assuring suitability and adequacy of the incident investigative method (ISO / IEC 27041:2015)”*
- *FprEN ISO / IEC 27042 - “IT - Security techniques - Guidelines for the analysis and interpretation of digital evidence (ISO / IEC 27042:2015)”*
- *FprEN ISO / IEC 27043 - “IT - Security techniques - Incident investigation principles and processes (ISO / IEC 27043:2015)”*
- *FprEN ISO / IEC 30121 - “IT - Governance of digital forensic risk framework (ISO / IEC 30121:2015)”*
- The CEN project committee on SCSs published two standards:
 - *CEN / TR 16412:2012 - “SCSs - Good practice guide for small and medium sized operators”*
 - *EN 16352:2013 - “Logistics - Specifications for reporting crime incident”*
- The CEN / Technical Committee (TC) 417 Project Committee “Maritime and port security services” issued the European Standard (EN) 16747:2015 on “Maritime and port security services”.

4.1.2.1. European Telecommunications Standard Institute (ETSI)

The European Telecommunications Standards Institute (ETSI) is a European Union-recognised standard institute that develops several globally-applicable standards for ICT. It produces specifications, standards, reports and guides, each with its own purpose. In particular, ETSI has published an extensive series of cybersecurity specifications, called ETSI TC CYBER that are designed to improve the cybersecurity landscape, especially the protection of IoT, the internet, security communications and for providing security tools for businesses, while others are awaiting approval. Some of the relevant specifications already published ETSI and ETSI TC CYBER are considered under this section.

ETSI Group Specification (GS) Information Security Indicators (ISI) 008 V1.1.1 (2018-06) - “ISI; Description of an Overall Organisation-wide SIEM Approach.” This version of ETSI specification defines and describes the various concepts and areas for developing SIEM. The specification describes the approaches to real-time monitoring of security events, management of residual risks associated with security events, enforcement of security policies, investigation of security events, as well as planning for security.

ETSI EN 303 645 V2.0.0 (2019-11) – “CYBER; Cyber Security for Consumer IoT” provides high-level guidance and specifications for the security of consumer IoT products connected to network infrastructure, including associated services and personal data such as smart cameras, TVs, wearable health trackers, smart home assistants etc. Although the specification is developed primarily to help protect consumer devices, other consumers of IoT can equally benefit from the specification, such as manufacturing, healthcare and other industrial applications.

ETSI GS ISI 007 V1.1.1 (2018-12) - “ISI; Guidelines for building and operating a secured SOC.” This specification covers the concept of incident detection services from both internal and external points of view. The requirements in this specification are implemented at two different levels of compliance, i.e. partial compliance and full compliance.

ETSI GS ISI 002 V1.2.1 (2015-11) - “ISI; Event Model A security event classification model and taxonomy.” In this specification, a comprehensive security event classification model and associated taxonomy are

provided. It covers both security incident and vulnerabilities. It is designed to support operational security staff and general stakeholders effectively to categorise detected security events using a common language.

ETSI GS ISI 003 V1.2.1 (2018-01) - “ISI; Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection.” This is the subsequent specification of ETSI GS ISI 002 V1.2.1 (2015-11) that aims to describe a set of KPSI that can be used for the evaluation of the performance and maturity levels of event detection, tools and processes used by an organisation. In particular, the specification enables organisations to assess the overall maturity level of security event detection.

ETSI TR 103 644 V1.1.1 (2019-12) - “CYBER; Increasing Smart Meter Security.” This specification provides crucial specifications for increasing the security of Smart Meters. It provides an overview of the Security Monitoring Framework architecture, including threat detection and countermeasures, design aspects and privacy by design concept for Smart Meters.

ETSI TR 103 331 V1.2.1 (2019-09) - “CYBER; Structured Threat Information Sharing” In this specification, an overview of the means for sharing and exchanging cyber threat information in a standardised and structured manner are covered. Threat information includes technical indicators of threat actors or adversary activity, exploitation targets and courses of action.

ETSI TR 103 305-5 V1.1.1 (2018-09) - “CYBER; CSC for Effective Cyber Defence; Part 5: Privacy Enhancement”

ETSI TR 103 303 V1.1.1 (2016-04) - “CYBER; Protection measures for ICT in the context of CI.” This document reviews specifications for the protection of CI for which loss or damage in whole or in part will lead to a significant negative impact on one or more of the economic activities of the stakeholders, the safety, security or health of the population. The specification also defines the relevant mechanisms, measures and processes for Critical Infrastructure Protection (CIP) where the CI in whole or in part is composed of ICT technologies using Cyber-Security.

4.1.2.2. European General Data Protection Regulation (GDPR)

The GDPR is a privacy and security legal framework that sets guidelines for the collection and processing of personal information from individuals within the European Union. The fundamental objectives are to standardise data protection law across all EU member countries by imposing rules on controlling and processing personally identifiable information. GDPR provides various Chapters consisting of Articles that enumerate the general regulations, principles, and standard contractual clauses for controllers and processors of personal data to ensure appropriate technical and organisational measures are put in place for the collection, handling and transfer of personal data.

Chapter 1 (Art. 2) - “Subject-matter and Objectives.” Provides basic regulation rules for the processing of personal data by wholly or partly automated means, and “to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.”

Chapter 1 (Art. 3) - “Territorial Scope.” “Provides regulations for an organisation that collects or process personal data in the EU, “regardless of whether the processing takes place in the EU or not”. It also applies to organisations in or outside the EU who process personal data of residents of the EU, mainly where the processing activities are related to the offering of goods or services and the monitoring of their behaviour as far as the behaviour takes place within the EU.

Chapter 1 (Art. 4) - “Definitions”. This article defines an array of legal at length for a consistent understanding of terminology within the regulation. The article provides a clear definition for terms such as “personal data”, “processing”, “restriction of processing”, “consent”, “personal data breach”, “data concerning health”, “corporate rules”, “cross border rules”, etc.

Chapter 2 (Art. 5) - “Principles Relating to Processing of Personal Data.” This article lays out the basic principles by which data shall be: processed lawfully, fairly and in a transparent manner; collected for specific, explicit and legitimate purposes and not further processed in a way that goes against those purposes; limited

to what is necessary about the purposes for which data is processed; accurately processed, and where appropriate, kept up to date; and processed in a way that ensures appropriate security of the personal data.

Chapter 3 (Art. 13) - “Information to be provided where personal data are collected from the data subject.” This article specifies that where personal data relating to an EU resident are collected, an organisation shall provide the resident with information such as the identity and contact details of the organisation, purposes of processing the personal data, and recipients of the personal data.

Chapter 3 (Art. 15) - “Right of access by the data subject.” The EU residents for which data is collected shall have the right to obtain from an organisation confirmation as to whether or not personal data concerning him or her are being processed, access to the personal data, and the purposes of the processing.

Chapter 4 (Art. 24) - “Responsibility of the controller.” This rule specifies the obligations of an organisation to take into account the scope and purposes of processing personal data of and as well as the varying likelihood and severity of risks to personal data. It also specifies the obligation of an organisation to ensure the implementation of appropriate technical and organisational control measures, including the implementation of appropriate data protection policies for the protection of personal data in their custody.

Chapter 5 (Art. 28) - “Processor.” In this article, obligations of an organisation that to use only third-party-providers (processors), where the processing of personal data is carried out by a third-party, in providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR regulations and ensure the protection of the rights of the data subject.

Chapter 5 (Art. 32) - “Security of Processing.” This regulation specifies the responsibilities of an organisation to implement appropriate technical and organisational measures to ensure a level of security commensurate with the cost of implementation, the nature, scope, context and purposes of the processing, as well as the risk of the varying likelihood of personal data.

