




**D9.2**

**Training Materials and  
Report on Training  
Processes**

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

<b>Deliverable type:</b>	Report
<b>Deliverable reference number:</b>	DS-01-833683 / D9.2/ Final   1.0 Training Materials and Report on Training Processes
<b>Work package contributing to the deliverable:</b>	WP 9
<b>Due date:</b>	February 2022 – M30
<b>Actual submission date:</b>	28/03/2022

<b>Responsible organisation:</b>	MAGGIOLI
<b>Editor:</b>	Spyridon Papastergiou
<b>Dissemination level:</b>	PU
<b>Revision:</b>	< FINAL   1.0 >

<p><b>Abstract:</b></p>	<p>This deliverable reports the outcomes of task T9.4 “Stakeholders Training”.</p> <p>It provides a concrete analysis of the training process for the use and operations of the CyberSANE system followed by the consortium to conduct training with pilot end-users and stakeholders, the method adopted to assess training requirements from T2.3 and all the training material that is available to the participants of the training process.</p>
<p><b>Keywords:</b></p>	<p>Training Needs Analysis, training session, training requirements, action plan, incident handling process, end-users, manual, CyberSANE system, Security Professional, training means.</p>
	<p>The project CyberSANE has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833683.</p>

## **Editor**

Spyridon Papastergiou (MAG)

## **Contributors**

Thanos Karantjias (MAG)

Serra Marcello (MAG)

Eleni-Maria Kalogeraki (UBI)

Matej Kovacic (JSI)

Oleksii Osliak (CNR)

Pablo Giménez (VPF)

Luís Landeiro Ribeiro (PDMFC)

Filippo Belinni (LSE)

Diarmuid O' Connor (LSE)



## Version History

Version	Date	Comments, Changes, Status	Authors, Contributors, Reviewers
<b>0.1</b>	24/11/2021	Draft ToC	Spyridon Papastergiou (MAG)
<b>0.2</b>	31/01/2022	Input added in Sections 1,2 and 3, the List of Abbreviations and References	Eleni-Maria Kalogeraki (UBI), Spyridon Papastergiou (MAG)
<b>0.3</b>	01/02/2022	Additional input provided in Sections 2 and 3	Pablo Giménez (VPF)
<b>0.4</b>	28/02/2022	General Revision	Luís Landeiro Ribeiro (PDMFC)
<b>0.5</b>	28/02/2022	Input added in Executive Summary, Introduction, Conclusion Sections and Annexes. Additional input provided in Sections 1,2 and 3	Eleni-Maria Kalogeraki (UBI), Spyridon Papastergiou (MAG), Thanos Karantjias (MAG), Serra Marcello (MAG), Matej Kovacic (JSI), Oleksii Osliak (CNR)
<b>0.6</b>	10/03/2022	Completion of Review Process	Diarmuid O' Connor, Filippo Bellini (LSE), Luís Landeiro Ribeiro (PDMFC)
<b>1.0</b>	11/03/2022	Final Version of Deliverable	Eleni-Maria Kalogeraki (UBI), Spyridon Papastergiou (MAG)

### **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.

## Executive Summary

Training process is the process of expanding one's skills, concepts or attitudes in terms of improving the performance within a working environment.

The current deliverable reports on the outcome of Task 9.4 "*Stakeholders Training*". It presents all the different types of training activities undertaken in the context of the CyberSANE project. In particular, the training activities include:

- The training process action plan
- Past training sessions and the ones planned to be conducted
- The training method followed to elicit training requirements
- The training material provided to educate the pilot end-users and stakeholders on the use and operations of the CyberSANE system together with its components which assisted in preparing the pilot end-users properly for the pilot operations.

The purpose of Task 9.4 is to provide efficient training capabilities to capture all unfulfilled training requirements of the pilot end-users (retrieved from a pilot end-users survey and from various data sources) and thereby facilitate their comprehension of the CyberSANE system usage flows and improve their security awareness, preparedness, response and decision making on incident handling.

Description of the utilized training material and means of supporting the training process are presented in the current report and a detailed list of the training materials' content is depicted in the Annexes.

# Contents

<b>Executive Summary .....</b>	<b>4</b>
<b>Contents.....</b>	<b>5</b>
<b>List of Figures.....</b>	<b>9</b>
<b>List of Tables .....</b>	<b>14</b>
<b>Chapter 1. Introduction .....</b>	<b>15</b>
1.1 Scope .....	15
1.2 Relation to other work packages and tasks .....	15
1.3 Structure of the document.....	15
<b>Chapter 2. Training Needs Analysis Method .....</b>	<b>16</b>
2.1 Introduction to the method .....	16
2.2 Scope and Objectives .....	16
2.3 Target Groups of the CyberSANE training process .....	16
2.4 Description and analysis of the method.....	17
2.5 Pilot end-users survey .....	17
2.6 Analysis of the existing information from various sources .....	18
<b>Chapter 3. Training Process .....</b>	<b>20</b>
3.1 Training Calendar and Action Plan.....	20
3.2 Train the Trainers .....	21
3.3 Train the Pilot End-Users .....	22
<b>Chapter 4. Training Material, Support and Equipment.....</b>	<b>23</b>
4.1 Training Material .....	23
4.2 Training Means Support and Equipment .....	23
<b>Chapter 5. Summary and Conclusion .....</b>	<b>25</b>
<b>Chapter 6. List of Abbreviations.....</b>	<b>26</b>
<b>Chapter 7. Bibliography .....</b>	<b>27</b>
<b>Annex I. Crash course on cybersecurity for organisations.....</b>	<b>28</b>
<b>Introduction .....</b>	<b>32</b>
<b>Taxonomy of cyber-threats.....</b>	<b>34</b>
<b>Main intentional threats to cybersecurity assets .....</b>	<b>36</b>
Physical access .....	36
Network attacks .....	36

Gathering information in the cyberspace.....	37
User-based attacks .....	38
<b>Actors who perform cyber attacks .....</b>	<b>40</b>
<b>Information system security basics .....</b>	<b>42</b>
Basic approaches to providing information security .....	42
Provision of network security .....	43
Passwords .....	44
Creating a secure password .....	45
Typical errors when using passwords .....	47
Changing passwords .....	48
Password management systems.....	48
Advanced authentication systems .....	49
Shared secrets .....	49
Physical security .....	50
Tempest attack.....	52
Backup .....	54
Encryption.....	55
Transport-level encryption and end-to-end encryption .....	56
Man-in-the-middle attack .....	57
Encryption of e-mail and internet communications .....	58
Encryption of mobile communications .....	59
Encryption of data media .....	60
Wiping data.....	60
VPN networks .....	62
Availability.....	64
Remote work .....	64
Anonymization .....	65
<b>Conclusion.....</b>	<b>67</b>
<b>Annex II. CyberSANE System User Manual .....</b>	<b>72</b>
<b>1. Introduction.....</b>	<b>75</b>
1.1 Incident Handling Phases at a glance .....	75
1.2 Structure of the manual .....	76
<b>2. Self-Registration, Support and Profiling.....</b>	<b>77</b>
2.1 Create Account .....	77

2.2 Login.....	78
2.3 Logout.....	79
2.4 Support.....	81
2.5 Profiling (User and Organisation) .....	82
2.5.1 Profile Overview.....	82
2.5.2 Change Password.....	82
2.5.3 Organisation Profile .....	82
<b>3. Overview of the Phases of the Incident Handling Process in the CyberSANE system .....</b>	<b>84</b>
<b>4. Preparation Phase .....</b>	<b>86</b>
4.1 Communication .....	86
4.1.1 Create Internal Contacts.....	87
4.1.2 Create External Contacts.....	88
4.2 Asset Inventory .....	88
4.2.1 Asset Management.....	89
4.2.2 Controls Management .....	94
4.2.3 Vendors Management .....	97
4.3 Threat Intelligence .....	99
4.3.1 Vulnerabilities Management .....	99
4.3.2 Threats Management.....	101
4.3.3 Attack Scenarios Management.....	103
4.3.4 Risk Appetites Management.....	104
4.4 Prevention .....	106
4.4.1 Risk Assessment .....	107
4.4.2 Business Service .....	114
<b>5. Detection and Analysis Phase.....</b>	<b>117</b>
5.1 Security Incidents .....	117
5.1.1 Review Security Incidents information .....	119
5.1.2 Security Incidents Analysis .....	121
5.2 Alerts and Notifications .....	122
5.2.1 View and Manage Alerts.....	122
5.2.2 Create an alert .....	123
5.3 Threat Hunting .....	124
5.3.1 Attack Patterns.....	124
5.3.2 Attack Patterns Analysis .....	125

5.3.3 Anomaly Detection.....	126
5.3.4 Anomaly Detection Analysis .....	127
5.4 Deep Web Threat Intelligence.....	128
5.4.1 Deep Web Articles .....	129
5.4.2 Categories and Concepts .....	132
5.4.3 Tag Cloud and Concept Graphs.....	135
5.4.4 Graph Analytics.....	136
5.4.5 Graph Significant .....	137
5.5 Open Web Threat Intelligence .....	137
5.5.1 Articles.....	138
<b>6. Containment, Eradication and Recovery Phase.....</b>	<b>140</b>
6.1 Create a Strategy.....	140
6.2 Manage a strategy .....	142
6.3 Simulation Environment .....	143
<b>7. Post Incident Activity Phase.....</b>	<b>147</b>
7.1 Create a Lesson Learned.....	147
7.2 Sharing .....	148
7.3 Data Sharing Agreements.....	149
7.3.1 Operations on DSA .....	149
7.3.2 Data Sharing Agreement structure .....	150
7.3.3 Parties Policies .....	151
7.3.4 Authorizations .....	151
7.3.5 Obligations .....	153
7.3.6 Prohibitions .....	154
<b>8. The CyberSANE services.....</b>	<b>156</b>
8.1 LiveNet .....	156
8.1.1 LiveNet Operations .....	157
8.1.2 LiveNet Tools .....	158
8.2 DarkNet .....	160
8.2.1 DarkNet Operations .....	161
8.2.2 DarkNet Tools .....	161
8.3 HybridNet.....	163
8.3.1 HybridNet Operations .....	164
8.3.2 HybridNet Tools .....	164
8.4 ShareNet .....	166

8.4.1 ShareNet Operations .....	167
8.4.2 ShareNet Tools .....	167
8.5 PrivacyNet .....	169
8.5.1 PrivacyNet Operations .....	169
8.5.2 PrivacyNet Tool.....	170
<b>Annex III. CyberSANE System Architecture .....</b>	<b>171</b>

## List of Figures

Figure 1: The four phases of the incident handling process in CyberSANE based on NIST. ....	76
Figure 2 –CyberSANE homepage. ....	77
Figure 3: Sign up the CyberSANE platform.....	78
Figure 4: Login the CyberSANE. ....	79
Figure 5: CyberSANE Dashboard menu. ....	79
Figure 6: Logout from CyberSANE.....	80
Figure 7: Screen after CyberSANE successful logout. ....	80
Figure 8: Contact with the CyberSANE support team in case of issues.....	81
Figure 9: Send an inquiry to the CyberSANE support team. ....	82
Figure 10: CyberSANE user management options. ....	82
Figure 11: CyberSANE organisation profile options. ....	83
Figure 12: Incident handling phases in CyberSANE .....	84
Figure 13: CyberSANE Preparation phase functionalities. ....	86
Figure 14: Creation of an internal contact. ....	87
Figure 15: Creation of an external contact. ....	88
Figure 16: Browse the Asset Inventory and its capabilities. ....	89
Figure 17: A list of the registered asset is depicted from the Asset menu. ....	89
Figure 18: Assets can be searched from the Asset menu. ....	90
Figure 19: Screens from the Asset registration process in CyberSANE. ....	91
Figure 20: The “Visualize” button produces asset graphs and provides security-related information. ....	92
Figure 21: A visualization of an organisation’s assets graph.....	92
Figure 22: An asset “Footprint” button appears upon clicking on a specific asset, herein on the “Public Portal”. ....	93
Figure 23: The asset “Public Portal” footprint displaying the asset’s threat probability and vulnerability impact heatmap. ....	93



Figure 24: Selection of “Very low” Vulnerability impact and “Very High” threat probability combination to explore the generated tuples for the “Public Portal” asset. ....	94
Figure 25: Tuples of identified threats and vulnerabilities for the “Public Portal” asset. .	94
Figure 26: A list of all controls appears in the “Controls Management” page.....	95
Figure 27: Security controls can be viewed in each details or edited. The current figure shows details for the “Web Application Firewall” security control from the CyberSANE control editor.....	95
Figure 28: Example of managing threats for the “Bot Management Solution” security control.....	96
Figure 29: A view of the “Add a new Control” editor .....	97
Figure 30: Vendors Management menu. ....	97
Figure 31: Manually created vendors can be edited or deleted.....	98
Figure 32: View of a vendor’s products. ....	98
Figure 33: Threat Intelligence functionalities.....	99
Figure 34: A screen from the “Vulnerabilities Management List”.....	100
Figure 35: Known affected products from the vulnerability CVE-2018-9979 exploitation. ....	100
Figure 36: Screens to create an unknown/zero-day vulnerability. ....	101
Figure 37: A screen of threats list from the “Threats Management” page. ....	102
Figure 38: Register a threat. ....	102
Figure 39: Attack scenarios Management screen.....	103
Figure 40: Attack scenario development. ....	104
Figure 41: A screen of the “Risk Appetite Management” page.....	104
Figure 42: Configure threat probability capability to define risk appetite. ....	105
Figure 43: Add a new risk appetite. ....	106
Figure 44: Prevention functionalities of the Preparation phase. ....	106
Figure 45: Risk Assessment main page.....	108
Figure 46: Initiate a Risk Assessment.....	108
Figure 47: Risk Assessment results different options. ....	109
Figure 48: The “Visualize” option depicts the organisation’s assets graph, where asset nodes are coloured by assets risk levels.....	109
Figure 49: “PostgreSQL” asset Footprint options are activated.....	110
Figure 50: The Asset Footprint depicts the real status of the asset “PostgreSQL” (after risk assessment) in a “Threat Probability-Vulnerability Impact” Heatmap. Additional options can be explored from the “Chart context” menu.....	110
Figure 51: Threat and Vulnerabilities information can be viewed by clicking on a specific value oof the “Threat Probability-Vulnerability Impact” Heatmap. ....	111
Figure 52: Different charts representing the Individual Risk Level on assets of a specific Business Service. ....	111

Figure 53: Different charts representing the Individual Risk Level on critical assets of a specific Business Service. ....	112
Figure 54: Risk assessment report in table format per asset and per risk level.....	112
Figure 55: Risk Assessment report showing the Dominant Individual Risk Level per asset and the identified threats with corresponding vulnerabilities.....	113
Figure 56: Asset list report related to risk assessment of a given Business Service. ...	113
Figure 57 - Attack scenarios information depicted per asset related to the risk assessment. ....	113
Figure 58: The Business Service functionality in CyberSANE.....	114
Figure 59: Business Service options. ....	115
Figure 60: A list of declared assets on a specific Business Service can be viewed or managed from the “Business Service” functionality. ....	115
Figure 61: Create a Business Service.....	116
Figure 62: CyberSANE Detection and Analysis phase functionalities. ....	117
Figure 63: The Security Professional can search for anomalies, attack patterns and security incidents identified within the organisation for a selected period. ....	118
Figure 64: The Security Professional can review analytics on identified anomalies, attack patterns and security incidents within the organisation upon a selected period. ..	118
Figure 65: Security Incidents functionality offers a detailed list of security incidents, attack patterns and anomalies detected within the organisation. ....	119
Figure 66: Security Incident page of the Detection and Analysis phase. ....	120
Figure 67: CyberSANE system provides a large-scale of attributes of a security incident identified on a specific asset.....	120
Figure 68: The Security Professional can search for anomalies, attack patterns and security incidents identified within the organisation for a selected period. ....	121
Figure 69: The Security Professional can review analytics on the security incidents and their criticality identified on the declared assets of the organisation upon a selected period. ....	121
Figure 70: Raised alerts can be viewed and managed from the “Alerts and Notifications” functionality. ....	122
Figure 71: The “Edit Alert” tab from the “Alerts and Notifications” functionality.....	123
Figure 72: Information on Loggers can be viewed for each alert from the “Alerts and Notifications” functionality. ....	123
Figure 73: The “Create alert” tab from the “Alerts and Notifications” functionality. ....	124
Figure 74: Attack Patterns page of the Detection and Analysis phase.....	125
Figure 75: An excerpt of the provided attributes of an Attack Pattern. ....	125
Figure 76: Attack Patterns Analysis page of the Detection and Analysis phase. ....	126
Figure 77: Anomaly Detection list of the Detection and Analysis phase. ....	127
Figure 78: An excerpt of the provided attributes for a detected anomaly. ....	127
Figure 79: Anomaly Detection Analysis page of the Detection and Analysis phase. ....	128

Figure 80: The Deep Web Threat Intelligence functionality of the Detection and Analysis phase.....	129
Figure 81: Deep Web Articles illustrate whether there is a reputation for the organisation in the Deep and Dark Web and crawls for documents related to the detected evidence.....	129
Figure 82: Documents retrieved from the Deep and Dark Web can be searched to gather specific information. ....	130
Figure 83: A list of documents can be viewed upon search. ....	130
Figure 84: The entire article of a specific document can be accessed and explored....	131
Figure 85: The crawler tab illustrates the different sources where the articles are published in the Deep and Dark Web.....	131
Figure 86: New keywords can be added by the Security Professional to further facilitate searching amid the Deep Web Articles. ....	132
Figure 87: Graphs and statistics on the articles retrieved from the Deep and Dark Web are provided from the Categories and Concepts option of the “Deep Web Threat Intelligence” functionality. ....	132
Figure 88: Popular cyber concepts and statistics can be viewed from related graphs. The current doughnut chart (graph on the left) illustrates the number of “exploits” cyber concept found for a specific period.....	133
Figure 89: Critical scores for popular cyber concepts can be viewed from related graphs. The current area chart (graph on the right) illustrates the critical score for the “Man-In-The-Middle” attack concept for a specific period. ....	133
Figure 90: A visualization of the “URLs Criticality based on Cyber Concepts” graph. ..	134
Figure 91: A graph from the “Categories and Concepts” option of the “Deep Web Threat Intelligence” functionality illustrating the number of crawled URLs per day within the selected period.....	134
Figure 92: A heatmap of URLs scores and cyber concepts is provided from the “Categories and Concepts” option of the “Deep Web Threat Intelligence” functionality. ....	135
Figure 93: A screen from the “Tag Cloud and Concept Graphs” of the “Deep Web Threat Intelligence” functionality. ....	136
Figure 94: A screen from the “Graph Analytics” of the “Deep Web Threat Intelligence” functionality. ....	136
Figure 95: A screen from the “Graph Significant” of the “Deep Web Threat Intelligence” functionality. ....	137
Figure 96: A screen from the “Open Web Threat Intelligence” functionality of the “Detection and Analysis” phase.....	138
Figure 97: Security articles can be searched from the open web from the “Open Web Threat Intelligence” functionality.....	138
Figure 98: Articles from the open web can be explored upon search from the “Open Web Threat Intelligence” functionality.....	139
Figure 99: The entire content of an article and the sources where it is published on the open web can be viewed from the “Open Web Threat Intelligence” functionality. ....	139

Figure 100: A screen from the “Containment, Eradication and Recovery” functionality of the CyberSANE system. ....	140
Figure 101: The “Create Strategy” tab from the “Containment, Eradication and Recovery” phase functionality. ....	141
Figure 102: Managing an existing strategy from the “Containment, Eradication and Recovery” phase functionality. ....	142
Figure 103: The Security Professional can edit information on an existing strategy from the “Edit Strategy” tab. ....	143
Figure 104: The “Simulation Environment” of the “Containment, Eradication and Recovery” phase. ....	143
Figure 105: Setting an attack path example. ....	144
Figure 106: Attack Path results are provided upon a given attack path query. The green coloured chains are successful attack paths that might have been occurred in the organisation’s assets according to the detected evidence. ....	144
Figure 107: Attack graphs illustrate the potential attack paths between asset nodes upon specific query. ....	145
Figure 108: Further security information can be viewed by clicking on a specific asset node. ....	145
Figure 109: The “Node Details” tab illustrates further security information of an asset node. ....	146
Figure 110: A screen from the “Post Incident Activity” phase of the CyberSANE system. ....	147
Figure 111: The “Create Lesson” tab shall be filled and saved to create a lesson learned. ....	148
Figure 112: DSA Editor - list of available operations on DSAs ....	149
Figure 113: DSA Editor - DSA metadata ....	150
Figure 114: DSA Editor - Parties Policies ....	151
Figure 115: DSA Editor - Authorisations ....	152
Figure 116: DSA Editor - Subject attributes for authorisations ....	152
Figure 117: DSA Editor - data attributes for authorisations ....	153
Figure 118: DSA Editor - Obligations ....	153
Figure 119: DSA Editor – Prohibitions ....	154
Figure 120: CyberSANE Post Incident Activity - select DSA ....	155
Figure 121: The CyberSANE LiveNet service. ....	157
Figure 122: CyberSANE DarkNet service. ....	160
Figure 123: The CyberSANE HybridNet service. ....	163
Figure 124: The CyberSANE ShareNet service. ....	166
Figure 125: The CyberSANE PrivacyNet service. ....	169

## List of Tables

Table 1: Training Sessions action plan.....	21
---	----

# Chapter 1. Introduction

## 1.1 Scope

This deliverable aims at presenting all the information related to the processes that will be undertaken, the method that will be followed and the training material that will be utilized to enlighten end-users on the operation and use of the CyberSANE system and each accompanying component. The Deliverable D9.2 “*Training Materials and Report on Training Processes*” is the outcome of task T9.4 “*Stakeholders’ Training*”. The ultimate purpose of the training processes is to familiarize Critical Information Infrastructure (CII) operators, Security Professionals and Security Analysts with the CyberSANE system and prepare pilot end-users to use its environment towards the three pilot demonstrations: the Container Cargo Transportation Pilot, the Solar Energy Production, Storage and Distribution Pilot and the Cyber-threat Identification and Communication in Healthcare Pilot. The CyberSANE training processes will be conducted by technical experts of the consortium.

## 1.2 Relation to other work packages and tasks

Considering the collection and analysis of the training requirements of the various CII operators and stakeholders of WP2 “*User requirements and Reference Scenarios*” – Task T2.3 “*Stakeholders’ Requirements*”, the current deliverable adopts a Training Needs Analysis (TNA) method to organize and execute the training processes of the CyberSANE project.

Within this deliverable, all the training activities of the project are reported, the training material and the documentation that will be used to train the selected end-users and stakeholders (T9.2 “*Stakeholders Mobilization and Workshops*”) who will be involved in the CyberSANE pilot operations (T9.5 “*Demonstrator Operation, Support and Measurements*”).

## 1.3 Structure of the document

This document is structured into five main chapters as follows:

- Chapter 1 sets an introduction to the Training process along with the Training Materials of the current report and provides the structure of the deliverable and the related project’s tasks;
- Chapter 2 presents the Training Needs Analysis (TNA) method adopted for the training process;
- Chapter 3 describes the training process, the different types of training adopted and the decided action plan;
- Chapter 4 presents all the training material that accompanies the training activities and the supporting human resources, mechanisms and tools that utilized to coordinate the overall training process
- Chapter 5 summarizes the current report and draws conclusions

## Chapter 2. Training Needs Analysis Method

### 2.1 Introduction to the method

TNA is the identification and analysis of the gap between employees' training and training requirements. The training process is considered the process during which "the acquisition of skills, concepts or attitudes that result in improved performance within the job environment" are obtained [1].

Training analysis delves into an operational domain recognizing all the initial skills, concepts and attitudes of the human elements of a system and specifying the appropriate training.

This chapter describes the TNA that will be adopted to conduct and implement the CyberSANE training process as part of T9.4. The adopted TNA addresses the following features:

- Review of current training;
- Task analysis;
- Identification of training gap;
- Statement of training requirement.

Training Analysis is usually carried out as part of the system development process. Due to the close tie between the design of the CyberSANE system and the training needs, the analysis run alongside the development.

### 2.2 Scope and Objectives

The main scope of the TNA for the CyberSANE project is to capture all the appropriate information that will organize and drive the CyberSANE training process. The adopted TNA meets the following characteristics:

- Context specific: Relevant to the CyberSANE Project and the participated Organisations (both as Technical Partners & Stakeholders) concerning the personnel skills and experience, requirements and expectations;
- Relevant to the trainees: Training process should guide and assist the trainees how to implement their tasks when using the CyberSANE platform;
- Appropriate in terms of structure, timing and learning styles: CyberSANE training process should be conducted in a way (i.e. structure, timing, and method of training) that facilitates the learning of the target group.

### 2.3 Target Groups of the CyberSANE training process

To identify the target groups that will participate in the CyberSANE training process, the training requirements must be considered. This information is captured from the pilot end-users' requirements retrieved from the implementation of Task T2.3 "*Stakeholders*'



*Requirements*". To this end, the main target groups of the CyberSANE training process are:

- Key Users (i.e. CII operators coming from the Transportation, Energy and Healthcare industry sectors);
- Administrators (i.e. Information Security Officers, Information Technology (IT) Administrators);
- Technical Staff (i.e. Security Professionals, Cybersecurity Analysts, IT Administrators, System Administrators, Technical personnel, Security Experts of Transportation, Energy and Healthcare stakeholders).

## 2.4 Description and analysis of the method

This section describes the main areas of enquiry and the TNA method used to conduct and implement the CyberSANE training process.

As described previously, the TNA is used to assess organisations and/or project's training needs following a gap analysis. The aim is to identify the gap between the knowledge, skills and attitudes that people in the organisation currently possess and the knowledge, skills and attitudes that they require to meet the organisation's objectives.

There are many ways to conduct a TNA, depending on the current situation each time. One size does not fit all. The purpose of the assessment of the training needs is to:

- Lead into a design of a specific purpose improvement initiative (e.g. user claim reduction)
- Enable the design of the Project's training calendar
- Identify training and development needs of individual staff during the performance appraisal cycle.

To identify the TNA, we considered the training needs at the organisation level, at the project level and at the department level of specific employees. These considerations help to determine:

- Who will conduct the TNA
- How the TNA will be conducted
- What data sources will be used.

To capture the training, education and development needs of CII operators a number of methods were utilized. This ensured that the data gathered was unbiased and identified gaps and balances under different perceptions. The approaches adopted to explore the CyberSANE training needs, have been assessed to consider the time constraints of those involved; costs involved if any; available resources; and the preferences of those involved.

## 2.5 Pilot end-users survey

A part of the training needs assessment has been conducted during the execution of Task 2.3 "*Stakeholders' requirements*". Furthermore, a survey was set up for stakeholders that will participate in the CyberSANE training process. In this vein,



information was collected from pilot end-users through the content of corresponding questionnaires to capture the CII operators' training requirements. This survey is reported in deliverable D2.3 "*Users and Stakeholders Requirements and Reference scenarios*" [2] which specifies why, what, who, when, where and how. The training needs assessment was obtained from pilot end-users answers and feedback to the following questions:

- Are there skilled and trained personnel on security and incident handling practices?
- Does your organisation offer / is willing to offer training programs on its employees about security awareness on their Critical Infrastructures (CIs)? If yes, how long is the average duration of each training program?
- Are drills conducted frequently? What is the duration of the training?
- Critical Infrastructure Protection (CIP) readiness: In recent years Security officers and IT employees tend to be ambivalent towards engaging their organisation in a CIP program?
- Do you see any addressed security requirement to engage a CIP program in your organisation?

The output of the survey related to the training needs assessment showed that:

- The organisations of most pilot end-users have some skilled and trained personnel on security and incident handling practices
- Above the average of the responders, answered positively that their organisations offer a training program about security awareness on their CIs. In most cases occasionally and in few cases on an annual basis. In most cases the organisations offer daily training programs and in few cases with 2-3 days duration
- Regarding, CIP readiness, half of the responders agree that within the last years the Security officers and IT employees tend to be ambivalent towards engaging their organisation in a CIP program and half of the responders disagree
- Above the average of the responders don't see any addressed security requirement to engage a CIP program in their organisation.

As a consequence, the personnel of the pilot end-users organisations is partially trained. A considerable number of responders have attended a training program in their organisation related to security awareness of their CIs, nevertheless, most of them occasionally. According to the results, there is a considerable requirement to train the pilot end-users on security and incident handling practices and raise their security awareness and consciousness on the involving threat landscape and help them improve their incident handling capabilities and skills.

## **2.6 Analysis of the existing information from various sources**

Apart from the stakeholders' survey, the training requirements were gathered through consultation from the CyberSANE Project's Pilot Sites and through open discussions with senior staff during dedicated teleconferences of T9.4. Thereby, the team and

## D9.2 – Training Materials and Report on Training Processes

---

gathered samples of work relating to the range of training activities delivered in the past (past deliverables, presentations, meetings) were considered.

This approach provides the following benefits:

- Quick, low-cost approach using information already available
- Provides information about individual, organisation and future needs
- Assists alignment of activities with organisational goals
- Demonstrates to staff that action is being taken to address issues they have identified
- Provides information to supplement and compare to other information sources (past maritime security projects e.g. [SAURON](#), [MITIGATE](#), MEDUSA, etc.).

## Chapter 3. Training Process

The CyberSANE training process is split into two phases:

- “*Train the trainers*” phase referring to stakeholders and pilot representatives end-users training of the CyberSANE system and its accompanying components
- “*Train the pilot end-users*” phase referring to the training of the internal and external pilot participants (end-users) of the CyberSANE system and its accompanying components.

The phases of the CyberSANE training process are presented in the following sections.

The CyberSANE training process follows a composite approach integrating different training types:

- Self-instruction utilizing training materials (e.g. manuals, online training videos, etc., cf. section 4)
- Face-to-face training by skilled technical experts of the project
- Online training sessions instructor lead which are organized by consortium members and presented in the following sections
- Online support from the technical partners via e-mails and other telecommunication.

The next sections describe the action plan of the training process decided by the consortium and analyses its distinct training phases.

### 3.1 Training Calendar and Action Plan

During WP9 and T9.4 devoted meetings, the consortium proposed a series of training sessions to capture the training requirements, analysed in Section 2 and educate properly all target groups (i.e., key users, administrators, technical staff). The aim of the current training action plan is to help pilot end-users deeply comprehend the CyberSANE system and its operations and get properly prepared for the pilots, raise the awareness of a group of stakeholders and project’s end-users on the incident handling process and therefore increase their preparedness, response and decision making capabilities. Upon these perspectives and considering that stakeholders’ training is a continuous process, the consortium decided to undertake the action plan presented in the following table:

Date	Description
11-01-2022	Training Session to Project End-Users (pilot representatives and supporting parties)
19-01-2022	Training Session to the Executive Advisor Board (EAB) and consortium end-users (cybersecurity specialists and pilot industries experts)

02-01-2022	Initiate the “ <i>Container Cargo Transportation</i> ” Pilot Event with a training session before the pilot operations (train pilot end-users and external stakeholders)
22-03-2022	Initiate the “ <i>Solar Energy Production Storage and Distribution</i> ” Pilot with a training session before the pilot operations take effect (train pilot end-users and external stakeholders)
Planned during May 2022	Initiate the “ <i>Cyber-threat identification and communication in healthcare</i> ” Pilot Event with a training session before the pilot operations take place (train pilot end-users and external stakeholders)

Table 1: Training Sessions action plan

The training action plan shall be managed & executed by all participating stakeholders.