4.1.3. Cyber Security-related standards Compliance

4.1.3.1. Compliance Domains

We studied and analysed the capabilities and functions of a set of existing security-related approaches which have been logically grouped in eight domains [42]. Each of the eight domains contains a structured set of cybersecurity objectives that represents the activities required for establishing and ensuring increased capability in the domain. A brief description of the eight domains is presented in Table 15.

Domains	Description	Domain Objectives
Risk Management	Establish, operate and maintain a cybersecurity risk management program to identify, analyse, and mitigate cybersecurity risks to the organisation taking into consideration the related interconnected infrastructures, and stakeholders.	Establishment of a Cybersecurity Risk Management Strategy
		Management of the Cybersecurity Risks
		Management of the Risk-related activities
Asset, Change, and Configuration Management	Identify and manage all cyber assets which are necessary in the provision of the supported business processes and needed to be protected commensurate with the risk and impact resulting from various threats	Asset Inventory Management
		Asset Security Configuration
		Asset Changes Management
		Asset Management Activities
Threat and Vulnerability Management	Identify, analyse, manage, and respond to cybersecurity threats and vulnerabilities commensurate with the risk to the involved ICT infrastructure and organisational objectives.	Threat Management
		Vulnerability Management
		Threat and Vulnerability Management Activities
Situational Awareness	Collect, analyse, correlate, and use cybersecurity security and risk related information, including	Establishment and Maintenance of an appropriate Security Picture

Domains	Description	Domain Objectives
	information retrieved from online repositories, to form the security state of the cyber assets.	Situational Awareness Management Activities
Information Sharing and Communications	Establish and maintain relationships with internal and external entities which will reveal their commitment to identify all of their organisations' cyber assets, the controls they have undertaken and provide cybersecurity information, including threats and vulnerabilities	Cybersecurity Information Sharing
		Cybersecurity Information Sharing Management Activities
Event and Incident Response, Continuity of Operations	Establish and maintain plans, procedures, and technologies to detect, analyse, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organisational objectives.	Detection of Cybersecurity Events
		Escalation of Cybersecurity Events and Declaration of Incidents
		Response to Incidents and Escalated Cybersecurity Events
		Planning for Continuity
Supply Chain and External Dependencies Management	Identify, analyse, and mitigate the cybersecurity risks associated with assets that are dependent on other entities, commensurate with the risk to the involved ICT infrastructure and organisational objectives.	Dependencies Identification
		Dependency Risk Management
		Dependency Risk Management Activities
Cybersecurity Program Management	Establish and maintain an enterprise cybersecurity program that is aligned with the identified risk to the examined infrastructure.	Establishment of a Cyber-Security Strategy Program

Table 15: Cyber-Security Standards Compliance Domains

4.1.3.2. Mapping of Cybersecurity Standards to Domains

In this Section, we will illustrate the conceptual linkage between the examined cybersecurity standards and the security domains as defined in the previous section. In particular, Table 16 provides a mapping of the examined cybersecurity standards to the eight domains [43, 44, 45, 46].

According to the analysis, a plethora of cyber-security methodologies, methods, initiatives and standards exist that provide a framework for assisting the organisations to identify, evaluate and respond to cyber-risks and threats. In particular, about one-third of the approaches cover most of the steps/phases of a complete risk management process. These steps concern the risk assessment process focusing on the evaluation of the security level and the prioritisation of actions establishing priorities for risk assessments, in order to identify where risk reduction is more compelling and then to determine protective measures that need to be taken.

Additionally, as has been noted, the CIIs comprise a variety of heterogeneous assets (ranging from computing centres to SCADA systems), which feature complex relationships among them. The latter relationships are not standardised and therefore poorly captured within relevant (state-of-the-art) risk assessment and incident management methodologies. In particular, only one-fifth of the approaches are able to identify the corporate assets developing an inventory and to capture the complexity of infrastructure interconnections and the dependencies with other systems or infrastructures within a sector or across sectors.

Regarding Threat and Vulnerability Management, most of the existing solutions are very generic, failing to provide targeted technical solutions that address cyber-related threats e.g. interdependent threats rising from associated entities, sector-specific threats. About one-third of the approaches provide an insight for the security management of the corporate ICT systems revealing and assessing vulnerabilities and threats (including SCADA, Industrial Automation and Control Systems (IACS) or SC related) that exist in the IT infrastructure.

D2.1 – Cyber Incident Handling Trend Analysis

Domains	Risk Management	Asset, Change, and Configuration Management	Threat and Vulnerability Management	Situational Awareness	Information Sharing and Communications	Event and Incident Response, Continuity of Operations	Supply Chain and External Dependencies Management	Cybersecurity Program Management	Reference
Cybersecurity Standards									
ISO 27001:2013 Information Technology – Security techniques – Information security management systems requirements		●	●	●	●	●		●	
ISO 27002:2005 Information technology – Security techniques – Code of practice for information security management		●	●	●	●	●		●	
ISO 27005:2011 International Organization for Standardization. (2011). Information security risk management	●							●	
ISO/IEC 21827:2008 International Organization for Standardization. (2008). Systems Security Engineering – Capability Maturity Model (SSE-CMM)			●		●			●	
ISO 28001:2007 International Organization for Standardization. (n.d.). Security management systems for the supply chain - Best practices for implementing supply chain security assessments and plans							●	●	
Security considerations in the information system development life cycle. [NIST Security Considerations in SDLC]	●							●	
Information security training requirements: A role- and performance-based model [NIST SP800-16]								●	
Guide for applying the risk management framework to federal information systems [NIST SP800-37]	●			●	●		●	●	
Creating a patch management and vulnerability management program [NIST SP800-40]			●			●			
Recommended security controls for federal information systems and organizations [NIST SP800-53]	●	●	●		●	●		●	
Computer security incident handling guide [NIST SP800-61]						●		●	
Security considerations in the system development life cycle [NIST SP800-64]			●			●		●	
Stouffer, K., Falco, J., & Scarfone, K. (2011). <i>Guide to industrial control systems (ICS) security</i> (NIST Special Publication 800-82). National Institute of Standards and Technology. ³						●			
Mell, P., Kent, K., & Nusbaum, J. (2005). <i>Guide to malware incident prevention and handling</i> (NIST Special Publication 800-83). National Institute of Standards and Technology. ⁴						●			
Guide for security-focused configuration management of information systems [NIST SP800-128]		●						●	
Information security continuous monitoring (ISCM) for federal information systems and organizations [NIST SP800-137]				●	●		●	●	
National vulnerability database. [NIST NVD]			●	●	●	●			
Piloting supply chain risk management for federal information systems [NISTIR 7622]							●	●	
Guidelines for smart grid cyber security: Vol. 1, smart grid cyber security strategy, architecture, and high-level requirements [NISTIR 7628]	●	●						●	
Guidelines for smart grid cyber security: Vol. 3, Supportive analyses and references [NISTIR 7628]			●		●			●	
Organisation for Economic Co-operation and Development [OECD Reducing Systemic Cybersecurity Risk]				●			●		
Key practices of the capability maturity model [SEI CMM]								●	
Generic SCADA risk management framework for Australian critical infrastructure. [SCADA AU RMF]	●							●	
[Situation Awareness in Dynamic Systems] Endsley, M. (1995). Toward a theory of situation awareness in dynamic systems. <i>Human Factors</i> , pp. 32-64				●	●			●	
Supply chain risk management awareness. Armed Forces Communication and Electronics Association Cyber Committee. [Supply Chain Risk Management Awareness]	●			●			●	●	
Department of Homeland Security. (2012, May). Industrial Control Systems Cyber Emergency Response Team4.		●				●			
Forum of Incident Response and Security Teams (FIRST). (2012). CSIRT case classification (Example for ...)				●	●	●			
International Society of Automation (ISA). (2009). Industrial automation and control systems security: Establishing an industrial automation and control systems security program (ANSI/ISA-99.02.01-2009)				●	●	●			
National Council of Information Sharing and Analysis Centres (ISACs). (2012) 6				●	●	●			
GS ISG ISI Series (Information security indicators, security event management)						●			

Table 16: Mapping of Cyber-Security Standards to Security Domains

D2.1 – Cyber Incident Handling Trend Analysis

Situational awareness is covered by several approaches. About one-third of the approaches is able to build situational awareness among organisations to enhance their insight into their infrastructures and provides them with capability to react in case of security risks and threats. These approaches provide precise controls or/and define frameworks that improves the detection and analysis of cyber-attacks and threats on the organisations as well as on their SCs and increase the knowledge on the current cyber threat landscape.