In addition, the training process shall combine theory and hands-on practice. Therefore, a set of training materials will be available to the trainers, to facilitate the training activities. The type of the training material is described in section 4 and the content of the material is presented in the Annexes of the current deliverable.

### 3.2 Train the Trainers

The current training sessions are mainly focused on the consortium end-users and internal pilot participants. The “Train the Trainers” phase involves the training conducted by the technical experts of the project’s consortium who have overseen the development of the CyberSANE system. These technical experts organized the following training sessions to train pilot representatives (trainers) assigned to each pilot site during January 2022:

- The 1<sup>st</sup> CyberSANE platform training session was organized for the pilot end-users representatives and other consortium’s end-users through an electronic webinar, carried out on 11<sup>th</sup> January 2022. It was a 2-hour training session dedicated to the project’s end-users (pilot sites and supporting partners). During the training session, a detailed presentation of the CyberSANE platform was provided by the technical representative from MAG showing online the CyberSANE system and each different module, screen and feature that will be used during the three CyberSANE pilot demonstrations. Moreover, a representative from CNR undertook the description of the Data Sharing Agreement (DSA) module of the ShareNet component of the CyberSANE system. This was the first contact of end-users with the CyberSANE environment.
- The 2<sup>nd</sup> CyberSANE platform training session was organized for the Executive Advisory Board (EAB), consortium end-users, pilot representatives and other stakeholders via a virtual workshop that occurred on 19<sup>th</sup> January 2022. The duration of the session was approximately 1 hour and a half, where the CyberSANE technical expert illustrated the CyberSANE system functionalities directly from the platform online in real-time. Within this session, cybersecurity specialists and industry experts trained on the CyberSANE system and incident handling process. Pilot end-users gained further experience with the CyberSANE system and got more familiarized with the user interface.

### 3.3 Train the Pilot End-Users

The current phase is mainly focused on pilot end-users (internal and external). This training phase is being performed in parallel with the pilot period.

According to the training calendar and action plan, training sessions are scheduled on the days of the three pilots at the beginning of the events prior to pilot operations which will be conducted by the CyberSANE technical team. In addition, during the three pilots (Transportation, Energy and Healthcare) CyberSANE trainers (pilot representatives), who were trained by the project's consortium technical experts during the previous period, undertake the responsibility to train other pilot end-users (both internal and external) on the CyberSANE environment to get them familiarized with it and be in position to evaluate the CyberSANE system and each accompanying components under the scope of the CyberSANE pilot reference scenarios. Within this phase, the training sessions are invited to be attended by Security Analysts, Security Professionals, IT experts, Industry players, CII operators and other interest groups inside and outside the consortium. Considering the training action plan described in section 3.1:

- A training session carried out at the beginning of the “*Container Cargo Transportation*” Pilot Event on 2<sup>nd</sup> February 2022
- A training session is planned to take place in the “*Solar Energy Production Storage and Distribution*” Pilot Event prior to the pilot operations (expected to occur between 22<sup>nd</sup> March 2022 and 10<sup>th</sup> of April 2022)
- A training session is planned to initiate the “*Cyber-threat identification and communication in healthcare*” Pilot Event before the pilot demonstrations (expected to occur during May).

## Chapter 4. Training Material, Support and Equipment

### 4.1 Training Material

To facilitate the training activities, educational material and tutorials are utilised within the training process. The material that is provided to help the pilot end-users and stakeholders get familiarized with the CyberSANE system and its components is the following:

- The “Crash course on cybersecurity for organisations”, which is a cybersecurity awareness documentation, provides guidance on Information Security and explores the various aspects of cybersecurity, involving business entities and indicating technologically neutral advice for the implementation of protection against cyber-attacks within companies. The respective guidance is contained in Annex-I of this deliverable
- The “CyberSANE System User Manual”. A document describing the CyberSANE system User Interface with showcases wherever required. It presents all CyberSANE usage flows as a guide to the CyberSANE users (e.g. Security Professional, Security Analyst, etc.) to indicate how they can take advantage of the CyberSANE system and its accompanying components to make proper decisions for the incident handling process. This guidance adopts the incident handling phases based on NIST SP 800-61 recommendations [3]. Moreover, it briefly presents the CyberSANE components LiveNet, DarkNet, HybridNet, ShareNet, PrivacyNet. The CyberSANE system User Manual is provided in Annex-II of the current deliverable
- Specialized training material in PowerPoint presentation format illustrating the CyberSANE system components for better comprehension Screenshots from the auxiliary material is provided in Annex-III of the current deliverable
- Video recording & Multimedia from conducted training session. A video was recorded during the online training session of “*Container Cargo Transportation*” illustrating all the main functionalities of the CyberSANE system directly through the platform. The video is available through the following link: <https://youtu.be/2ilz--LZPuY>.
- Training Agenda helps the user to get an idea of the training session and feature walkthrough
- Public version Deliverables of the CyberSANE project related to the CyberSANE system and its components
- E-mails, online Frequently Asked Questions (FAQs) and online helpdesk are available for responding to inquiries.

### 4.2 Training Means Support and Equipment

To carry out and support the training activities, a set of elements are utilized:

- Platform Uniform Resource Locators (URLs) to provide remote access to the CyberSANE system
- User accounts for trainees
- Continuous monitoring of virtual tools to ensure that their operations work properly
- Workspaces, technical support and IT equipment (i.e., digital and physical networking equipment, switches, routers, workstations, databases, cloud-based and mailing services, etc.) to run the training

- Telecommunication equipment (i.e., audiovisual devices, teleconference applications, Personal Computers (PCs), mobile devices, microphones etc.) to carry out the online sessions

In addition, a group of people from the project's technical partners, security experts and IT specialists are engaged to support the training process with various roles (i.e., instructors, helpdesk, system administrators and back-end office, etc.). To coordinate the training process, one-to-one meetings and workshops are carried out.

## Chapter 5. Summary and Conclusion

The current Deliverable D9.2 “*Training Materials and Report on Training Processes*” provided an extensive description of all the activities, proposed plans, material, equipment, human resources, infrastructures, means are engaged in the training process of the CyberSANE system.

To conduct the training process efficiently, the CyberSANE consortium followed acknowledged methods and practices to collect information regarding potential gaps between the end-users training and the training requirements. In particular, with the conduction of a TNA method, the CyberSANE consortium performed an assessment on the end-users training requirements. Scope and objectives of undertaking this TNA method, its content and training target groups (e.g. key users, administrators, technical personnel) are described in Section 2. In addition, the section justifies the conditions under which the TNA was performed and the data sources that were used (e.g. initiate a pilot end-users training survey by disseminating questionnaires to end-users related to training and gathering their responses, explore information from various sources (e.g. from public reports of past projects, etc.)

Section 3 described the training process that is undertaken by the CyberSANE consortium to train pilot end-users and stakeholders on the use and operations of the CyberSANE system. This process falls into two phases; the “*Train the trainers*” phase and the “*Train the pilot end-users*” phase. An action plan to organize five training sessions (two in the first phase and three in the latter phase), is to be followed in an efficient manner that will capture the identified end-users’ training requirements. Different types of training are realized during the training execution and respectively reported.

Training means and educational material accompany and support the training process to facilitate the courses and allow trainees to better comprehend the content. Such training material is the CyberSANE user manual, the information security guide, training recordings, etc., analyzed in section 4. The content of the main training material utilized by stakeholders to learn how to use the CyberSANE system is presented in the Annexes of this deliverable.

The presented training process along with the accompanying material aimed at allowing pilot end-users and stakeholders to get familiarized with the CyberSANE system and its components, leverage their knowledge incident handling, increase their security awareness and raise their consciousness to improve protection on their CILs.



## Chapter 6. List of Abbreviations

Abbreviation	Translation
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIP	Critical Infrastructure Protection
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
DSA	Data Sharing Agreement
EAB	Executive Advisory Board
FAQ	Frequently Asked Question
IT	Information Technology
PC	Personal Computer
TNA	Training Needs Analysis
URL	Uniform Resource Locator

## Chapter 7. Bibliography

- [1] *How to Conduct a Training Needs Analysis*. Directory Journal. Available online: <https://www.dirjournal.com/blogs/how-to-conduct-a-training-needs-analysis/> . Accessed: 2022-01-28.
- [2] CyberSANE project. D2.3 - “*Users and Stakeholders Requirements and Reference scenarios*”. 2020.
- [3] Cichonski, P.; Millar, T.; Grance, T.; Scarfone K.; (2012). *Computer Security Incident Handling Guide*. National Institute of Standards and Technology (NIST); Special Publication (SP) 800-61, Rev.2. U.S. Department of Commerce. Available online: <http://dx.doi.org/10.6028/NIST.SP.800-61r2> . Accessed: 2022-02-08.

## **Annex I. Crash course on cybersecurity for organisations**

# **Crash course on cybersecurity for organisations**

A manual for surviving in a networked world

Matej Kovačič

February 2022

The aim of this handbook is to provide a clear overview of the various aspects of cyber security that are relevant for business entities and to provide technologically neutral advice for the implementation of protection against cyber-attacks within companies.

This handbook is intended for managers who are primarily responsible for the implementation of information security solutions in their business environment and for users of information technology. The provision of information security requires both technology and appropriate organisational rules (security policies). An important part of the provision of information security in an organisation is also the education of users (employees). Employees who are not aware of the security risks for the organisation represent a major hazard and poor information security can ultimately jeopardize the very existence of the organisation.

**About the author**

Matej Kovacic, PhD, works as a researcher at Jozef Stefan Institute (<https://www.ijs.si/>) and International Research Centre on Artificial Intelligence (<https://ircai.org/>). He is also a Senior Lecturer in Information Security at the University of Nova Gorica (<https://www.ung.si>).

He has done several presentations on cryptography and information security (especially in the area of mobile communications security) and has extensive knowledge on IT law related issues. He has experience in digital forensic analysis and is a member of expert's council of Institute for forensics of information technology (IFIT - <http://www.ifit.si/>). Personal website and blog (mostly in Slovenian language): <https://telefoncek.si>.

## Introduction

Information security involves the defence and protection of data, information systems and the entire information environment against unauthorised or unlawful access; use, disclosure, interference, modification or destruction. Information security helps us to mitigate these risks and their consequences. The goal of information security is to ensure confidentiality; authenticity, integrity and availability of data, regardless of their format: electronic, printed or any other. Cyber security covers a broader scope; it is defined as the ability to defend, protect and secure a cyber-space (the global information environment, formed by electronic communication networks and computer systems) against cyber threats, incidents and cyber-attacks.

The field of information security has become increasingly important in recent years, both in the public and private sectors. Since the modern business environment is largely digital, it is necessary to ensure that business information and other data are protected and that the information environment is secured. Information security is not only necessary to ensure compliance with regulations and legislation (GDPR, etc.), protect the intellectual property of an organisation and to maintain a competitive advantage. It is also important, because the level of information security will often influence the operations or even existence of the company. A properly regulated area of information security provides risk management and business reliability for organisations, however an equilibrium must be found between risk management and productivity.

Overall, it must be kept in mind that security is not just technology or a product or a service that is procured, but a process. The provision of information security involves both technology and people.

It cannot be guaranteed by simply purchasing suitable security equipment - it requires a strategic approach and must be managed comprehensively. The provision of information security is therefore a continuous process including organisational and technical measures to protect data or information and information systems as well to educate people (i.e. employees and users). Education is one of the most important parts of information security in an organisation, but it is often overlooked at the expense of automated technical solutions. Although the technical solutions for automating information security are certainly important, automated systems cannot completely replace IT (information technology) administrators in companies and cannot resolve all user errors.

A security culture must be developed and grown continuously, whereby we can draw an analogy from traffic safety – the safety of participants on the road depends not only on a successfully completed driver's exam; the knowledge about safety must be constantly renewed and applied.

The provision of information security therefore starts with the information infrastructure itself and continues with the protection of devices, data and applications. Users are also of utmost importance, as they are often the most exposed link in cyber-attacks. In addition to adequate protection of the final users and their devices, education must be provided as well, since employees who are not aware of the security risks for the organisation represent a major hazard.

## D9.2 – Training Materials and Report on Training Processes

---

Additionally, security mechanisms must comply with regulatory and legal requirements and support operational requirements.



## Taxonomy of cyber-threats

Cyber-threats and cyber-attacks can vary considerably in a technical sense, with new forms of attacks constantly emerging. Therefore it can be difficult to establish a complete map of the attacks, since the area is always evolving. On the other hand, we must also consider threat actors with different intents, objectives and strategies to breach the protection of data and systems.

However, cyber-threats have certain characteristics that enable their classification into different subgroups. In the past years, several cyber threats classification systems (also known as threat taxonomies) were introduced.

The *European Union Agency for Network and Security Information* (ENISA) threat taxonomy defines the following threats (ENISA, 2016):

- **Physical attacks** (fraud, sabotage, vandalism, theft, information leakage/sharing, unauthorized physical access (entry to premises), coercion, extortion or corruption, damage from the warfare and terrorists attacks);
- **Unintentional damage or loss of information or IT assets** (information leakage or sharing due to human error, erroneous use or administration of devices and systems, using information from an unreliable source, unintentional change of data in an information system, inadequate design and planning or improperly adaptation, damage caused by a third party, damages resulting from penetration testing, loss of information in the cloud, loss of (integrity of) sensitive information, loss of devices, storage media and documents, destruction of records);
- **Disasters** (natural and human caused disasters);
- **Failures and malfunctions** (of devices or systems, disruption of communication links, main supply, service providers (supply chain) and malfunction of equipment);
- **Outages** (loss of resources, absence of personnel, loss of support services, Internet or network outage);
- **Eavesdropping, interception or hijacking** (war driving, intercepting compromising emissions, interception of information, interfering radiation, replay of messages, network reconnaissance, network traffic manipulation and information gathering, man in the middle attacks);
- **Nefarious activity or abuse** (identity theft, spam mail, denial of service, malware, social engineering, abuse of information leakage, generation and use of rogue certificates, manipulation of hardware and software, manipulation of information, misuse of audit tools, information and information systems, unauthorized activities (including unauthorized installation of software, data breaches, hoaxes, remote activities (execution), targeted attacks (APTs etc.), failed of business process, brute force and abuse of authorizations);
- **Legal** (violation of laws or regulations, failure to meet contractual requirements, unauthorized use of IPR protected resources, abuse of personal data, judiciary decisions/court orders).

We can see that ENISA's classification includes cyber and non-cyber threats, human and non-human induced threats and that threats could be intentional or accidental.

However, as we already mentioned, security is not just about technology. It also involves people and sometimes even broader environment (threats from human and non-human events in environment).

If we focus to people and technology, cyber-threats could therefore be classified into four main groups:

- **Loss of assets** because of disasters, failures, damage, malfunctions and outages. These threats could be accidental or intentional (for instance denial of service attacks, etc.).
- **Cyber-attacks to the systems and data** (some of them require physical access to the systems, while others could be performed with network access (for instance several attacks on communications, like intercepting or manipulation of network traffic as well as direct attacks on "virtual space"), exploiting human errors, mistakes by administration of devices and systems, 0-day vulnerabilities, etc.).
- **Network reconnaissance and information gathering**, which also includes information leakage due to human errors or lack of knowledge (for instance information mistakenly published on an Internet).
- **User-based attacks**. These include all cases where users of information technology are manipulated, for instance with social engineering, hoaxes but also extortion or corruption, cases where users are subject to identity and/or credentials theft or information leakage and cases where users are intentionally taking activities like sabotage, vandalism, theft, manipulation of hardware, software or information performing unauthorized activities.