In modern day organisation infrastructures, there are no boundaries on sources of data. Data can originate not only from internal corporate systems, but also from interconnected infrastructures. Therefore, there is a need to deal with information sharing in a holistic manner as the awareness of the SC as a system is distributed across the interconnected SC entities. Thus, regarding Information Sharing and Communications, more than one-third of the approaches support and facilitate swift and effective cooperation among the SCs’ entities in terms of exchanging specific cyber-security incidents information and sharing information about risks and threats. In this context, these solutions provide the ability to strengthen and streamline the cyber-security cooperation in the SC.

Regarding the SC and External Dependencies Management, nearly one quarter of the approaches consider the whole overall SC picture and are able to identify and evaluate risks and threats as well as their various cascading effects that are associated with security events occurring from interacting entities.

Finally, most of the approaches implement a Cyber-Security Program that include the deployment of specific protection measures while only a limited number of the applications apply the stage of measuring effectiveness establishing indicators to provide information on achieving specific security goals.

4.2. Mapping of CyberSANE Solutions to Domains

In this section, we provide the mapping between the CyberSANE Solutions described in Section 3 and the security domains as defined in Section 4.1.3. The aim is to develop a better understanding of the domains implemented by CyberSANE to achieve effective security management and incident handling by overcoming various challenges. In the following table, we map the Solutions with the identified security domains (see Table 17).

CyberSANE Component	CyberSANE Solutions	Risk Management	Asset, Change, and Configuration Management	Threat and Vulnerability Management	Situational Awareness	Information Sharing and Communications	Event and Incident Response, Continuity of Operations	Supply Chain and External Dependencies Management	Cybersecurity Program Management
LiveNet	eMAS SOM		X				X		
	SiVi Tool						X		
	Live Anomaly Detection System (L-ADS)						X		
DarkNet	MEDUSA Cyber Intelligence suite			X	X				
HybridNet	XL-SIEM				X		X		
	Centre of Log Analysis and Mining of Events (CARMEN)				X		X		

CyberSANE Component	CyberSANE Solutions	Risk Management	Asset, Change, and Configuration Management	Threat and Vulnerability Management	Situational Awareness	Information Sharing and Communications	Event and Incident Response, Continuity of Operations	Supply Chain and External Dependencies Management	Cybersecurity Program Management
	Metadon SIEM				X		X		
	Smart Profiling Application (SPA)				X				
	OLISTIC Enterprise Risk Management Suite	X	X	X	X			X	
	Evidence-driven Maritime Supply Chain Risk Assessment (MITIGATE) System	X	X	X	X			X	
PrivacyNet	CHIMERA					X			

Table 17: CyberSANE Solutions to Domains

4.3. Open issues, and future challenges in Critical Information Infrastructure Protection

The CPIs becomes more complex every year with the evolution and adaptation of new technological advancements. New technologies and services also mean the rise of new threats against the CIs and the CIA triad [47], Confidentiality, Integrity, Availability. Thus, creating the need for continuous research of the new challenges that arise, open issues that haven’t be resolved and all the research efforts in the area of CI protection. Figure 18 depicts various types of cyberattacks against CIs, along with information about the attack and its impact.

Before moving forward, we need to pay extra attention to “cascading effects” that are closely related to CIs, homeland security and protection. The term is used to reference the breakdown or failure of infrastructure systems/networks that result in subsequent breakdowns or failures of additional infrastructure systems/networks due to the dependencies between them. However, a number of other terms or labels have been used in place of “cascading effects” throughout the research with potentially different implications. In order to correctly describe cascading effects a Disaster Spreading in Networks need to be constructed, to identify the series of elements that characterise the Spreading conditions such as network topologies, dependencies, system parameters and the optimal recovery strategies. A series of elements that could mark the spreading disasters are the following as described by D. Helbing et al. [49]: Causal dependencies (directed), Initial event (internal, external), Redistribution of loads, Delays in propagation, Capacities of nodes (robustness), Cascade of failures. A more complete study of CIs and the Cascading effects was performed in the context of CIPSEC project [50, 51].

There are a number of open issues that affect the security of CIs. The main issue and ongoing challenge is the transformation of the CI paradigm from a closed system, built on top of proprietary protocols and applications, to a more open, interconnected platform, that potentially provides ICT based services to end users or other CIs. Additionally, all these new and inter-connected technologies are being coupled together with legacy systems that were built to work in isolation. This vigorous adaptation of new technologies and systems greatly broadens

D2.1 – Cyber Incident Handling Trend Analysis

the attack surface against a traditional CI. Taking into account the type of services and the criticality of these infrastructure, renders them a high value targets for the attackers' community.

Attack	Consequence	Instigation	Attack type	Impact	Severity
Ransomware attacks on SCADA systems	Locked PLCs, spread of a ransomware	Vulnerable PLCs, weak authentication, weak integrity control	External	Financial loss	High
Attacks on industrial robots	Auto-execution of malicious node, altered robot firmware	Vulnerable OS and web interface, weak authentication	External	Sabotaged throughput, safety threat, financial loss	High
FDI Attacks on real-time market model and state estimation systems	Fabricated data, profit gain from selling and purchasing of virtual power	Vulnerable AMI and sensor network	External	Disrupted smart grid operations, profit loss	High
Remote attacks on IoT-enabled traffic control systems	Eavesdropping, remotely controlled traffic lights	No encryption and authentication mechanisms	Internal	DoS attack causing road accidents, loss of credibility	High
Remote attacks on mission-critical systems on a ship	Mission-critical systems on acquired ship, compromised navigation system	Weak authentication, weak web interfaces, no network segmentation	External	Human injuries, financial loss	High
Attack on e-health infrastructure	Compromised hospital medical devices	Vulnerable PMDs and web interface, weak authentication	External	Loss of credibility, threat to human lives	High
Phishing attacks on a container port systems and devices	Compromised devices	Outdated OS, vulnerable network protocols, no network isolation, weak authentication mechanism	External	Loss of credibility, threat to human lives	High
Spear-phishing attack on smart grid	Credential stealth, control over SCADA system	Vulnerable OS, weak authentication, no network isolation	External	Power outage, disrupted services, loss of credibility	High
Worm attack on SCADA systems	Self-replication, exploited access privileges	No network isolation	Internal	Compromised infrastructure, decreased efficiency	Medium
Attacks on SCADA honeypots	Modified device functionality, pump shut down	Weak security policies, vulnerable servers	External	Loss of functionality, disrupted production, device damage, loss of credibility	High

Figure 18: Types of Cyber Attacks on CI. Image source [48]

One of the typical instances of CI is ICS, which are in charge of controlling and monitoring services within industrial infrastructures starting from the water treatment systems and electrical distribution up to oil and gas refineries and nuclear power plants. A great part of ICS relies on SCADA that allows sending commands from the control centre to remote substations by using either the Ethernet or Internet connection.

Main challenges of ICS security caused by three factors [52]: i). *Isolated system assumption*, ii). *Increased connectivity* and iii). *Heterogeneity of the system*. Thus, from the cybersecurity perspective, currently the most important issues of ICS systems and approaches are:

- *input data validation*: allows ensuring that the input data is not used by an attacker in gaining access privileges. However, almost no ICS are able to perform this operation;
- *insecure access*: access to ICS provides through simple access control with a combination of password/username or even without any authorisation. Moreover, access is not controlled continuously, i.e., it is not possible to automatically control any ongoing operations before their actual execution;
- *quality of the code*: a review of the code might help to indicate that the software for ICSs was designed or integrated without following secure concepts. However, usually, an organisation's capabilities limit this operation;
- *sensitive data protection*: communication protocols contain unprotected sensitive data. Thus, an attacker can easily obtain this information and use it for performing an attack;
- *insufficient network security*: many ICS networks contain firewalls with weak rules. Moreover, ICS LAN might be not routed through firewalls.

The trend of “security by obscurity” was dominant in most, if not all, ICS applications since their initial design. The focus was on designing reliable, effective and personnel safe systems, whereas information security was not great importance. This is because the systems were supposed to be isolated from the outside world, and therefore, considered secure. For example, in ICS and power grids, before they became “smart”, security relied on the assumption that systems are isolated from the outside world, and the monitoring, as well as control operations, was performing locally. In fact, most of attacks on ICS have been internal until 2001; after that, most of the attacks originate from external (Internet-based) sources. This is clearly due to the increased connectivity deployed in ICS. Moreover, ICS are multivendor systems that combine multiple products and each of them has its own security vulnerabilities. Thus, different entities can manufacture and implement a single component that is eventually can be integrated by another organisation. Hence, components of ICS are more integrated and such integration invites the inherent vulnerabilities of each product. For example, one of the steps in the Stuxnet attack was exploiting of the default password in Siemens Programmable Logic Controllers (PLC) to access a computer running a Windows OS [53]. There is a constant rise in the research efforts of security and evaluation of ICS / SCADA CI systems, focusing on the modernisation and rising

interconnection of these systems [48, 54]. In CyberSANE we will keep on staying in sync with the research efforts and advancing the state of the art in the area of the CI security.

The first priority topic of the “CI Security and Resilience Stakeholder Workshop”, of the National Technology Security Coalition (NSTC) was the growth of complex interdependencies [55] within CI systems. This interdependency and the interconnection with other CIs provides the potential of Cascading Effects exceeding the borders of a single CI. This remains as an open issue and constitutes a future challenge of identifying and modelling interdependencies and the residual cascading effects. Moreover, the risk of a cyber-attack is continuously on the rise, thus all future security efforts for CIs need invest into research for detection, prevention and mitigation of CI threats as well as promoting automation to the security systems, with better understanding of “human in the loop” concept.

Another challenge, that can be perceived as an open security issue, is the adaptation of emerging technologies and new materials, developed prominently by the private sector. Some paradigms include new materials for improving life-cycle issues. IoT-based sensing technologies could allow for continuous system monitoring and more precise inspection, imposing new threats to the CIs as most IoT systems are not secure by design and just recently security by design concept [56] has been introduced. Moving on to the future, big data analysis and fast simulation will provide insights on the CI’s status and longevity. Other next-generation technologies may also include AI, use of autonomous robotics, 3-D printing materials and more. The report from the white house [55] suggests that all strategies and standards need to be reevaluated for the integration of the new technologies and materials in the existing CI paradigm.

An additional challenge is the rapid cyber threat information sharing between CIs, states, governments and industry that allow CIs to respond to real-world challenged and crises, in a swift and coordinated way. International cooperation can be proved helpful, as common incidents, response practised and mitigation experiences can greatly improve the response time against a major cyber incident. Moreover, public-private collaborations foster the creation of large cyber-threat datasets, that require processing employing big-data techniques and automated algorithms, incorporating diverse datasets. The whole process of the datasets creation the propagation and storing of the threat information should be protected from data alterations ensuring data integrity at all levels. Finally, the whole process should include humans in the loop providing a visual digest of the most important cyber threat information integrated into an information dashboard.

Needs for cyber threat information sharing and professional personnel training [57] were demonstrated during attacks of the Ukrainian power grid as well as the financial sector in 2015 [48] and 2017 respectively. Intruders used a banal spear-phishing technique as an initial step during the attack on the power grid. The corporate network was compromised by the BlackEnergy malware that was attached to the personal email of personnel who used corporate PC to access the mailbox. Therefore, sharing information about the latest cyber-attacks, threats and recently discovered vulnerabilities, is an important aspect of achieving strong defence capabilities. However, due to the critically confidential data (e.g., system description, tools used to detect an attack, existing vulnerabilities, etc..) that cyber threat information might include, organisations usually do not share it since it can cause additional financial and reputational losses. However, due to the critically confidential data (e.g., system description, tools used to detect an attack, existing vulnerabilities) that cyber threat information might include, organisations usually do not share it since it can cause additional financial and reputational losses. At the same time, the analytical capabilities of an organisation can be limited due to the financial and/or intellectual factors. Therefore, sharing system-related information (e.g., Indicators of Compromise, installed software description) and its analysis by external platforms (e.g., Collaborative and Confidential Information Sharing and Analysis for Cyber Protection (C3ISP)) becomes highly important in identifying possible threats to the organisation’s assets. Hence, the challenging task is to not only motivate organisations to exchange cyber threat information through relatively secure and automated communication technology but also implement new and improve existing technologies for data exchange and analysis that also suffer from imperfections of integrated security mechanisms, e.g., weak encryption, insecure communication channels, sensitive data anonymisation and continuous data usage control.

5. Conclusion

In this deliverable, we have provided a categorisation of inventoried attacks that could occur on a Critical Information Infrastructure. We have described the lists of existing partner tools and how we could use them in the framework of CyberSANE to secure efficiently CII against these attacks. We focused on these tools for CyberSANE since they are the ones we master and the ones where we have control over the licensing, feature set and availability. They are also the ones we wrote about on the DOA.

But our tools alone don't cover the full spectre of categories, and commercial tools of reference are presented as a way to gauge how the competitive market is faring, in the analysed categories, and what strengths can be gained by learning from them, and what weaknesses can be avoided by understanding their shortcomings. It's also important to understand what each external tool offers in terms of integration, so we can aim to make CyberSANE core as compatible with existing previously deployed solutions. For each tool, we have presented strengths and limitations and for the ones owned by the consortium partners how they could apply to the envisioned framework of CyberSANE. The security incident handling market is very broad and large, as such it was impractical to test and compare all the tools and all categories. So, our focus was on tools related to incident handling and incident analysis, or tools that enable them to be more efficient.

From our analysis of the 3rd party landscape we can conclude that generally opensource tools are not competitive in terms of maintainability and support levels, unless they are backed by a company that provides professional services with them. We can make the case that Elastic SIEM or Packet Fence which are both very big players in their niche, as noteworthy champions of opensource quality. Sadly, on other subjects such as honeypots the general maturity level is very low, some of them are not even usable in production environment for anything serious. On the commercial side, tools have generally good support and are kept updated with frequent releases. Price can be a big issue for large deployments, and from a public funding perspective they are constrained do to licensing issues. As such their main relevance is as third parties that some organizations might already have, and as such API for interconnection should be the main focus to ensure ease of interoperability.

Finally, we have revised the different standards and highlighted the important points to follow and respect in the following of the project, detailing the usual best practices.

This Deliverable will serve as a basis reference document to the other WP of the project since it gathers main information useful for the project and general instructions to follow all along the deployment of the CyberSANE infrastructure.