While it is very hard to prevent all threats, in many cases these threats could be mitigated by adequate design of systems, adequate planning and education of users and administrators of these systems. This includes implementing active and passive measures for systems and information protection, including preparation of contingency plans and disaster recovery.

While some of the outlined threats are accidental / non-intentional (for instance failures, outages, etc.), some others are intentional, which refer to purposeful actions to attack cybersecurity assets.

## **Main intentional threats to cybersecurity assets**

In the following chapters we will outline some main intentional threats to the cybersecurity assets. These are physical access to the systems and data, network attacks (access through virtual space), gathering information in the cyberspace and user-based attacks (which is actually an indirect attack on cybersecurity assets through people).

### **Physical access**

Physical security is a very important aspect of information system security that is neglected all too often. The purpose of physical protection of access to information systems is to prevent unauthorised access to the information system and the information contained within. This is not just an issue of theft; an attacker may use physical access to the information system to install malicious software or hardware to circumvent the existing security mechanisms or obtain remote access to the system. We should also be mindful of discarded computer components which may still contain sensitive data. This includes not only hard drives and flash drives but also mobile phones and even printers with built-in data storage and other peripheral devices.

Physical access therefore do not mean only access to premises where the cybersecurity assets are located, but a general access to them. That includes access from the point of manufacturing (this includes possibility of supply-chain interdiction, i.e. intercepting equipment that is being shipped to the target customer), access by servicemen and all up to when equipment is discarded.

### **Network attacks**

Network attacks could be divided into attacks on network links and communications and attacks on so called virtual space.

Attacks on network links and communications are including all methods and techniques of intercepting or manipulation (including redirection) of network traffic, where an attacker can gain access to the content of the communication or insert fake content into the communication between any two point.

Attacks on a virtual space (that includes unwarranted entry to the virtual space) of the user or organisation typically involves various types of intrusion or any other form of unauthorized access to the systems, for instance guessing access credentials, gaining access with unchanged default passwords, exploiting human errors and mistakes by administration of devices and systems, exploiting 0-day vulnerabilities, etc.

## Gathering information in the cyberspace

Internet search engines and social networks are a valuable source of information. Attackers know that, so information gathering is usually the first step or a preparation tool for an actual attack. Some information that could be gathered are public by the nature. Typical examples are information that could be gathered by browsing internet resources, querying DNS<sup>1</sup> and Whois databases<sup>2</sup> and information from various official registries. This is sometimes also called open-source intelligence (OSINT), which is a set of strategies and methods for the collection and analysis of data gathered from publicly available sources to produce actionable intelligence. However, some information is sometimes available as a consequence of information leakage due to human errors, carelessness or lack of knowledge (typical example of the latter is the information mistakenly published on an Internet).

Users often publish a lot of information on social networks; some have been doing so for several years. An analysis of this information can reveal a significant amount about the user. Internet search engines are particularly interesting, as they can also reveal hidden information. For example, files that users have erroneously stored on publicly available servers (sometimes even confidential and secret documents can be found in this way), accidentally opened access to databases as well as various devices that are inadvertently accessible to the public (e.g. webcams, printers, baby-cameras 'babycams', routers, even industrial systems that can be remotely controlled). The analysis of metadata in publicly available documents may also reveal additional information.

Among the first to be aware of the possibilities of the collection of such information were members of an American hacker group *LOpht Heavy Industries*, active in the years between 1992 - 2000, who scoured public web sites of various organisations, searching for documents containing terms such as "confidential" or "password". A security researcher from Poland, Michal Zalewski, was probably the first person who published a post (in August 2001) describing use of the search engines for attacking internet servers (Zalewski, 2001). The same year, in November 2001, a French security researcher Vincent Gaillot demonstrated how confidential information can be searched using the Google search engine (Gaillot, 2001), and a few years later, security researchers Johnny Long and Ed Skoudis wrote a book titled *Google Hacking for Penetration Testers* on this topic (Long and Skoudis, 2005). In 2009, a specialised search engine, Shodan, appeared on the internet, which could be used to find unprotected IoT<sup>3</sup> devices and services, and today several tools exist that can help hackers or security researchers to search for various types of devices connected to the internet and to analyse metadata in public documents.

As we can see, network reconnaissance attacks are usually the first step of an actual attack, and that kind of information gathering could be very effective while it does not require extensive technical knowledge from the attacker. Network reconnaissance

---

1 DNS – Domain Name System is the hierarchical and decentralized naming system that translates human readable domain names to machine readable IP addresses.

2 WHOIS - a database which stores registered users or assignees of Internet resources like domain name, IP address block or autonomous system data.

3 IoT – Internet of Things, physical objects that are embedded with sensors and software that connect and exchange data with other devices and systems over the communications networks.

attacks are usually divided into public, social and software reconnaissance attacks. In public reconnaissance attacks an attacker collects information about the target from public domains, while in software reconnaissance attacks an attacker uses special software tools to gather information about the target. These include tools for DNS querying, network scanning, service discovery, and so on. In social reconnaissance attack a target are humans and an attacker uses social engineering to gather information. This will be discussed in more detail in the next chapter.

## User-based attacks

Social engineering describes a set of techniques that attackers use to gain benefits by manipulating or abusing an individual's trust. The attacker (also referred to as social engineer) uses social skills and psychological techniques (i.e. persuasion, deception, inspiring trust, exploitation of people's reactions in a certain situation) to obtain personal or sensitive information (which would then be exploited in the next phase) from the victim, to persuade the victim to take a certain course of action or to blackmail or threaten the victim. Social engineering is also often used in combination with classic "hacker" techniques (e.g. sending fake e-mails, redirecting to fake websites).

For example, attackers may use social engineering to convince or mislead the user to provide their e-mail access information, and this information is then used to illegally log into the user's mail account. Subsequently, they may take on the identity of the user for further deception.

Social engineering attacks consist of four steps. In the first step, the attacker attempts to gather as much information as possible on the potential victim. This includes both personal data and data on their information environment and the organisation itself (e.g. information on suppliers, customers etc.). This data is then used by the attacker in the second phase to establish and develop a relationship with the victim. At this stage, the attacker plays a certain role (e.g. they present themselves as a computer repairer, supplier representative) and seeks to gain the trust of the victim through the provision of information or knowledge obtained during the first phase. The third phase involves the exploitation of the established trust (e.g. tricking the victim into providing confidential information), and phase four involves using the data obtained to achieve the objective pursued. At this point, the life cycle of a social engineering attack can be repeated (the attacker collects additional data or broadens the attack, uses the collected data on a second victim, etc.).

Attackers use various methods for collecting data for social engineering. The simplest way is searching for data through internet search engines and social networks, but attackers can also use phishing (an act of misleading users, in which the attacker attempts to extract personal and other sensitive information from victims using false websites or e-mails), pharming (redirecting victims to false websites through DNS rerouting) and malware based attacks.

Some more direct approaches include social engineering by telephone (e.g. the attacker will call a company posing as a service provider or pretending to conduct a survey) and so-called vishing (voice phishing), where the attacker calls the victim by phone but modifies the call identification by replacing the real telephone number with another number (e.g. a supplier's or the true service provider's telephone number). Then there is also physical observation of the victim, so-called shoulder surfing. This can take place in public places (e.g. credit card payments, ATM cash withdrawals, etc.) as well as in business premises (e.g. when an employee logs on to a computer). A large source of information can be found by dumpster diving or *trashing*, which includes the examination

of discarded computer equipment and business documentation. Attackers may also plant infected storage media (flash drives, CD/DVD media, etc.), and there have even been cases where attackers physically broke into the company to install a backdoor to the organisation's ICT<sup>4</sup> infrastructure (for instance a wireless access point that enabled them access to the network, keylogger, malware, etc.).

However, users can fail security in other ways too, not just by manipulation. The problem is also carelessness, ignorance and negligence of users, not following security protocols and lack of knowledge and not developed security culture. This type of social reconnaissance attacks could be reduced by education and training of users.

However, a very special problem are cases where users are intentionally taking prohibited activities like sabotage, vandalism, theft, espionage, manipulation of hardware, software or information and performing unauthorized activities. A defence of insider threats in a form of rogue or disgruntled insiders (users) that are intentionally performing malicious acts is very hard and this is definitively not a problem that could be solved solely with technology. Technology (technical controls and proactive detection of abnormal user activity) and training of users definitively helps, however for mitigating these threats approaches like long term creation of trust and loyalty are also important.

---

<sup>4</sup> ICT – Information and Communications Technology is the infrastructure and components that enable modern computing.



## Actors who perform cyber attacks

Some define cybercrime as any form of crime involving computers and, more generally, information technology (IT). However, cybercrime is not only the use of information and communication technology for criminal purposes; an essential element of cybercrime is that it could not be possible without the use of technology, at least not to this extent.

Cybercrime differs from its traditional counterpart in three essential characteristics. First, it can be carried out remotely. Second, the identity of the attacker is relatively easily concealed or falsified. And third, tracking the information system that is the origin of the attack is not always possible, since attackers often employ methods like looping or weaving. In the latter, the attacker does not connect to the target system directly but through a number of other systems, possibly located in different countries, which prevents, or at least complicates, tracking them down.

The term "hacker" was coined by Joseph Weizenbaum in 1976 (Voiskounsky, Babveva and Smyslova, 2000: 57), and today it is popularly used to describe an individual possessing a lot of technical computer knowledge and using this knowledge to attack computer systems; this firmly places hackers within the realm of computer crime. Consequently, the term is presently associated with sophisticated illegal activities, although so-called "hacking" is more of a way of thinking rather than the methods employed to use these skills. White-hat hackers, or ethical hackers, who are information or network security experts, attempt to discover the shortcomings in the security of information systems of companies in a completely legal manner, using various attack methods. Ethical hackers use exactly the same methods as so-called black hat hackers, but the goal of the former is not to perform harm, but a security review and thorough analysis of the information system and to prepare recommendations to improve the security.

For organisations wishing to provide a higher level of security, it is therefore certainly reasonable to hire ethical hackers to run a security check or a penetration test (checking the organisation's security protection through simulated attack). Performing security checks on the organisation's key applications makes sense as well, and it can be performed by external or internal experts.

In some sectors, for example banking, such checks are mandatory. The internationally accepted security recommendations of the PCI-DSS (Payment Card Industry Data Standard - intended for organisations that directly or indirectly manage payment card information) provide that security checks (of different intensities) are to be carried out at least once a year or upon any major changes to the information system. The Standard stipulates that organisations are to conduct an internal and external vulnerability scan at least on a quarterly basis as well as thorough penetration testing following any major modification of the information system or annually.

The motives of cybercriminals in the past have been often the desire for discovery and self-expression, but today, most cyber-attacks are akin to traditional crime - carried out purely for profit. Some present-day cyber-attacks are also motivated by political activism (so-called hacktivism), and there have even been cases of cyberterrorism and cyber-sabotage. In recent years, we have seen the emergence of countries as actors in the

field of cyber-attacks. This resulted in an increase in information-intelligence attacks, carried out both for industrial espionage purposes as well as spreading political or public opinions and propaganda and military intelligence hacking. The final stage in this development are cyberwarfare and cyber war,<sup>5</sup> the elements of which could be seen in some traditional military conflicts as early as in 2008 in the Russo-Georgian war,<sup>6</sup> when Russia allegedly began a cyber-attacks on the Georgian IT infrastructure (government websites, news agency and radio, some industrial infrastructure, and others).<sup>7</sup>

However, the entry of state actors into the field of cyber-attacks, and the use of information-intelligence attacks for industrial espionage, is of particular concern to business organisations. Thus, the provision of information security for businesses is also becoming increasingly important from a strategic viewpoint.

---

5 The term war inherently refers to a large scale action, it is an actual, intentional and widespread armed conflict. Warfare refers to the activities of war in general. Cyber warfare includes techniques and tactics which may be involved in a cyber war.

6 The Russo-Georgian war was a military conflict between Georgia, Russia and the (Russian-backed) self-proclaimed republics of South Ossetia and Abkhazia.

7 The Russian government later denied the allegations that it was behind the attacks and stated it was possible that individuals in Russia had taken it upon themselves to start the attacks. (Markoff, 2008). However, the first-wave of cyber-attacks launched against Georgian media sites seems to be in line with military operations in Russo-Georgian war (Prince, 2009). There were also an estimates that cyber-attacks on Georgia (and also on Azerbaijan in 2008) may have been out-sourced to the Russian Business Network, cybercrime organization from Russia (Leyden, 2009) to create plausible deniability for the Russian government.



## Information system security basics

The provision of information security involves both technology and people (see above). It is important that we see this as a process. Technical solutions can only provide part of the solution. It is also important to adopt and implement appropriate security policies and to educate employees of basic security behaviour. Although education is one of the most important parts of information security in an organisation, it is often overlooked at the expense of automated technical solutions. In this context, it is important to remember that education must be continuous, as this is the only way for employees to acquire and maintain the appropriate competences to deal with cyber threats, as information technology is changing rapidly and new risks and threats are emerging in the field of information security.

Below we will look at some of the most important approaches to information security within an organisation, but similar approaches can also be used in private life.

### Basic approaches to providing information security

Today, the basics of information security primarily include regular software updates. This does not mean just the operating system but also all applications, software libraries and firmware on all devices, including peripherals such as Wi-Fi access points, routers, etc., as well as phones, tablets and similar devices. This is an area where great progress has been made in recent years, with operating system manufacturers regularly releasing security updates and increasingly pushing users to keep up-to-date as much as possible. Whereas in the past you had to go through a lot of trouble to install security updates, today you have difficulties to avoid installing security updates.

The basic building blocks of enterprise information security include the use of anti-virus and anti-malware software, but for virtually any organisation, the use of at least basic network security is worth considering as well. In addition to antivirus software, it makes sense to install Endpoint Detection and Response (EDR) software on computers. As mentioned above, these tools are installed on endpoint devices (PCs, laptops and mobile devices), not on the network, and are designed to detect and log suspicious activity and prevent cyber threats on these devices as well as to respond quickly to perceived potential security incidents.

It is also sensible to install applications to block online trackers<sup>8</sup> and so-called “junk removers” on end-user computers (these are applications which provide cleaning a computer system).<sup>9</sup> In order to increase privacy in the Windows environment, it is also worth considering blocking Windows telemetry.<sup>10</sup>

---

<sup>8</sup> Some of these applications or add-ons for web browsers are: Ghostery, Privacy Badger, Adblock Plus, uBlock Origin, Facebook Container, NoScript...

<sup>9</sup> Eg. Bleachbit, CCleaner in Windows, Onyx in Mac, etc.

<sup>10</sup> Blocking Windows telemetry on the PC is possible with applications such as Blackbird, WPD, ... or by blocking the

At the same time, it must not be forgotten that the preparation of appropriate security policies, also formally define security within the organisation and user rights, as well as systems for logging and monitoring compliance with established rules. This includes regular efforts to develop an appropriate security culture to equip IT administrators and users with the skills to identify cyber-attacks.

## **Provision of network security**

A firewall is the most important element of protection against network attacks. In principle, the use of a firewall can only be omitted if no application or service that receives connections from the network is running on a computer or other devices on the network. In all other cases, the use of a firewall is almost always sensible, as a conventional firewall puts only a minimal load on the system.

A firewall is basically designed to separate two network segments, and the rules defined in the firewall allow or disallow communication between two network nodes or two network segments. Although the firewall is responsible for limiting network connections, we should be aware that the firewall itself does not prevent all unwanted access to a computer. Access is still possible through applications that connect to the network or services running on the computer. If, for example, files and network resources are allowed to be shared on the computer, it is logical that the firewall will allow this type of access to a computer, while other access attempts will be blocked (if set). Thus, the firewall will provide a certain level of security, but unwanted access to the computer may still be possible through the misuse of the sharing of files and network resources.