In this deliverable, we have provided a categorisation of inventoried attacks that could occur on a Critical Information Infrastructure. We have described the lists of existing partner tools and how we could use them in the framework of CyberSANE to secure efficiently CII against these attacks. We focused on these tools for CyberSANE since they are the ones we master and the ones where we have control over the licensing, feature set and availability. They are also the ones we wrote about on the DOA.

But our tools alone don't cover the full spectre of categories, and commercial tools of reference are presented as a way to gauge how the competitive market is faring, in the analysed categories, and what strengths can be gained by learning from them, and what weaknesses can be avoided by understanding their shortcomings. It's also important to understand what each external tool offers in terms of integration, so we can aim to make CyberSANE core as compatible with existing previously deployed solutions. For each tool, we have presented strengths and limitations and for the ones owned by the consortium partners how they could apply to the envisioned framework of CyberSANE. The security incident handling market is very broad and large, as such it was impractical to test and compare all the tools and all categories. So, our focus was on tools related to incident handling and incident analysis, or tools that enable them to be more efficient.

From our analysis of the 3rd party landscape we can conclude that generally opensource tools are not competitive in terms of maintainability and support levels, unless they are backed by a company that provides professional services with them. We can make the case that Elastic SIEM or Packet Fence which are both very

D2.1 – Cyber Incident Handling Trend Analysis

big players in their niche, as noteworthy champions of opensource quality. Sadly, on other subjects such as honeypots the general maturity level is very low, some of them are not even usable in production environment for anything serious. On the commercial side, tools have generally good support and are kept updated with frequent releases. Price can be a big issue for large deployments, and from a public funding perspective they are constrained do to licensing issues. As such their main relevance is as third parties that some organizations might already have, and as such API for interconnection should be the main focus to ensure ease of interoperability.

Finally, we have revised the different standards and highlighted the important points to follow and respect in the following of the project, detailing the usual best practices.

This Deliverable will serve as a basis reference document to the other WP of the project since it gathers main information useful for the project and general instructions to follow all along the deployment of the CyberSANE infrastructure.

6. List of Abbreviations

Abbreviation	Translation
ACL	Access Control Lists
ADS	Anomaly Detection System
AI	Artificial Intelligence
AIDS	Anomaly-based Intrusion Detection Service
AIRS	Automated Intrusion Response System
AP	Access Point
API	Advanced Programming Interface
APT	Advanced Persistent Threats
BYOD	Bring-Your-Own-Device
C3ISP	Collaborative and Confidential Information Sharing and Analysis for Cyber Protection
CB	Certification Body
CEN	European Committee for Standardisation
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIP	Critical Infrastructure Protection
CIS	Centre for Internet Security
CMDB	Configuration Management DataBase
CPE	Common Platform Enumeration
CPS	Cyber-Physical System
CRL	Cumulative Risk Level
CSC	Critical Security Controls
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
dACL	Downloadable Access Control Systems
DBSCAN	Density-Based Spatial Clustering of Applications with Noise
DCS	Distributed Control Systems
DoS	Denial of Service
DPA	Data Protection Act

D2.1 – Cyber Incident Handling Trend Analysis

EAP	Extensible Authentication Protocol
EDR	Endpoint Detection and Response
EM	Expectation -- Maximisation
EMD	Earth Mover's Distance
EN	European Standard
EPP	Endpoint Protection Platform
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
FprEN	Draft European Standard for formal vote
FTK	Forensic Toolkit
GDPR	General Data Protection Regulation
GS	Group Specification
GUI	Graphical User Interface
HIDS	Host-based Intrusion Detection Service
HPA	Host Protected Area
HR	Human Resources
IACS	Industrial Automation and Control Systems
IAM	Identity and Access Management
ICS	Industrial Control Systems
ICT	Information Communication Technologies
IDS	Intrusion Detection Service
IEC	International Electrotechnical Commission
IOC	Indicator of Compromise
IoT	Internet of Things
IPC	Inter-Process Communication
IR	Incident Response
IRL	Individual Risk Level
IRP	Incident Response Platform
ISE	Identity Service Engine
ISI	Information Security Indicators
ISMS	Information Security Management Systems

D2.1 – Cyber Incident Handling Trend Analysis

ISO	International Organisation for Standardisation
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KNN	K-Nearest Neighbour
KPSI	Key Performance Security Indicators
L-ADS	Live Anomaly Detection System
LDA	Latent Dirichlet Allocation Algorithm
MAD	Multivariate Correlation Analysis
MCA	Multivariate Correlation Analysis
MitM	Man-in-the-Middle
MQL	Metadon Query Language
MTTC	Mean-Time-To-Contain
MTTD	Mean-Time-To-Detect
NAC	Network Access Control
NCC	Nonlinear Correlation Coefficient
NER	Named Entity Recognition
NIDS	Network-based Intrusion Detection Service
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
NIST JTFTI	National Institute of Standards and Technology, Joint task Force Transformation Initiative
NLP	Natural Language Processing
NSRL	National Software Reference Library
NSTC	National Technology Security Coalition
OCR	Optical Character Recognition
OSI	Open Systems Interconnection model
OT	Operational Technology
OVVL	Open Weakness and Vulnerability Modeler
PCA	Principal Component Analysis
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PLC	Programmable Logic Controllers

D2.1 – Cyber Incident Handling Trend Analysis

PRL	Propagated Risk Level
RDP	Remote Desktop Protocol
RDPy	Remote Desktop Protocol honeypot
SaaS	Software as a Service
SAP	Systems, Applications and Products for data processing
SC	Supply Chain
SCADA	Supervisor Control and Data Acquisition
SCS	Supply Chain Service
SCSs	Supply Chain Security
SDLC	Systems Development Life Cycle
SEB-SIC	Supervised IEarning-Based Secure Information Classification
SEM	Security Event Management
SG	Security Group
SGT	Security Group Tag
SIDS	Signature-based Intrusion Detection Service
SIEM	Security Information and Event Management
SIM	Security Information Management
SLA	Service Level Agreement
SOC	Security Operations Centre
SOM	Security Operations Manager
SP	Special Publication
SPA	Smart profiling Application
SSO	Single Sign-On
SVM	Support Vector Machine
SXP	Security group tag eXchange Protocol
TACAS+	Terminal Access Controller Access-control System Plus
TC	Technical Committee
TMT	Microsoft Threat Modelling Tool
TR	Technical Report
UEBA	User and Entity Behaviour Analysis
VLAN	Virtual Lan

D2.1 – Cyber Incident Handling Trend Analysis

VPN	Virtual Private Network
WLC	Wireless LAN Controller
WMI	Windows Management Interface