It should be emphasized that it is not necessary to start communication from the outside to perform the attack. In other words, a firewall can block all attempts to connect from the network to our computer, but this does not guarantee that an attacker will not be able to connect to a computer. Even a very restrictive firewall will usually allow connections from a computer to the external network (otherwise it would not be possible to browse the web, etc.). This allows the attacker to set up a so-called reverse tunnel. An attacker can install a malicious application or send the user a web link that opens a communication channel from the victim's computer to the attacker. The attacker can then enter the victim's computer through this communication channel. Therefore, as part of network security, it makes sense to define firewall rules at the level of the individual applications.

In the context of network monitoring, it is worth to consider using tools to monitor internet usage (so-called parental controls) to block access to unwanted content (for instance pornography, phishing sites, malware distribution sites, etc.). At network level, it makes sense to consider the use of tools for scanning (and possibly also limiting) bandwidth usage (which can detect suspicious network activity) or an IDS/IPS system (so-called Intrusion Detection/Prevention Systems - these are solutions for the detection and/or prevention of network attacks). There are many open source and commercial solutions available on the market today that can enable us to protect our network against known threats in real time. There are also more advanced firewalls that use artificial intelligence

---

access to the telemetry servers directly on the network.

(AI) or machine learning (ML) to automatically adapt the rules or levels of network security.

## Passwords

Passwords are the basic and most used security mechanism, so passwords should generally be complex and long enough to provide the desired level of security. Like passwords, are 'encryption keys', which are protective mechanisms that are usually longer than passwords and have more entropy as they often involve randomly generated data. Passwords can also be stored in a file (for instance in a digital certificate) or on a special device (so called hardware tokens).

The problem with passwords is that complex passwords are difficult to remember, so when we are creating passwords, we are faced with the dilemma of whether we want more security or easier use. In the following, we will initially look at how to create appropriate (secure) passwords, the most common mistakes in creating passwords and how to save and secure a password in a simple and safe manner.

We can use several methods for creating passwords, but it is important that the password is as long as possible and as complex as possible (a mixture of letters and numbers, preferably a mixture of upper- and lower-case letters and numbers). We are of course talking about important passwords, e.g. password for access to encrypted data, password for access to email. At this point, we should also mention one-time passwords - these are passwords that can only be used once, after which they expire and are no longer valid.

When creating passwords, pay attention to the fact that when entering passwords, we can encounter different localization systems or different keyboard layouts. The *English Keyboard* does not contain your local language characters (for instance in Slovenian language we have characters like "č", "š" and "ž"), and some letters on the keyboard could be switched (for example, "z" and "y"), etc. When you start the system, the operating system does not yet have a default language set, so the *English Keyboard* layout is usually used at that time; entering a password containing the letter "z" may be different at start-up than later, when the system is already active.

When using passwords, it is also important to be aware of some of the security limitations of passwords. One originates from the ability of the system administrator to reset or recover the password (there are special schemes for recovering (forgotten) passwords, e.g. key escrow). Another possibility to consider is, that sometimes data could be accessed with forensic tools without a password. There is also the possibility of the existence of backup passwords (e.g. master key) to unlock the data. While password recovery systems are encouraged, it is important to be aware that these systems can also be abused. Which is just additional proof that security also involves people (loyalty and trust in the system administrators).

In some cases, "biometric passwords" are used to access the system. However, it is important to be aware that the use of biometric parameters for passwords is problematic, as biometric parameters cannot be changed or revoked, and there are known cases of biometric parameters being forged using relatively simple technology (e.g. fingerprint forgery). It is important that the identity ("Who are you?") and authentication ("How can you prove it?") of the user remain separate, which is not the case when using biometric passwords. Biometrics should therefore only be used for identification (as a substitute for a username), and the user is then authenticated with a password or key.

### ***Creating a secure password***

In the modern world it makes sense to use a special app - a *password generator* - to create a password. There are also different methods available to choose a more secure password. When choosing a password, it is not a good idea to choose passwords that are associated with the user or that contain dates, phone numbers or different sequences (letters, numbers or keyboard sequences).

Below we will see four possible methods for creating a password, but it is important that we do not use the same or similar passwords for different services. Initially, it makes sense to ask how important the password really is. If it is a password required by a web page, (e.g. for downloading a file), and we will never use the password or service again, it is, of course, pointless to create a very secure password. This is completely different with passwords for access to important internet services, encrypted data or access passwords for our user accounts.

The first method to create a password is to construct the password from a sentence, or the password is identical to a sentence. For example, we can use the sentence "This is my password". In this way, it is not too difficult to create a long enough password that can easily be remembered. We can also invent a (meaningless) sequence of words, e.g. "Mountains Sea Hill Valley". It also makes sense to use numbers and other characters, but it's good to keep in mind that you may need to enter your password on a keyboard with a different character layout than the one you used to create your password (e.g. one that has no characters for your local language).

The second method involves replacing certain letters in the password with numbers that visually resemble those letters. For example, "O" is replaced with the number zero, "L" with one, "A" with four, etc. Example: "th1s1smyp4ssw0rd".

In the third method, the password is assembled from the first (or second, or last ...) letters of the parts of text. For example, from "One, two, sky blue, all out except you", we get "otsbaocy". Of course, other combinations are possible (e.g. a combination of words and numbers), the only important thing is that the password is long enough and complex enough to be unguessable.

The fourth method is known as *diceware*. This is a method for creating passwords using a regular dice, which serves as a random number generator. The password is made up of several words, and to select each word, the dice must be rolled five times. This gives us a 5-digit number, which returns the word to be used for the password part in a separate table.<sup>11</sup> The words in the tables are chosen to be easy to pronounce and easy to remember, and the word tables are available for different languages. There are 7776 words in each language table ( $6^5$  - the dice returns values from 1 to 6, for each word the dice is rolled five times).

For example (in the case of English), "13554" returns "befall", "32425" returns "have", and "54244" returns "ski". The final password consisting of these three words would be "befallhaveski". The author of the *diceware* method, Arnold Reinhold, has recommended that the method should be used to choose a password containing at least six words.

---

<sup>11</sup> The tables for the different languages are available at <https://diceware.com> and at the <https://theworld.com/~reinhold/diceware.html>.

It is also important to remember that passwords must be sufficiently different from each other. For example, it does not make sense to use phrases like "This is the e-mail password", "This is the bank password", etc. An attacker who manages to reveal the contents of one password (e.g. on a forum) can quickly guess the system used to create the passwords and thus guess all the others.

There is very well known case of a security researcher Dan Kaminsky, whose computer was hacked in 2009 and whose passwords were later publicly disclosed. Kaminsky was using passwords created using the following system: "fuck.hackers", "fuck.omg", "fuck.vps", "fuck.mysql", etc. Once the attackers had discovered the pattern of passwords used to access a few systems, guessing the remaining passwords was much easier.

In short, passwords for access to encrypted data (e.g. encrypted disks, etc.) must be significantly different from passwords for access to less important online services and other systems.

The length of the password is important, because a password that is too short allows an effective brute force attack (guessing all possible combinations of letters and numbers) or dictionary attack (guessing passwords from dictionary words). There are a number of programs on the web that allow you to recover "forgotten" passwords, and these programs are very effective at guessing passwords that are short enough on modern computers. Password cracking can be greatly facilitated by modern GPUs (*Graphics Processing Units*). Graphics cards speed up password cracking by 50 to 100 times compared to conventional computers, and GPU password cracking can be parallelised (using multiple graphics cards to crack passwords in parallel). Modern graphics cards can check billions of passwords per second, and as computers evolve, the time it takes to successfully crack a password is only decreasing.

As mentioned earlier, the password should be as long as possible. The question is, what is the minimum reasonable length? The answer depends on the type of a password. If it is a password for accessing a system that has a time limit on password retries (e.g. is waiting after an incorrect password, and this waiting time may even increase for each subsequent incorrect entry) or if the number of attempts to enter the password is limited (e.g. in mobile phones, you can only try to enter the PIN three times, after which the SIM card is locked), the password can be shorter. But if the password is for access to our encrypted data that a possible attacker who physically obtains access to it will be able to try to decrypt infinitely many times, on a very fast computer, the password must of course be longer.

The quality of the password is measured by entropy (a measure for the randomness, or uncertainty of a message system). Entropy increases with the length of the password and depends on the character set used. While individual characters in the full ASCII set are considered to contain 8 bits of entropy, characters in the "normal" ASCII alphabet (upper- and lower-case letters, numbers, punctuation, etc.) are considered to have only about 5 bits of entropy. However, if you use a natural language text for the password, the password must be even longer, because the entropy of natural language is even lower due to grammar and word-building rules.

According to some estimates, English text has an average of about 1.2 bits of entropy per character (this is a conservative estimate), which means that for a really high level of



security, you need a password over 54 characters long (which achieves 64 bits of entropy). The level of entropy of Slovenian literary texts was estimated by Primož Jakopin. In his book, *Entropija v slovenskih leposlovnih besedilih (Entropy in Slovenian literary texts)*, published in 2002<sup>12</sup>, he estimated that average entropy of Slovenian literary texts is 2.2 bits per character. It follows that a password in the Slovenian language must be at least 30 characters long to reach 64 bits of entropy. Entropy measures for different languages are different. Estimates of how much entropy a password should have vary widely. The *Network Working Group Recommendation* from 2005, "Randomness Requirements for Security"<sup>13</sup>, states that passwords of low importance should have at least 29 bits of entropy, while those of high importance should have up to 96 bits of entropy. But this estimate is rather old, and some other estimates indicate even higher numbers. How the entropy is translated to password length depends on used character set. Password could be composed from numbers only or Latin alphabet, but it could also be alphanumeric (combination of alphabetical and numerical characters), case sensitive or case insensitive or even can contain some special characters (separators, etc.).

General advice would be that passwords should contain case sensitive alphanumeric and special characters and should be long at least 20 characters or more (preferably at least 32). Passwords that are very important should be even longer (45 or more characters long).

It is, of course, up to the user to decide what is a reasonable password length for a given password, as passwords also have a usability component – longer passwords are harder to remember.

### ***Typical errors when using passwords***

Typical mistakes when using sufficiently long and complex passwords are not storing them properly (e.g. on sticky notes on the monitor or under the keyboard) and password recycling, i.e. using the same passwords on different systems (if an attacker manages to break into one system and steal a poorly protected password, they will gain access to more protected systems). As stated above, passwords for access to encrypted data must be significantly different from passwords for access to online services and other systems.

Some password recovery systems are also problematic, e.g. authentication with known data (typical examples are "security questions" that allow password recovery, e.g. "name of your dog"), since the attacker could be able to discover this information using public available data or social networks.

Several studies have shown that guessing (inappropriate) passwords is a very effective attack, so we cannot stress enough the importance of using appropriate passwords. The passwords should therefore be long enough, include upper- and lower-case letters, numbers and symbols, not use sequences, not include any association with the user and passwords should not be recycled.

---

<sup>12</sup> Book has been published in Slovenian language.

<sup>13</sup> The text of the recommendation can be found at: <https://tools.ietf.org/html/rfc4086>.

Analyses of stolen passwords that subsequently circulated on the web showed that the most common passwords (globally) were e.g. password1, abc123, password, qwerty1, fuckyou, 123abc, iloveyou1, ... Research has also shown that 1000 roots of certain words (e.g. "letmein", "temp", etc.) in combination with 100 add-ons ("1", "abc", etc.) recovers about 24% of all passwords, and by taking into account personal data, dates of birth, etc., it is possible to guess as many as two thirds of all passwords within a month.

While it is true that password formatting patterns change over time, the following shows typical password formatting mistakes and of course, not changing your password is also a common mistake. A password that we suspect has been misused should be changed **immediately**.

### ***Changing passwords***

All systems that use passwords to authenticate users should also be able to change passwords. It is essential to change a password whenever we suspect that it has been disclosed to unauthorised persons or stolen.

Some organisations also have a security policy that requires users to change their password periodically (every certain number of days). However, such policies are being abandoned. If users are forced to change their passwords too often, users start choosing easy-to-remember passwords, or they start writing down their passwords, e.g. on a sheet of paper. This reduces security, so it's not surprising that a few years ago, both security experts and technology giants such as Microsoft started advising against enforcing policies of changing passwords periodically.

### ***Password management systems***

The first step to better security is to design passwords properly. Once we have well-designed passwords, we are faced with the problem of how to store them in such a way that they are not forgotten, or that an attacker is unable to get to them because of improper storage. Fortunately, the problem can be solved with some self-discipline and the use of password managers – special applications that serve as a repository for all our passwords, digital certificates and encryption keys. Such applications allow passwords to be entered in a special encrypted file, and can also attach files (e.g. digital certificate files or other encryption keys) in this protected storage. This file serves as a repository for passwords and is protected by a single password.

Today, there are many password managers available on the internet,<sup>14</sup> many of them free and open source. As mentioned above, passwords are one of the most important protection mechanisms, so they must be appropriate and their storage must be secure. Following the rules for creating appropriate or sufficiently secure passwords is therefore the first step in improving the security of our information and information systems. Safe and secure password storage makes it easy to use long and complex passwords and protects us from losing or forgetting passwords that we use less often. In addition, some password management systems help prevent attacks by logging keystrokes -

---

<sup>14</sup> E.g. Keepass, Lastpass, Bitwarden, Lesspass...

keylogging, as they allow you to fill in the password fields automatically, thus disabling keylogging via keystrokes on the keyboard.

Adequate backups of your password stores (if your password store is sufficiently protected needs to be ensured. It may also warrant consideration of uploading the password to a private cloud); however a password should be remembered for accessing your password storage.

### ***Advanced authentication systems***

The most common way to identify and authenticate a user today is through a combination of username and password. However, passwords have their limitations.

Recently, alternative authentication methods have become increasingly popular. There are other ways to authenticate that do not require passwords. One option is to use smart cards or hardware tokens containing a microprocessor and appropriate cryptographic mechanisms to authenticate or deny access to data. This method requires additional hardware and software (card reader, USB token<sup>15</sup>,...).

Another option is to use one-time passwords. In this case, for example, logging in to the system requires entering a new password each time. One-time passwords are created by one-time password generators, which can be hardware (a special device with a screen that displays a one-time password) or software (e.g. running on the user's mobile phone). One-time password generators are often used in combination with two-factor authentication (2FA) or multi-factor authentication (MFA). Two-factor authentication refers to authenticating a user by combining two independent components (factors). A typical example is a bank card, which requires a PIN number or the use of two passwords, one of which is a one-time password. The user will first have to enter their username and password (first factor), and then the login service will send an additional one-time password to their mobile phone (second factor), which they will then use to successfully log in to the system. Two-factor authentication or two-step login thus provides an additional layer of protection and significantly reduces the risk of intrusion. It is therefore recommended to enable two-factor authentication in all services that allow this type of login.

### ***Shared secrets***

As mentioned earlier, most systems, especially business systems, use one of the password recovery schemes. These systems are used in case the user forgets the password, but they also have their limitations. One of the main limitations is that these systems are prone to abuse (e.g. by a malicious system administrator).

A possible solution to ensure secure password storage or password recovery is called secret sharing or secret splitting. These are special methods of distributing encryption keys among multiple individuals, but these encryption keys are designed in such a way that multiple keys (but not all of them) must be used for access. So, we can create e.g. 10 different keys, and decryption may be possible with any three keys. These systems

---

<sup>15</sup> USB tokens are USB devices that work like smart cards. They are offering password management, encryption, two-factor authentication, and digital signing, but they do not need special card reader device. Instead, they can be inserted in universal serial bus (USB) connector.



are also called threshold cryptographic systems, where encryption keys are distributed among several entities (persons), and at least a certain number of these persons must participate in the decryption.

Secret sharing systems are useful in many applications. These systems can ensure that parts of the keys are located in multiple locations, making it more difficult for an attacker to steal them. Another option is to share responsibility between several people who are not fully trusted. For example, only the bank manager can unlock the vault in a bank, but if he or she is not available, three staff members can unlock it together. Other systems are possible as well, e.g. one general can be replaced by ten soldiers (vault could be unlocked by one general or, if he is not available, by ten soldiers), etc. With the help of a cryptographic secret sharing system, it is possible to set up a system to keep our passwords and encryption keys safe in case of accident, death or unavailability of key users.

## Physical security

Physical security is ensured by physical protection (alarm devices, video surveillance, etc.) and by controlling and recording physical access to the key parts of the information system. Physical security of portable electronic devices is also considered the most important measure to prevent data theft or misuse.

There are also some additional measures, both appropriate software and certain hardware, to make unauthorised access to the system even more difficult in the event of physical access. An important element in preventing unauthorised access to information is both the encryption of data media and the implementation of procedures for the permanent deletion of data from data media or the appropriate destruction of data media (e.g. commissioned destruction, etc.). Discarded computer components containing data carriers (e.g. hard drives, mobile phones, etc., as well as internal data storage on different peripheral and IoT devices) may contain sensitive data that can be misused.

One of the attackers' techniques in the case of physical access is to install a keylogger, a device that can record or intercept the user's keystrokes (e.g. when they enter the password). Such devices are relatively inexpensive and attackers can build them themselves.<sup>16</sup> The attacker simply plugs the device between the keyboard and the computer, and the device then stores (and, if wireless, transmits) all the user's keystrokes on the keyboard. While older keyloggers could be detected visually, modern ones are so miniature that they can be hidden in a cable. There are also software keyloggers, which are special (malicious) applications that intercept keystrokes. These applications are also available for mobile phones. While it is possible to protect against hardware or software keystroke interception by using the on-screen keyboard, this protection works if the attacker is not recording the content of the display.

Similarly, we need to be careful when installing different applications, as some of them may have "dual function" - in addition to the basic function, they can also be implemented to steal data, allow remote access, etc. It is also a good idea to be careful

---

<sup>16</sup> Some of the most known commercial devices with these abilities are *Rubber Ducky* (it is keyboard emulator) and *Bash Bunny* (keyboard, Flash drive, Ethernet adapter and a serial device emulator). However, there are several open hardware projects with detailed instructions how to build similar device for a couple of Euros.

when connecting unknown devices, such as "found" USB sticks or similar devices that may contain malicious code that can be planted on your computer when you connect the device.

The next more well-known attacking technique is the execution of an evil maid attack. An evil maid attack is an attack on an unattended device, in which an attacker with physical access alters it to get access to the device, or the data on it later. Usually, this type of an attack is used to physically access a computer with encrypted disks, booting the computer using a USB stick or CD<sup>17</sup> and installing a software keystroke logger on the boot sector of the hard disk. In 2009, well-known information security expert Joanna Rutkowska demonstrated a practical evil maid attack on a computer fully encrypted with the well-known *TrueCrypt* encryption program. She developed a special program that slightly changes the original *TrueCrypt* program code, which asks the user for a password. The changed program code intercepts the typed password, stores it in a particular location on the disk and then passes it on to *TrueCrypt*. The special application can then be used to extract the stored password the next time the computer is physically accessed, thus bypassing encryption protection (Rutkowska, 2009).

According to some media reports, this is how the Israeli secret service obtained the access to the data on a computer of a Syrian diplomat who had left his computer unattended in a hotel room in London in 2006 (Gardham, 2011). The data obtained that way had proved that Syria was building the secret Al-Kibar nuclear facility in the desert (in IAEA documents it is also referred as Dair Alzour). The nuclear facility was subsequently bombed in Operation Orchard (also known as Operation Outside the Box) on 6 September 2007.

The evil maid attack can be defended against using smart cards or hardware tokens, which contain a microprocessor and a digital certificate that unlocks access to the data. Of course, in this case, we need to ensure that the smart card itself is properly physically secured. Protection (at least in part) may also be implemented using embedded (BIOS) hard disk encryption and the use of the TPM module (Trust Platform – this is a computer-integrated crypto-processor designed to secure the storage of encryption keys). A third option is to boot the computer from trusted removable media, but this is less useful in practice.

It is important to be aware that security of access to all output devices, especially printers and displays, must also be considered. Particular attention should be paid to network printers, where data transmission from the computer to the printer is generally not encrypted, and modern printers (especially larger multifunction devices) have built-in data storage on which documents in the printing queue are stored. This memory can be removed from retired (or stolen) printers, and the latest documents that were printed on this device can be reconstructed from the memory with relatively simple digital forensic analysis techniques. It should also be noted that modern printer servers are usually storing logs about the documents that have been printed (e.g. which user printed them, from which computer, the number of pages, the document title, etc.), but in some cases they also store the entire content of the documents that were sent to the printer for printing.

When using a laptop in public places (e.g. in a café, airport, etc.), physical security is even more difficult to ensure, as the content of our screen can be seen by all (random)

---

<sup>17</sup> CD stands for Compact Disk, a digital optical disc data storage format.

passers-by. Polarising filters are an interesting solution to this problem, providing at least some protection from the prying eyes of people in the vicinity of your computer (or mobile phone) screen. These filters are sold as “privacy filters”, and when placed on the screen, they block the view of the screen from the side. If you look directly in front of the screen, the image is visible (although the light transmission is reduced by about 40%), but if you look at the screen from an angle, the content is invisible or at least heavily obscured.<sup>18</sup> As mobile phones are becoming more and more important attack vector, buying polarising (privacy) filters for mobile phones should be considered.

There are some attacks that require the physical presence or proximity of a computer, but these are more difficult to implement in practice or require quite specialised equipment. One such attack is the Cold Boot attack, which can be used to reconstruct the contents of the working (temporary) RAM memory<sup>19</sup> from a shutdown computer and e.g. gain access to encryption keys, and another is a tempest attack - this involves intercepting and reconstructing the electromagnetic signals (allowing, for example, the reconstruction of the display on a computer screen) emitted by computing devices into space.

But it is also important to remember that physical security must be provided to the network as well. If an organisation provides free Wi-Fi connections to its visitors or even complete strangers, it must ensure that users of such a Wi-Fi network cannot access the organisation's network where company computers or even servers are located. It is necessary to pay attention to multi-user environments, as users with lower privileges can use so-called escalation of privileges to gain unauthorized access to parts of the system that are otherwise inaccessible to them.

### ***Tempest attack***

Tempest (*Transient Electromagnetic Pulse Emanation Surveillance Technology* or *Transient Electromagnetic Pulse Emanation Standard*) is a method of intercepting temporary electromagnetic signals. While the method has been known since the middle of the last century, there is very little published research in the field. Tempest attacks are based on the fact that computer or electronic devices emit electromagnetic signals into the environment, and these signals can be intercepted and "reconstructed" in the vicinity of the attacked device. The first publicly published paper on tempest was by Dutch researcher Vim van Eck in 1985, hence the terms Van Eck Snooping or Van Eck Phreaking are also used for this eavesdropping technique. The term "tempest" is therefore sometimes used as a synonym for unwanted electromagnetic radiation that spreads in an uncontrolled manner and allows sensitive data to leak out. The protection against this type of interception of information is called emission security or EMSEC.

Most electronic equipment inadvertently emits electromagnetic interference (EMI)<sup>20</sup> emanations. The electromagnetic signals emitted by the monitor, keyboard, hard disk and other electronic components of a computer or other electronic device can be

---

18 Recently some laptop manufacturers started to sell laptops with built-in polarisation filters. They are marketed as laptops with privacy screens.

19 RAM memory – Random-Access Memory is a form of computer memory that can be read and changed directly. Typically is used to store working data and machine code.

20 EMI – electromagnetic interference.

intercepted and reconstructed by special devices from a distance of a few dozen to a few hundred metres in such a way that an attacker can see the image on the monitor, which keys the user is pressing, what data is being written to the disk, etc. Data from EMI emanations can be also leaked through power lines.

This way the passwords or unencrypted data can be intercepted before they are encrypted in the computer. However, the eavesdropper does not need to have direct physical access to the device being eavesdropped on, as it is possible to carry out a tempest attack remotely, even up to 1 km away (under ideal conditions) according to some studies. While a tempest attack requires quite specialised equipment, in recent years this equipment has become more widely available, so it is not surprising that security researchers were able to break the secrecy of Dutch voting machines in 2006 and Brazilian voting machines in 2009 (the machines that allowed the casting of an electronic ballot at the polling station) with a tempest attack.

Protection against tempest attacks on classified information in the field of national security is usually required by the legislation regarding the protection of classified information. This legislation requires that devices handling classified information marked as “CONFIDENTIAL” or higher must be protected against tempest attacks. There are also some international standards on tempest protection (so called shielding standards), the most known are NATO<sup>21</sup> standards. Most of those standards are classified, however, some of their elements are publicly available.

There are some technical solutions for tempest protection, but not all of them are appropriate. Transmitting interfering signals is not useful in practice. The most used solutions include metal shielding. This creates a Faraday cage around the device to prevent electromagnetic signals from “leaking” into the surroundings. The protection must also include appropriate modifications to the device's power supply, as electromagnetic signals may also leak into the surrounding area through power sources.

It is now possible to buy special tempest-certified computers on the market, which are properly shielded and made of specially designed electronic components that reduce tempest leakage. There are also solutions for shielding a whole building with metal (or to build so-called safe rooms) to prevent information leakage. These solutions are also available for the private sector and are quite affordable today.

Leakage of tempest radiation can be reduced by using shielded cables, which should be as short as possible, and by installing filters to reduce electromagnetic interference, also known as EMI filters.<sup>22</sup> However, there are also some programming solutions based on the use of specific tempest prevention fonts. These fonts are designed in such a way that the reconstructed image is blurred by the tempest attack. These techniques do not completely prevent a tempest attack, but they do raise the threshold of difficulty of carrying out such an attack.

---

21 NATO – North Atlantic Treaty Organization is an intergovernmental military alliance between 27 European countries, 2 North American countries, and 1 Eurasian country (as the situation is in 2022).

22 EMI filters, also called EMI suppression filters can be used to protect against the impacts of electromagnetic interference by suppressing electromagnetic noise transmitted through conduction and/or noise from grid power.

## Backup

The primary task of backup is to make copies of data that can be restored in the event of a hardware failure, hacker attack (e.g. by crypto-viruses), user error (e.g. deletion or overwriting of data) and other similar events. The loss of critical data may cause serious financial problems for an organisation. Operational interruptions lasting more than ten days may have permanent consequences for the organisation's operation. The problem is not only the permanent loss of data but also the damage caused by the interruption of work or the business process. Therefore, along with the implementation of backups, it is important to also have a disaster recovery plan in place.

Backups can be performed manually (on demand) or periodically. As it turns out, humans are not very consistent when it comes to manual backups. So it makes the most sense to automate the backup process. There are several backup strategies. The first is the full or mirrored backup, where each backup covers all the selected data.<sup>23</sup> The advantage of this approach is that the updating of data is faster, but, on the other hand, the creation of a single copy is more time-and space-consuming. Such archived data can be either compacted (to save space) or encrypted (to protect data from unauthorised access).

The second strategy is incremental backup, where each backup includes only the data that has changed since the last backup. This strategy is less time and space consuming, but it is more time-consuming to recover the data. Also, if one of the increments fails, the data cannot be restored correctly, as the first (full) copy of the data as well as all the differences (increments) are needed to restore the image. The longer the period between the full copy and the copy we would like to restore, the more incremental copies (so called increments) are required.

The third strategy is differential backup. It operates by backing up the modified data between the full copy and the current state. In the case of restoring, we only need the last full copy and the latest copy (or the copy we want to restore). This type of archive is safer and faster than an incremental one but slightly more space consuming.

As outlined above, it makes sense to compress and consider encrypting the data in a backup archive. We could also use deduplication, the process of eliminating duplicates, which helps us to reduce the amount of storage space used. When implementing backup archiving, it is important to consider making backups not only of important data but of the entire system (including operating system and installed applications), so that in the event of a major failure, the system can be restored to its original state more quickly.

An important question is also where to store the data. The most obvious option is of course to store it on an external data carrier (such as a portable drive, or a dedicated NAS device<sup>24</sup>), but to improve security, we should also consider the creation of a backup copy to an external location, or better yet, on several external sites. One option is also to store backup data in a cloud, however, it is very important to understand that data in the cloud are not under our control and therefore consider using the encryption. Use of cloud

---

<sup>23</sup> Please note that solutions like RAID can provide enhanced data protection, however it should not be considered as a backup! (RAID – Redundant Array of Independent Disks is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both.)

<sup>24</sup> NAS – Network-Attached Storage is a file-level data storage server providing data access to clients over the computer network.



computing also entails a certain dependency on the service provider (which can even lead to a so-called "vendor lock-in"), and the availability of data in this case also depends on the availability of the cloud. This does not mean only possible cloud service failure, but also possible internet connection failure. So, the use of cloud services should be subject to serious consideration and maybe used for a secondary backup location because the cloud infrastructure could be prone to failure too.

In the case of emergency, it is important, that backups are quickly available. Usually this is achieved with local backup. But in case of some disaster event (fire, flood, quake, other) original data and their local backup could be damaged. In that case an external copy of the data could be a lifesaver. Therefore, it is a good strategy to implement the local backup (for instance in a NAS located within the organisation), and from data are then archived to external location. Devices such as laptops that employees carry with them or use when working from home, can be backed up via a VPN<sup>25</sup> connection.

The so called "Rule 3-2-1" describes what should the good backup strategy be. It explains as: there should be 3 copies of data, on 2 different media, with 1 copy being off site. The rule was later upgraded to the "3-2-1-1-0 rule", which explains there should be 3 copies of data, on 2 different media, with 1 copy being off site, with 1 copy being offline, air-gapped or immutable and with 0 errors by regular verification (Vanover, 2021).

Several solutions are available on the market today for the implementation of backups. Nevertheless, the creation of a good system for backups requires consideration and smart organisation. It makes sense to implement an automatic solution that allows multiple versions of data to be stored. It also makes sense to store important data in multiple locations, and if data is stored externally (especially in the cloud), it should be protected with encryption. It is also necessary to ensure that, in the event of an emergency, the data are available and can be quickly restored. Therefore, it is not enough simply to just implement a backup solution, but it is crucial that performance and reliability of backups is verified in practiced regularly.

## Encryption

Encryption is the process of encoding information (text messages, files, speech, video, etc.) into a form that cannot be understood by unauthorised persons. Cryptology is the science concerned with secure data communication and secure storage of data. It encompasses both cryptography, which is dealing with encryption and obscuring the content of data, and cryptanalysis, which is dealing with revealing of encrypted data. Cryptography can therefore be used to prevent communications from being eavesdropped on, while cryptanalysis is concerned with breaking encrypted messages.

In encryption, content (sometimes called plain text) is converted by an algorithm and a password (key or passphrase) into a form that is difficult or impossible to reconstruct back to its original form without the password (sometimes called cipher text). Strong encryption is therefore the most effective way to protect the content of messages, files, etc. from unauthorised access. In addition to enabling privacy, modern cryptography protects our financial transactions, secures our data on storage media and in the cloud

---

25 VPN – Virtual Private Network.

and enables digital signatures and integrity checks on data and software. In some cases, we are also legally obliged to protect certain categories of sensitive data with encryption.