7. References

- [1] A. Gupta and R. K. Jha. Security threats of wireless networks: A survey. In Proceedings of International Conference on Computing, Communication Automation, pages 389–395, May 2015.
- [2] J. Singh, S. Kaur, Gu. Kaur, and Go. Kaur. A detailed survey and classification of commonly recurring cyber attacks. In International Journal of Computer Applications (0975 – 8887) Volume 141 – No.10, May, 2016.
- [3] G. Elbez, H. B. Keller, and V. Hagenmeyer. A new classification of attacks against the cyber-physical security of smart grids. In Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018, pages 63:1–63:6.
- [4] K. Chelli. Security issues in wireless sensor networks: Attacks and countermeasures. In Proceedings of the World Congress on Engineering, volume 1, 2015.
- [5] F. Shahzad, M. Pasha, and A. Ahmad. A survey of active attacks on wireless sensor networks and their countermeasures. CoRR, 2017.
- [6] S. Karchowdhury and M. Sen. Survey on attacks on wireless body area network. In International Journal of Computational Intelligence & IoT, Forthcoming, pages 638–644, Mar. 2019.
- [7] N. H. Ab Rahman and K.-K. R. Choo. A survey of information security incident handling in the cloud. In Computers & Security, 49:45–69, 2015.
- [8] T. Wu, J. Ferdinand P. Disso, K. Jones, and A. Campos. Towards a SCADA forensics architecture. In 1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013) 1, pages 12–21, 2013.
- [9] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman. Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity, 2:20, 2019.
- [10] A. Ibor, F. Oladeji, and O. Okunoye. A survey of cyber security approaches for attack detection, prediction, and prevention. International Journal of Security and its Applications, 12:15–28, 07 2018.
- [11] M. Ahmed, A. N. Mahmood, and J. Hu. A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60:19–31, 2016.
- [12] N. Ben-Asher and C. Gonzalez. Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48:51–61, 2015.
- [13] IT Governance UK. Cyber security risk management. <https://www.itgovernance.co.uk/cyber-security-risk-management>, 2019. Accessed: 2020-02-05.
- [14] IT Governance UK. Cyber security risk assessment. <https://www.itgovernance.co.uk/cyber-security-risk-assessments>, 2013. Accessed: 2020-02-05.
- [15] P. Radanliev, D. Charles De Roure, J. R.C. Nurse, P. Burnap, E. Anthi, A. Uchenna, L. Maddox, O. Santos, and R. Mantilla Montalvo. Cyber risk management for the internet of things. In Preprints 2019, 2019.
- [16] M.-E. Paté-Cornell, M. Kuypers, M. Smith, and P. Keller. Cyber risk management for critical infrastructure: A risk analysis model and three case studies. Risk Analysis, 38(2):226–241, 2018.
- [17] H. Ögüt, S. Raghunathan, and N. Menon. Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. Risk Analysis, 31(3):497–512, 2011.
- [18] K. Gai, M. Qiu, and S. A. Elnagdy. Security-aware information classifications using supervised learning for cloud-based cyber risk management in financial big data. In 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High

- Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), pages 197–202, Apr. 2016.
- [19] S. Papastergiou and N. Polemi. Mitigate: A dynamic supply chain cyber risk assessment methodology. In *Smart Trends in Systems, Security and Sustainability*, pages 1–9. Springer, 2018.
- [20] E. M. Kalogeraki, D. Polemi, S. Papastergiou, and T. Panayiotopoulos. Modeling SCADA Attacks. In: Yang XS., Nagar A., Joshi A. (eds) *Smart Trends in Systems, Security and Sustainability*. Lecture Notes in Networks and Systems, vol 18. Springer, Singapore, pages 47–55. 01 2018.
- [21] S. Papastergiou and D. Polemi. Securing maritime logistics and supply chain: The medusa and mitigate approaches. *Marit. Interdiction Oper. J.*, 14:42–48, 2017.
- [22] Elastic NV. Elasticsearch website. <https://www.elastic.co/>, 2010. Accessed: 2020-02-06.
- [23] Splunk Inc. Splunk website. <https://www.splunk.com/>, 2003. Accessed: 2020-02-06.
- [24] Graylog. Graylog website. <https://www.graylog.org>, 2009. Accessed: 2020-02-11.
- [25] IBM. IBM Qradar SIEM data sheet. https://www.insight.com/content/dam/insight-web/en_US/pdfs/ibm/ibm-qradar-siem-datasheet.pdf, 2018. Accessed: 2020-02-11.
- [26] Y. Dunchych, P. Bahrs, K. Birkler, B. Eberhardt, N. Goyal, J. Hunter, D. Jennings, J. Kaczmarek, M. Laaroussi, M. Love, et al. IBM Software for SAP Solutions. IBM Redbooks, 2015.
- [27] Anodot. Anodot website. <https://www.anodot.com/>, 2014. Accessed: 2020-02-11.
- [28] Anodot. Getting started with anodot. <https://s3.amazonaws.com/anodot-documentation/AnodotHelpDoc.pdf>, 2015. Accessed: 2020-02-11.
- [29] X. Zhu. *Semi-Supervised Learning*, pages 892–897. Springer US, Boston, MA, 2010.
- [30] Anodot. Ultimate guide to building a machine learning anomaly detection system, part 3 - correlating abnormal behaviour. *OpsMatters White Paper*, 2018.
- [31] Wikipedia. Autocorrelation. <https://en.wikipedia.org/wiki/Autocorrelation>, 2020. Accessed: 2020-02-11.
- [32] Anodot. Ultimate guide to building a machine learning anomaly detection system, part 2 - learning normal time series behaviour. *OpsMatters White Paper*, 2018.
- [33] D. M. Blei, A. Y. Ng, and M. I. Jordan. Latent dirichlet allocation. *Journal of machine Learning research*, 3(Jan):993–1022, 2003.
- [34] Wikipedia. Weka (machine learning). [https://en.wikipedia.org/wiki/Weka_\(machine_learning\)](https://en.wikipedia.org/wiki/Weka_(machine_learning)), 2020. Accessed: 2020-02-11.
- [35] J. Brownlee. What is the weka machine learning workbench. <https://machinelearningmastery.com/what-is-the-weka-machine-learning-workbench/>, 2019. Accessed: 2020-02-11.
- [36] E. Frank, M. A. Hall, and I. H. Witten. The weka workbench. Online Appendix for "Data Mining: Practical Machine Learning Tools and Techniques", 2016.
- [37] Honeynet. Honeynet website. <https://www.honeynet.org/>, 2008. Accessed: 2020-02-11.
- [38] OpenText. Encase[®] endpoint security. <https://www.guidancesoftware.com/encase-endpoint-security>, 2015. Accessed: 2020-02-11.
- [39] Tanium. Tanium products. <https://www.tanium.com/#products>, 2013. Accessed: 2020-02-11.
- [40] VmWare[®] Carbon Black. Threat hunting and incident response for hybrid deployments. <https://www.carbonblack.com/products/edr/>, 2016. Accessed: 2020-02-11.
- [41] Patrick Kral. The incident handler's handbook. <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>, Dec. 2011. Accessed: 2020-02-06.

- [42] D. Gonzalez, D. W. White, J. Stevens, J. Grundman, P. Mehravari, T Curtis, and T. Dolan. Cyber-security capability maturity model version 1.1 (c2m2). department of energy, office of electricity delivery and energy reliability (doe-oe). http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf, 2014. Accessed: 2020-02-06.
- [43] K. Stouffer, J. Falco, and K. Scarfone. Guide to industrial control systems (ICS) security. NIST special publication, 800(82):16–16, 2011.
- [44] P. Mell, K. Kent, and J. Nusbaum. Guide to malware incident prevention and handling. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2005.
- [45] U.S. Department of Homeland Security CISA Cyber Infrastructure. Industrial control systems. http://www.us-cert.gov/control_systems/ics-cert/, Oct. 2019. Accessed: 2020-02-07.
- [46] Network Solutions. Network solutions website. <http://www.isaccouncil.org/>, 2020. Accessed: 2020-02-07.
- [47] J. Andress. The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress, 2014.
- [48] N. Tariq, M. Asim, and F. A. Khan. Securing SCADA-based critical infrastructures: Challenges and open issues. *Procedia Computer Science*, 155:612–617, 2019. The 16th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2019), The 14th International Conference on Future Networks and Communications (FNC-2019), The 9th International Conference on Sustainable Energy Information Technology.
- [49] D. Helbing, L. Buzna, L. Issacharoff, I. Simonsen, C. Kühnert, H. Ammoser, and K. Peters. Cascading disaster spreading and optimal, network-dependant response strategies. http://www.lsa.ethz.ch/news/07.06.20_helbing_cascading.disaster.spreading.pdf, 2007. Accessed: 2020-02-06.
- [50] CIPSEC. D3.4 CIPSEC intra inter dependencies analysis. preliminary report. <https://www.cipsec.eu/content/d34-cipsec-intra-inter-dependencies-analysis-preliminary-report>, 2017. Accessed: 2020-02-06.
- [51] CIPSEC. D3.4 CIPSEC intra / inter dependencies analysis report. <https://www.cipsec.eu/content/d38-cipsec-intra-inter-dependencies-analysis-report>, 2017. Accessed: 2020-02-06.
- [52] A. Humayed, J. Lin, F. Li, and B. Luo. Cyber-physical systems security—a survey. *IEEE Internet of Things Journal*, 4(6):1802–1831, Dec. 2017.
- [53] T. M. Chen. Stuxnet, the real start of cyber warfare? [editor’s note]. *IEEE Network*, 24(6):2–3, Nov. 2010.
- [54] V. M Ijure, S. A Laughter, and R. D Williams. Security issues in SCADA networks. *computers & security*, 25(7):498–506, 2006.
- [55] National Science and Technology Council (U.S.). Summary of the 2018 critical infrastructure security and resilience stakeholder workshop: product of the subcommittee on critical infrastructure security and resilience, committee on homeland and national security of the national science & technology council, Feb. 2018.
- [56] ENISA. How to implement security by design for IoT. <https://www.enisa.europa.eu/news/enisa-news/how-to-implement-security-by-design-for-iot>, Nov. 2019. Accessed: 2020-02-06.
- [57] I. Overland. The geopolitics of renewable energy: Debunking four emerging myths. *Energy Research & Social Science*, 49:36–40, 2019.
- [58] WIRED. Inside the cunning, unprecedented hack of Ukraine’s power grid. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>, March 2016. Accessed: 2020-02-06.