Alongside cryptography, we should briefly mention steganography. It is a set of methods for hiding messages that enables us to share messages that are hidden in other files or other messages, implement so called invisible encryption, electronic watermarking and marking files with electronic serial numbers. Steganography methods can be used in both the physical<sup>26</sup> and digital environment. In combination with cryptography, steganography enables the implementation of plausible deniability - plausibly deniable encryption. Typically, this is used for concealing encrypted data into other encrypted data. From user perspective works the following way. The user has two encrypted keys: one unlocks the basic encrypted data, while the other unlocks the hidden encrypted data. This is particularly useful if the user is forced to disclose their encryption keys – in this case, they disclose only the first key, thereby not giving access to the hidden data. Plausible deniability and steganography systems are therefore especially useful for those living in non-democratic countries.

It should be noted that cryptography is not all-powerful. Cryptographic implementations can be attacked through weaknesses in cryptographic algorithms or weaknesses in the implementation of these algorithms. More frequent are attacks on cryptographic keys and passwords and indirect attacks on cryptography (channel side attacks). However, security problems often arise because individuals do not use the cryptography in the proper way. The security of a cryptographic implementation depends, in a narrower sense, on the cryptographic algorithm used, and the length of the encryption key or the password adequacy used for encryption. In general, using encryption keys is better for security, because key could be longer and contain more entropy. But using passphrase is usually much easier. We can also use a special hardware – a smart card – which can be used to easily unlock encrypted data.

Since access to encrypted data depends on a password (or a smart cards), we need to make sure not to lose them. So, when using encryption, it is essential to introduce appropriate mechanisms for revoking lost passwords and to securely restore access to the data user loses their password or a smart card.

### ***Transport-level encryption and end-to-end encryption***

Regarding the implementation of encryption of the communications, two concepts apply. One is to use encryption at the data transfer level where the message is encrypted only during transfers between different servers (but not on the servers). In this case data at the target server is decrypted and then stored on a server or forwarded to another server (in that case it could be re-encrypted, but with different key). The second concept is encrypting the entire communication path. This concept is also known as end-to-end encryption (E2E). Here, an encrypted session is established between each endpoint (e.g., two communication terminals), which means that communications are encrypted along the entire communication path from user A to user B. Therefore, they cannot be eavesdropped by the network infrastructure provider or by the communications service provider (however, it could be intercepted at the source or target endpoint).

---

<sup>26</sup> For instance, some laser printers print a sample of small yellow dots on each printed paper sheet, the layout of which contains information about the printer serial number and the date and time the document was printed.

Using the example of e-mail, the use of transport-level encryption involves the email client establishing an encrypted communication session to the mail server over which outgoing email is transferred. However, this mail is stored on the server in an unencrypted format. If the e-mail needs to be forwarded towards other servers, this server then establishes a new encrypted session to the next server through which it forwards the e-mail. And so on, to the destination server. In this case, the electronic message is encrypted during the transfer, but an attacker who has access to one of the interface servers will be able to read the message (including traffic data).

Using end-to-end encryption, the email example would mean that user A's message would be encrypted for user B. The message is encrypted the entire time it is transmitted from one user to another and is also stored in encrypted form on all intermediate servers. The message can be decrypted and its contents viewed exclusively by the final recipient. In this case, eavesdropping on the intermediate infrastructure is not possible, but the intermediate servers can record traffic data - who is communicating with whom, when and to what extent.

### ***Man-in-the-middle attack***

One of the more common attacks on encryption is the man-in-the-middle attack (MITM), where the attacker impersonates both communication partners to intercept their encrypted communications. MITM attack can also be carried out between the client and the server, e.g. web browser and web server.

In a man-in-the-middle attack, the attacker first places himself between the two communication partners (e.g. between the client and the server), where he intercepts the communication between them. He then starts to spoof both - presenting himself to the server as the client and to the client as the server. In this way, the client establishes an encrypted connection; not to the real server, but rather to the attacker's fake server. The server also establishes an encrypted connection; not to the real client, but to an attacker impersonating the client. At this intermediate point, the attacker decrypts the traffic and thus gains insight into the content of the otherwise encrypted communication.

A man-in-the-middle attack can be prevented by checking encryption keys or digital certificates, for which several techniques are available. On the web, this is done by digitally signing server certificates from trusted certificate authorities (CAs) or by setting up a so-called web of trust, but there are also other technical solutions, e.g. digital certificate pinning, Trust On First Use / Persistence Of Pseudonym (TOFU/POP), etc. Modern browsers are designed in such a way that they try to detect several MITM attacks and they warn users of potential risks regarding expired, self-signed or improper certificates.

There are several techniques for performing MITM attacks, for instance *IP<sup>27</sup> spoofing attack*, when an adversary masks their identity by presenting themselves with the IP address of a legitimate device, *DNS spoofing* (also called *DNS poisoning*), where adversary intercepts DNS request and returns the address that leads to its own server

---

27 IP – Internet Protocol, IP address is a unique address that identifies a device on the internet or a local network. IP addresses serve two functions: network interface identification and location addressing.



instead of the real one, *HTTPS<sup>28</sup> spoofing* (also known as *homograph attacks*), where attacker registers a domain name that is similar to the target website (and also *SSL<sup>29</sup>* certificate to make everything look more legitimate). This attack exploits a Punycode standard that enables the registration of hostnames that contain non-ASCII characters. Other techniques for performing MITM attacks include *Man in the Browser (MITB)*, where an attacker is compromising a web browser used by the user to perform eavesdropping, changing the displayed content, perform data theft, etc. By *SSL stripping*, an attacker downgrades the communications between the client and server into unencrypted format and then intercept (and possibly modify) communication. Attackers can also use *session hijacking* (sometimes called *browser cookies theft*), where an attacker steals the user's session token (cookie) and uses it to access the user's account. There is also a special type of MITM attack where an attacker hijacks or spoofs email to perform further attacks.

This all means that just using encryption does not guarantee the adequate level of security. Encryption should be used the correct way and user should have some basic understanding of security to avoid potential risks.

### ***Encryption of e-mail and internet communications***

We often exchange confidential information via email. Since technically email is more like a postcard than a sealed envelope, encrypting email messages would make perfect sense. However, for historical and partly technical reasons, encryption of communications has not taken hold in the field of email. There are two main protocols used for encrypting email, OpenPGP and S/MIME (Secure/Multipurpose Internet Mail Extensions), which, in addition to encryption, also provide sender authentication and digital signing of messages and allow end-to-end encryption. Unfortunately, they are quite rarely used in practice.

Alternatively in the world of email, transmission level encryption is now much more widely implemented. This includes mail clients connecting to mail servers using an encrypted connection, even though the exchanged email messages itself are not encrypted. It is therefore, recommended to check with your email service provider whether it supports and enables encrypted protocols. If your organisation has its own email server, it is best to enable only encrypted connections (and completely disable unencrypted connections) to the server.

It is also reasonable to implement a security protocol for the verification of the authenticity of e-mail (SPF - Sender Policy Framework, DKIM - DomainKeys Identified Mail, and DMARC - Domain-based Message Authentication, Reporting & Conformance). These protocols make it much harder to send spoofed or phishing emails and thus to implement so-called director's fraud. The latter involves attackers sending a fake email

---

28 HTTPS – Hypertext Transfer Protocol Secure is an extension of the Hypertext Transfer Protocol, which is the primary protocol used to transmit data between a web browser and a website. HTTPS is encrypted, which increases security of data transfer over the Internet.

29 SSL – Secure Sockets Layer is a cryptographic protocol designed to provide communications security over a computer network. It is deprecated from 2015 by TLS – Transport Layer Security, which is also a cryptographic protocol designed to provide cryptography, confidentiality (privacy), integrity, and authenticity through the use of digital certificates, between two or more communicating computer applications.

to the company's secretarial or accounting email address from the CEO,<sup>30</sup> instructing them to transfer money to a specific transaction account. This is termed spear-phishing, where the attacker carefully examines his target and then uses this information to assume the identity of a person important to the organisation (CEO, supplier, etc.) and then executes the attack.

If an organisation owns or manages its own e-mail server,<sup>31</sup> it is a good idea to install antivirus and anti-spam filters. It is also good to consider implementation of disk encryption on a server to protect the e-mails in the event of physical theft or physical access to the e-mail server. However, encryption has gained significant traction in online communications in recent years. More and more websites are available exclusively over HTTPS connections, and the use of encryption is also increasing by using other communication protocols. It is advisable to enable support for HTTPS connections for all websites, or even better, mandatory use of it. Organisations that use HTTPS on their websites (even if website does not contain any sensitive information) are outwardly showing that they care about security. In addition, modern web browsers are marking web sites without HTTPS as insecure, and the use of HTTPS also affects the ranking of a website on search engines, which means that it ultimately affects the visibility of a company online.

The concept of end-to-end encryption is also gaining ground also in interpersonal communication, especially in instant messaging and voice and video communication over the internet. Currently a major development in the implementation of end-to-end encryption is being held in group communication.

### ***Encryption of mobile communications***

The emergence of smart mobile phones has made strong encryption of instant messages, voice and video communications easily accessible to a wide range of ordinary mobile users. With the help of Android and iOS apps, we can keep our mobile communications well protected from interception.<sup>32</sup>

The first devices for encrypting voice communications were developed during World War II. They were hard to use and the devices were colossal. First such a device, called *SIGSALY* used by United States military to encrypt voice communications, weighed 55 tonnes, and filled a medium-sized room (Boone, Peterson and United States. 2000). Today, we can see how quickly technology is evolving, since we can have a much more powerful devices for encrypting voice communications literally in our pockets.

In addition to appropriate encryption protocols for secure exchange and authentication of encryption keys, it is important that such applications also use appropriate codecs for

---

30 CEO – Chief Executive Officer or managing director.

31 It should also be noted that biggest e-mail providers are marking e-mail messages as spam, if it is coming from mail servers which do not have the proper implementation of SPF, DKIM and DMARC security protocols and PTR records. DNS PTR record is used for reverse DNS lookups. It matches domain names with IP addresses and is therefore a security tool that mainly helps to check if the server's name is associated with the IP address from where the connection was initiated.

32 There are several applications for secure communications but regarding the security model, used cryptography, implementation and operating, Signal application could be recommended (Signal is also open source and free).

audio compression. Choosing inappropriate codecs can present a security risk, as it can enable eavesdropping even if encrypted data transmissions are used. Researchers has shown that when using encryption with voice streams compressed using variable bit rate (VBR) codecs, the length of the compressed data packets depend on the characteristics of the speech signal. In other words, different sounds are encoded differently, and these small variations in packet sizes can be observed, and that could be used to reconstruct (“decrypt”) encrypted data (researchers have shown that the lengths of encrypted VoIP<sup>33</sup> packets can be used to identify the pre-recorded phrases spoken within a call). Additionally, applications for encrypting mobile communications need to solve a number of technical problems (e.g. network latency problems, echo cancellation). In all this, however, these applications must also ensure the best possible user experience without compromising security.

It is therefore fundamental to understand that securing mobile communications is a complex process, among the many apps that advertise themselves as impenetrable, it is important to choose one that does more than just provide security on paper. When selecting security solutions, it is therefore a good idea to consult the relevant experts rather than simply trusting the vendors of the solutions they offer.

### ***Encryption of data media***

To protect the data on your computer from unauthorised misuse or access, it needs to be encrypted, which is particularly important in case of loss or theft of mobile devices or external storage devices. With today's technology, it is very easy to encrypt data media (e. g. disks, thumb drives, etc.), and it is also very easy to encrypt an entire operating system or computer. Encryption options are already embedded in all modern operating systems. For example, BitLocker can be used in a Windows environment, *LUKS* in a Linux environment and *FileVault* in a Mac environment. Also, internal storage encryption is enabled by default on most modern mobile phones, some of them even do not have an option to disable internal storage encryption, which is a very good from the privacy standpoint.

As the use of encryption can lead to data loss in the event of a data carrier failure or malfunction, it is essential to ensure that adequate backup strategy is implemented. The importance of backup when using data encryption cannot be stressed enough.

### **Wiping data**

As outlined above, physical access to data media is one of the major risks of unauthorised access to data. The best solution is to encrypt the entire data carrier, but if this is not possible, the data that we no longer need should be overwritten or wiped. Normally, the deletion of data does not, in fact, erase them permanently. In principle, deleted files (including those removed from the so called *Recycle Bin* or *Trash* – a place where deleted files are temporarily stored unless they are permanently deleted), can be recovered relatively easily by digital forensics techniques. If a file is to be deleted

---

33 VoIP – Voice over Internet Protocol, also called IP telephony, is a group of technologies for the implementation of voice communications and multimedia sessions over Internet Protocol networks.

permanently, its contents must be overwritten with other data. That is not always an easy and reliable task. In certain circumstances, the content of overwritten files can also be (at least partially) restored by forensic analysis.

Several options or methods can be used for overwriting data intended to be permanently deleted. The simplest method is to overwrite the data with zeros only once. A slightly better method is to overwrite with random or pseudorandom data, preferably multiple times. There is also the option of deleting using a low-level format, but this method is not reliable.

If a hard drive contains sensitive data, it is best to use multiple overwriting passes using special methods where the overwriting is done in a specific pattern. The best known is the *Gutmann method*, which requires 35 overwrite passes following a specific pattern, but there are others as well. Therefore, when selecting software applications for overwriting or wiping data, it is a good idea to find out what erasing methods are supported by the application and choose one that follows established standards.

When overwriting data, we can choose to overwrite the content of files, overwrite the free space (space that is not occupied by the file system but contains the remains of deleted files), overwrite slack space (space that the filesystem occupies on disk but is not used; slack space is particularly problematic in the FAT file system<sup>34</sup>), overwrite the contents of the swap space (space that holds data that used to be in RAM and may include passwords and encryption keys) or overwrite the contents of the entire storage medium. The best option is the latter, if feasible.

It is important to remember that permanent deletion of only the content of files in journal file systems is not easy and above all not reliable. Permanent deletion of data on network file systems or in the cloud is even more unreliable. Deleting the contents of files is also unreliable if disk defragmentation has been used before deleting. In all these cases, the data are not located in one place on the data medium but (possibly) in several places. Some file systems even have implemented so called snapshot technology and they can keep several previous versions of files.

Modern disks also contain certain reserved sectors where data may be stored (namely Host Protected Area (HPA) and Device Configuration Overlay (DCO), which are used for hiding sectors of a hard disk from being accessible by the end-user). Specific approaches are therefore needed to delete data in these spaces.

When we talk about wiping data, we should not have in mind only computer disks. Sometimes data on mobile phones,<sup>35</sup> SD cards<sup>36</sup> or other media should also be wiped.<sup>37</sup>

In view of the above, the best way to protect data is through encryption. If this is not possible, it may be a good idea to use one of the wiping methods to erase the data on the device you are planning to sell or dispose of. In addition, it is necessary to emphasize that devices containing data are not only computer hard drives but also

---

34 FAT – File Allocation Table is a file system developed for personal computers in 1977, however later was adapted and extended and it is still used nowadays.

35 Data on a mobile phone after factory reset could be recovered. For completely wiping the data from your mobile phone check for data erasing options or protect data with encryption.

36 SD card – Secure Digital non-volatile memory card.

37 Data on non-erasable media such as CD, DVD (Digital Versatile Disc) and other could be destroyed by physically destroying the media, for instance by shredding.

various peripherals (e.g. printers). Many of these devices have built-in features that allow permanent deletion of all data in the internal data storage. For business organisations, it makes sense for their IT system administrators to check how data on these devices can be deleted and to perform such deletions periodically or at least when the device goes out of service or out of use.