- [59] E. M. Kalogeraki, S. Papastergiou, H. Mouratidis and N. Polemi (2018) “A novel risk assessment methodology for SCADA maritime logistics environments”, Applied Sciences, MDPI AG, Switzerland, 8(9): 1477, ISSN: 2076-3417, <https://doi.org/10.3390/app8091477> .
- [60] Eleni Maria Kalogeraki., Dimitrios Apostolou, Nineta Polemi, Spyros Papastergiou S. (2018) "Knowledge Management Methodology for Identifying Threats in Maritime/Logistics Supply Chains" in S. Durtst, P. Evangelista (Eds) (SI) “Logistics knowledge management: state of the art and future perspectives”, Knowledge Management Research and Practice Journal, Taylor and Francis, ISSN: 1477-8238 (Print) 1477-8246, DOI: 10.1080/14778238.2018.1486789, 16(4): 50
- [61] Cynet 360, Autonomous Breach Protection Platform. Cynet Sensor Fusion. Available online: <https://www.cynet.com/platform/> (accessed on 2020-02-18).
- [62] RSA NetWitness platform. Threat Detection and Response. RSA Security LLC – Dell Technologies Inc. Available online: <https://www.rsa.com/en-us/products/threat-detection-response> (accessed on 2020-02-18).
- [63] Forensic Toolkit. Digital Investigations. AccessData. Available online: <https://accessdata.com/products-services/forensic-toolkit-ftk> (accessed on 2020-02-18).
- [64] ProDiscover suite. Computer Forensics. Dot C Technologies Pvt Ltd. Available online: <https://www.prodiscover.com/> (accessed on 2020-02-18).
- [65] I. H. Witten, E. Frank, and M. A. Hall. The WEKA Workbench. Data mining: practical machine learning tools and techniques. Morgan Kaufmann, 4(2016). Available online: http://www.cs.waikato.ac.nz/ml/weka/Witten_et_al_2016_appendix.pdf (accessed on 2020-02-18).
- [66] scikit-learn Machine Learning in Python. Scikit-Learn. Available online: <https://scikit-learn.org/stable/> (accessed on 2020-02-18).
- [67] Keras: The Python Deep Learning library. Available online: <https://keras.io/> (accessed on 2020-02-18).
- [68] OpenNAC. Open-source NAC Solution Available online: <http://opennac.org/opennac/en.html> (accessed on 2020-02-18).
- [69] Cisco Identity Services Engine. Cisco. Available online: <https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html> (accessed on 2020-02-18).
- [70] ISO/IEC 27001 Information security management. International Organization for Standardization (ISO). Available online: <https://www.iso.org/isoiec-27001-information-security.html> (accessed on 2020-02-18).
- [71] ISO/IEC 27009:2016 Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/42508.html> (accessed on 2020-02-18).
- [72] ISO/IEC 27006:2015 — Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems (third edition). International Organization for Standardization (ISO). Available online: <https://www.iso27001security.com/html/27006.html> (accessed on 2020-02-18).
- [73] ISO/IEC 17021-1:2015 Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/61651.html> (accessed on 2020-02-18).
- [74] ISO / IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls. International Organization for Standardization (ISO). Available online: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en> (accessed on 2020-02-18).

- [75] ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance. International Organization for Standardization (ISO). Available online: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-2:v1:en> (accessed on 2020-02-18).
- [76] ISO/IEC 27004:2009 Information technology — Security techniques — Information security management — Measurement. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/42106.html> (accessed on 2020-02-18).
- [77] ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/75281.html> (accessed on 2020-02-18).
- [78] ISO 31000:2018 Risk management — Guidelines. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/65694.html> (accessed on 2020-02-18).
- [79] ISO/IEC 27007:2017 Information technology — Security techniques — Guidelines for information security management systems auditing. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/67398.html> (accessed on 2020-02-18).
- [80] ISO/IEC TS 27008:2019 Information technology — Security techniques — Guidelines for the assessment of information security controls. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/67397.html> (accessed on 2020-02-18).
- [81] ISO/IEC 27010:2015 Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/68427.html> (accessed on 2020-02-18).
- [82] Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/64143.html> (accessed on 2020-02-18).
- [83] ISO/IEC 27013:2015 Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/64138.html> (accessed on 2020-02-18).
- [84] ISO/IEC 27014:2013 Information technology — Security techniques — Governance of information security. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/43754.html> (accessed on 2020-02-18).
- [85] ISO/IEC TR 27015:2012 Information technology — Security techniques — Information security management guidelines for financial services. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/43755.html> (accessed on 2020-02-18).
- [86] ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/44374.html> (accessed on 2020-02-18).
- [87] ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/44375.html> (accessed on 2020-02-18).
- [88] ISO/IEC 27034-1:2011 Information technology — Security techniques — Application security — Part 1: Overview and concepts. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/44378.html> (accessed on 2020-02-18).

- [89] ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/44379.html> (accessed on 2020-02-18).
- [90] ISO/IEC 27036-3:2013 Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/59688.html> (accessed on 2020-02-18).
- [91] ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/44381.html> (accessed on 2020-02-18).
- [92] ISO/IEC 27042:2015 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/44406.html> (accessed on 2020-02-18).
- [93] ISO 27799:2016 Health informatics — Information security management in health using ISO/IEC 27002. International Organization for Standardization (ISO). Available online: <https://www.iso.org/standard/62777.html> (accessed on 2020-02-18).
- [94] NIST SP 800-61 Rev. 2 "Computer Security Incident Handling Guide" (2012) Supersedes: SP 800-61 Rev. 1 (03/07/2008). National Institute of Standards and Technology.
- [95] NIST Special Publication 800-30, Revision 1 (2012) "Guide for Conducting Risk Assessments", National Institute of Standards and Technology, Gaithersburg.
- [96] NIST Special Publication 800-39 (2011) "Managing Information Security Risk Organization, Mission, and Information System View", National Institute of Standards and Technology, Gaithersburg.
- [97] NIST Special Publication 800-83, Revision 1(2013) "Guide to Malware Incident Prevention and Handling for Desktops and Laptops", National Institute of Standards and Technology.
- [98] NIST SP 800-53, Revision 4 (2013) "Security and Privacy Controls for Federal Information Systems and Organizations", National Institute of Standards and Technology.
- [99] NIST SP 800-86 (2006) "Guide to Integrating Forensic Techniques into Incident Response", Recommendations of the National Institute of Standards and Technology.
- [100] NIST SP 800-150 (2016) "Guide to Cyber Threat Information Sharing", National Institute of Standards and Technology.
- [101] NIST SP 800-184 (2016) "Guide for Cybersecurity Event Recovery", National Institute of Standards and Technology.
- [102] IBM, The total economic impact of IBM resilient, <https://www.ibm.com/downloads/cas/NZREMROM>, Oct. 2017. Accessed: 2020-02-25
- [103] Resolve, Resolve. <https://resolve.io/it-automation-resources/accelerate-security-incident-response-with-automation-soar>, 2019, Accessed: 2020-02-26
- [104] OpenText. Encase® forensic. <https://www.guidancesoftware.com/encase-forensic>, 2015. Accessed: 2020-02-26.
- [105] Forescout, NAC solutions, <https://www.forescout.com/solutions/network-access-control/>, 2018, Accessed: 2020-02-26.
- [106] Inverse, Packetfence v9.3.0, <https://packetfence.org/>, 2020, Accessed: 2020-02-26.
- [107] Harry W. Getting started with cyber incident management, <https://www.ncsc.gov.uk/blog-post/getting-started-with-cyber-incident-management>, Sep. 2019, Accessed 2020-02-26

- [108] Andreas Sfakianakis, Christos Douligeris, Louis Marinos, Marco Louren co, and Omid Raghimi. ENISA threat landscape report 2018, 15 top cyberthreats and trends. ENISA Report, Jan. 2019.
- [109] Hugh Taylor, What are cyber threats and what to do about them, <https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/>, 22nd Jan. 2020, Prey Project, Accessed: 2020-02-26.
- [110] Abi Tyas Tunggal, What is a cyber attack?, <https://www.upguard.com/blog/cyber-attack>, 22nd Jan. 2020, UpGuard™ Website, Accessed: 2020-02-26.
- [111] R. Khan, K. McLaughlin, D. Lavery, and S. Sezer. Stride-based threat modeling for cyber-physical systems. In 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), pages 1–6, Sep. 2017.
- [112] Tobias Schaad and Andreas Reski. "Open Weakness and Vulnerability Modeler"(OVVL): An updated approach to threat modeling. 2019.
- [113] AO Kaspersky Lab, Kaspersky Endpoint Detection and Response, <https://www.kaspersky.com/enterprise-security/endpoint-detection-response-edr>, 2020, Kaspersky website, Accessed: 2020-06-20.
- [114] AO Kaspersky Lab, MITRE ATT&CK: Round 2 Evaluation results, <https://www.kaspersky.com/enterprise-security/mitre/round2-results>, 2020, Kaspersky website, Accessed: 2020-06-20.
- [115] Broadcom, Symantec Endpoint Security, <https://www.broadcom.com/products/cyber-security/endpoint>, 16th Jun. 2019, Broadcom website, Accessed: 2020-06-20.
- [116] CrowdStrike, Falcon Enterprise: Endpoint Security Bundle, <https://www.crowdstrike.com/endpoint-security-products/falcon-endpoint-protection-enterprise/>, 4th May 2020, CrowdStrike website, Accessed: 2020-06-20.
- [117] Cybereason, DR | Cybereason Defense Platform, <https://www.cybereason.com/platform/endpoint-detection-response-edr>, 2020, Cybereason website, Accessed: 2020-06-20.
- [118] Forrester Research, The Forrester Wave™: Enterprise Detection and Response”, Q1 2020, Forrester
- [119] Gartner, Magic Quadrant for Endpoint Protection Platforms, https://www.gartner.com/doc/reprints?id=1-1OEZ6HOU&ct=190822&st=sb&aid=elq_15859, 20th Aug. 2019, Gartner website, Accessed: 2020-06-20.
- [120] MITRE, APT29 Emulation – Cybereason: All Results, <https://attckevals.mitre.org/APT29/results/cybereason/allresults.html>, 2019, MITRE website, Accessed : 2020-06-20.
- [121] MITRE, APT29 Emulation – Kaspersky: All Results, <https://attckevals.mitre.org/APT29/results/kaspersky/allresults.html>, 2019, MITRE website, Accessed : 2020-06-20.
- [122] MITRE, APT29 Emulation – SentinelOne: All Results, <https://attckevals.mitre.org/APT29/results/sentinelone/allresults.html>, 2019, MITRE website, Accessed : 2020-06-20.
- [123] SentinelOne, Endpoint Protection Platform (EPP), <https://www.sentinelone.com/platform/>, 17th Apr. 2020, SentinelOne website, Accessed: 2020-06-20.
- [124] BATADAL Team, Battle of the Attack Detection Algorithms: Disclosing Cyber Attacks on Water Distribution Networks. Journal of Water Resources Planning and Management, 2018
- [125] Beaver, J., Borges-Hink, R., & Buckner, M., An Evaluation of Machine Learning Methods to Detect Malicious SCADA Communications. 2013 12th International Conference on Machine Learning and Applications, pages 54-59, 2013

- [126] Blowers, M., & Williams, J., Machine Learning Applied to Cyber Operations. Network Science and Cybersecurity. Advances in Information Security, Pino R., Ed., vol. 55, pages 155-175, 2014
- [127] Brahmi, I., Ben Yahia, S., Aouadi, H., & Poncelet, P., Towards a Multiagent-Based Distributed Intrusion Detection System Using Data Mining Approaches. Agents and Data Mining Interaction, L. Cao, A. Bazzan, A. Symeonidis, V. Gorodetsky, G. Weiss, & P. Yu (Ed.), pages 173-194, 2012
- [128] D’Antonio, S., Oliviero, F., & Setola, R., High-Speed Intrusion Detection in Support of Critical Infrastructure Protection. Critical Information Infrastructures Security. CRITIS 2006. Lecture Notes in Computer Science, Lopez J. Ed., pages 222-234, 2016
- [129] Hurst, W., Merabti, M., & Fergus, P., Big Data Analysis Techniques for Cyber-threat Detection in Critical Infrastructures. 2014 28th International Conference on Advanced Information Networking and Applications Workshops, pages 916-921, 2014
- [130] Kumar, D., & Fet, D, Performance Analysis of Various Data Mining Algorithms: A Review. International Journal of Computer Applications, vol. 32, num 6, pages 9-16, 2011
- [131] Naik, N., Jenkins, P., Gillett, J., Mouratidis, H., Naik, K., & Song, J, Lockout-Tagout Ransomware: A Detection Method for Ransomware using Fuzzy Hashing and Clustering. 2019 IEEE Symposium Series on Computational Intelligence (SSCI), pages 641-648
- [132] Taormina, R., & Galelli, S, Deep-Learning Approach to the Detection and Localization of Cyber-Physical Attacks on Water Distribution Systems. Journal of Water Resources Planning and Management, 2018
- [133] Tianfield, H, Data mining based cyber-attack detection. System simulation technology, vol. 13, number 2, pages 90-104, 2017
- [134] Yasakethu, S., & Jiang, J., Intrusion Detection via Machine Learning for SCADA System Protection. 1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013), pages 101-105, 2013
- [135] Elastic SIEM, <https://www.elastic.co/siem>, Elastic Website, Accessed: 2020-06-20
- [136] Lucene, <https://lucene.apache.org/>, Lucene Website, Accessed: 2020-06-20
- [137] RTIR, <https://bestpractical.com/rtir>, RTIR Website, Accessed: 2020-06-20
- [138] Use Splunk Phantom, <https://docs.splunk.com/Documentation/Phantom/4.9/User/Intro>, Splunk Website, Accessed: 2020-06-20