## VPN networks

Many organisations, especially those that are moving towards more home working, want their business information system to be accessible to remote users (e.g. for employees working from home or on business trips). This can include the use of Virtual Private Networking (VPN) technology, which allows us to connect different networks or computers securely using (usually encrypted) tunnels. Through such a tunnel, users can access a remote network or remote servers in a similar way to being physically present on the corporate network or even redirect all internet traffic from a remote computer to the organisation's network through the tunnel. VPNs are also used to circumvent regional access restrictions (e.g. video or other content that is not available in one region, but can be accessed via a VPN connection from the other region) to avoid censorship and to connect securely to the internet via unsecured network connections (e.g. wireless networks). In the latter case, VPN server acts as a secure gateway to the internet.

There are several types of VPNs. Some are simply used to connect remote computers to an internal network, while others can connect entire networks to each other. Some VPN connections allow networks to be connected at the data link layer (this is known as the 2<sup>nd</sup> layer of the OSI model<sup>38</sup>) and some at the network layer (3<sup>rd</sup> layer of the OSI model). Through VPN connections, the organisation can provide its employees an access to the internal IT system or internal services of the organisation – e.g. application servers, NAS servers, printers, etc. In short, through VPN remote authorized users can gain access to all those services that are not accessible outside the organisation. There are several different VPN solutions available today. When implementing, it is necessary to pay attention to security as well as throughput (the volume of traffic that can pass through a VPN). We also should not forget about ease of use for both users and maintainers. Certain VPN solutions have complex configuration, and this can lead to mistakes by IT support personnel.

The fact that VPNs are blocked on some networks can also be a problem. While this usually does not apply to public communications networks used by employees at home, restrictions can be encountered in hotels, cybercafés and abroad (especially in non-democratic countries). It therefore makes sense to consider using remote access solutions that are more difficult to block at network level or to use a solution that allows so-called obfuscation (hiding) of VPN connections.

For remote access, it is of course important to protect access to the core network as well as to implement network segmentation within the organisation. This could be accomplished with a firewall, which can be used to set up general network access rules

---

38 OSI model – the Open Systems Interconnection model is a conceptual model that characterises and standardises the communication functions of a telecommunication or computing systems.



as well as specific rules for access to individual parts of the network. Sometimes it makes sense to use an intrusion prevention system that protects computer network from brute-force attacks by dynamically adjusting firewall rules according to multiple failed connection attempts or network traffic analysis.

It is important to mention that transparency and trust are vital in the VPN industry. While the technology is important, it is also important to know how well is VPN infrastructure protected and is it maintained regularly?

While several VPN solutions for so called “safe browsing” are advertised on the Internet and through social media, we should be aware that these solutions are generally not suitable for organisations, especially if organisation wants to connect their endpoints (computers and other devices) through the VPN. In that case self-hosting solutions should be considered as best option.

But if we are talking about commercial VPN providers which are usually offering solutions for browsing on the internet through their gateways, several important should be raised. For instance, who is the operator of exit points (VPN gateways to the internet) and how user’s data is handled there. Are VPN connections really encrypted? Where are VPN servers and exit points located (in which country, under which legislation)? And, how trustworthy is the internet service provider of a VPN provider?

In 2016 *Australia’s Commonwealth Scientific and Industrial Research Organisation* (CSIRO) with researchers from the *University of South Wales* and *UC Berkley* did research of the VPN applications for Android mobile phones. They tested 283 VPN applications from *Google Play Store* and found that 18 percent of the applications failed to encrypt users’ traffic, 38 percent of the applications injected malware or *malvertising*, over 82 percent of applications requested access to sensitive data such as user accounts and text messages, three quarters of the applications used third-party user tracking libraries and majority of them had several security issues (for instance did not prevent DNS leaking,<sup>39</sup> etc.) (Ikram, Vallina-Rodriguez, Seneviratne, Kaafar and Paxson, 2016).

Also, a study from 2021 analysing different VPN products has shown that a lot of these products were owned or operated by the same company (for at least of 104 VPN products researchers found out that they are owned or operated by only 24 companies) and that VPN service providers were not transparent with users regarding their owners and parent companies’ locations. Research has also shown that VPN services were in different “privacy unfriendly” countries including China<sup>40</sup> and Hong Kong (up to 30% of VPNs had connections with or were owned by Chinese companies), but also Pakistan,<sup>41</sup>

---

39 DNS leaking refers to a security flaw that allows DNS requests to be revealed to DNS servers of the internet service provider, despite the use of a VPN service to attempt to conceal them.

40 China has a high level of surveillance and cyber spying (especially on foreign officials). It imposes obligations on companies, who are broadly required to help decrypt information (source: World map of encryption laws and policies). Also, VPN applications are generally not available on the Chinese Android and iOS application stores, and China is also known for blocking VPN connections from China to outside world.

41 Pakistan law enforcement officers have various powers relating to decryption including requiring officers access to data, device or information system “in unencrypted or decrypted intelligible format” for the purposes of investigating the offence. Licensed mobile and telephony service providers must establish systems for monitoring telecommunication traffic and these systems must ensure that voice and data signalling information is uncompressed, unencrypted, and not formatted in a manner which the installed monitoring system is unable to decipher (source: World map of encryption laws and policies).

United Arab Emirates, United States of America,<sup>42</sup> United Kingdom,<sup>43</sup> Switzerland,<sup>44</sup> etc. (Youngren, 2021).

## **Availability**

An important part of information security is also the availability of information and systems. Availability ensures reliable and timely access to the information system when users need it. A reliable and available IT system in an organisation is the foundation for the smooth execution of work and business processes and therefore plays a key role in business efficiency. The failure or unplanned downtime of an IT system usually causes unexpected interruptions to business processes, resulting in unnecessary costs.

Organisations should therefore have a business continuity plan in place, which defines the measures to maintain a certain level of service in the event of hardware or software failure. These are measures aimed at ensuring continuous operations or disaster recovery. At the hardware level, the measures mainly include the purchase and implementation of redundant computer, network and other hardware components, while at the software level it makes sense to implement all those solutions that protect information systems against attacks, user errors and software failures.

As the establishment of a business continuity system involves a certain financial investment, it is necessary to develop an appropriate plan to ensure that the organisation's critical functions are successfully established as quickly as possible and at the lowest possible cost. In this context, it is necessary to consider both the short-term and long-term consequences of an IT system failure for the organisation as a whole.

## **Remote work**

If an organisation wants to organise remote working even in the event of major crises or emergencies, it needs to design its information system to be available not only within the organisation but also for remote users.

A fundamental building block of the IT system's external accessibility is VPN technology, which allows employees to connect securely to the corporate network from remote locations. In this case, however, the security of the organisation's entire IT system must be designed in a significantly different way, as the security of the terminal equipment used by users accessing the organisation's internal network from remote locations must also be considered.

---

42 United States of America is the founding member of the Five Eyes alliance, a major surveillance state. Its National Security Agency (NSA) invests heavily in backdooring encryption technology, and Federal Bureau of Investigation (FBI) can access almost any data by secret subpoenas (so called National Security Letters).

43 United Kingdom is a founding member of the Five Eyes alliance and has surveillance legislation (Investigatory Powers Act, or Snooper's Charter, introduced in 2016) that gives law enforcement strong surveillance powers.

44 While Switzerland is advertised as a safe haven for digital privacy, but in fact has one of the strictest anti-terrorism laws in Europe (Ibrahim, 2021). Also, Swiss Federal Act on the Surveillance of Post and Telecommunications and Federal Intelligence Service Act had introduced broad surveillance of all electronic communication (Schönenberger, 2016) (Schönenberger, 2018). Regarding intelligence cooperation, Switzerland has several bilateral agreements with EU and is bound by a Mutual Legal Assistance Treaty with the United States. It is also important to point out that at least two Swiss companies, CryptoAG (Miller, 2020) and Omnisec (Endres, 2020), were closely cooperating with foreign intelligence services and were selling rigged cryptography equipment.

If employees work from home, they must also have the appropriate technical equipment. In times of crisis, the latter may not be available (to buy), so it makes sense to keep them in stock. Alternatively, it is possible to make use of the BYOD concept (*"Bring Your Own Device"*). This is the practice of employees bringing their own personal devices (laptops, tablets, smartphones) to work environments to access business, personal and other data in the organisation's IT system or, when working from home, using their own personal devices to connect remotely to the organisation's IT system. While BYOD enables greater mobility and ease of use for users and in principle reduces hardware costs for the organisation, it also brings several risks, both in terms of business information security and the protection of personal data and information security in general. The risks include not only the increased possibility of losing devices (mobile phones and laptops), but also the issue of securing these devices according to the legal requirements regarding personal data protection, classified information, labour, and competition legislation. When using the BYOD concept and enabling remote working, it is therefore important that the organisation carries out a proper assessment of whether employees' private devices are sufficiently secure. Risks need to be identified, analysed and procedures and measures put in place to reduce or even eliminate these risks. At the same time, it is important to be aware that an organisation cannot impose overly strict security policies on employee-owned devices, as this could infringe too much on users' privacy or even motivate employees to take shortcuts. For the latter reason in particular, user education is also very important. Using different user accounts for work and private purposes is also a good strategy to reduce the risks.

It is important to anticipate that employees may need help when working from home, and that some maintenance work may need to be done on their computers (with their consent). It is therefore advisable to install appropriate software equipment on the computers to allow remote access in case such assistance is needed.

Video conferencing systems are also becoming increasingly crucial for remote working, allowing companies to hold meetings between employees and business partners. Again, this also requires the right equipment. For example, an external headset with a microphone will offer a significantly better user experience than a built-in microphone and speakers. It is also necessary to ensure that users working from home will have a sufficiently powerful internet connection, or that they will be able to use a mobile connection to access the internet. Some videoconferencing solutions also provide end-to-end encryption – even in the case of group communication – which is certainly important to consider when these systems are being used in business environments.

For companies, it is crucial that their information systems are designed in a way that enables the simplest transition to remote work if necessary. Business organisations should focus on building and maintaining the adequate infrastructure and ensuring that employees have the suitable skills and knowledge for remote work.

## **Anonymization**

At a times when we are confronted with the increasing collection and use of traffic data on the one hand, and with increasingly blatant attempts of censorship even in democratic countries on the other, many people are seeking technical measures that can be applied against that.

One possible type of protection against the collection of traffic data and restrictions on access to information on the internet, are anonymization systems. These systems allow



us to hide our real IP address while also allowing us to circumvent censorship restrictions. There are several types of anonymization systems available. Most systems are intended for the anonymization of online services, but there are also special applications aimed at the anonymization of other services, e.g. P2P file sharing or other traffic.

It is important to realise that complete anonymization is almost impossible in practice, because with enough motivation and, above all, a lot of resources, anonymization systems can be subjected to a variety of attacks that allow an attacker to reveal the identity of their users. One of these techniques is *netflow* data analysis, which is performed to analyse traffic flow and traffic volume across the network. This can show which network node is communicating with another and can be used for tracking the users of anonymization networks. But usually deanonymization techniques require significant resources which means that they cannot be used on a wide scale. Using of anonymization systems can consequently increase the level of anonymization so the identity of the user of such a system is much more difficult to disclose.

Some of the first anonymization systems were anonymous proxies, which were the interfaces between the user and the website or service being visited. While proxy servers are still in use today, they are no longer used for anonymization but for monitoring and analysing traffic (to protect users from malicious code or unwanted content) or to speed up web browsing (by caching static web content).

The *Tor* anonymization and anticensorship network has set a standard for modern anonymization systems. It is a distributed network of anonymization servers, between which each user's encrypted traffic is routed until it leaves the network at one of its exit nodes. To use the *Tor* network, the user installs a *Tor* client or a special *Tor* browser on their computer, which redirects their web traffic to the *Tor* network. In addition to anonymization, the *Tor* network also offers the possibility to publish online content anonymously or to offer various network services anonymously. The developers of the *Tor* network have also built in so-called hidden services. These are (mostly web and mail) servers that are located within the *Tor* network and are not accessible from the "regular" web. They are accessed using special URLs<sup>45</sup> with the extension .onion and they could be accessed only from the *Tor* network (hence the name dark web).

Unfortunately, due to the human nature, anonymization technology often attracts various illegal and undesirable activities. Alongside perfectly legitimate and legal content, the *dark web* is thus also home to a wide range of illegal content, from child pornography to marketplaces with stolen credit card numbers, illegal online betting sites and the like. Nevertheless, the use of the *dark web* is not illegal by itself. *Dark web* is not used only by hackers and criminals. It is also used by investigative journalists who want to communicate anonymously with their sources, *whistleblowers*, political dissidents and even intelligence officers. The *Tor* network is the only uncensored and unmonitored window to the world for many people in non-democratic countries. The network can also be used by all those who visit such countries as tourists or on business trips and want to avoid local censorship restrictions.

---

45 URL – Uniform Resource Locator or web address, is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

## Conclusion

The provision of information security includes adequate infrastructure, protection of devices, data and applications and empowered users.

To ensure the overall information security of an organisation against cyber-attacks, it is necessary to implement security mechanisms at the level of the network, servers, user computers, peripheral devices and mobile devices (phones, tablets, etc.). Regular maintenance and updating of software and hardware equipment, at least basic physical security, implementation of a firewall or IDS/IPS system, a backup system and encryption should be provided in as many places as possible. This includes both the use of encrypted protocols wherever possible (for access to email and websites) and the implementation of data media encryption. It is recommended to use anti-virus and anti-spam software, applications to block online tracking technologies and so-called “junk” removers.

Users need to be made aware of the basic risks and how to protect themselves from threats. They should also be familiarised with how to choose appropriate passwords and, where possible, it is advisable to implement more advanced forms of authentication (use of one-time passwords, two-factor authentication, etc.).

Security policies should define procedures for protecting the organisation's information, installing and updating software and hardware handling procedures, including the implementation of a data wiping policy. If remote access is required, a properly secured VPN network should be set up, and at least the basics of a business continuity system should be put in place.

It cannot be guaranteed that the above will provide total security. But with these measures, an organisation will increase its overall protection, improve the management of information risks and ensure that it has secure and reliable operations.

## List of acronyms of Annex I

URL – Uniform Resource Locator or web address, is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

CD – Compact Disk, a digital optical disc data storage format.

CEO – Chief Executive Officer or managing director.

DNS – Domain Name System is the hierarchical and decentralized naming system that translates human readable domain names to machine readable IP addresses.

DVD – Digital Versatile Disc is a digital optical disc data storage format.

EMI – electromagnetic interference.

FAT – File Allocation Table is a file system developed for personal computers in 1977, however later was adapted and extended and it is still used nowadays.

FBI – Federal Bureau of Investigation is the domestic intelligence and security service of the United States and its principal federal law enforcement agency.

HTTPS – Hypertext Transfer Protocol Secure is an extension of the Hypertext Transfer Protocol, which is the primary protocol used to transmit data between a web browser and a website. HTTPS is encrypted, which increases security of data transfer over the Internet.

ICT – Information and Communications Technology, is the infrastructure and components that enable modern computing.

IoT – Internet of Things, physical objects that are embedded with sensors and software, that connect and exchange data with other devices and systems over the communications networks.

IP – Internet Protocol, IP address is a unique address that identifies a device on the internet or a local network. IP addresses serve two functions: network interface identification and location addressing.

IT – Information Technology.

NAS – Network-Attached Storage is a file-level data storage server providing data access to clients over the computer network.

NATO – North Atlantic Treaty Organisation is an intergovernmental military alliance between 27 European countries, 2 North American countries, and 1 Eurasian country (as the situation is in 2022).

NSA – National Security Agency is a national-level intelligence agency of the United States Department of Defence.

OSI model – the Open Systems Interconnection model is a conceptual model that characterises and standardises the communication functions of a telecommunication or computing systems.

OSINT – Open-Source Intelligence, a set of strategies and methods for the collection and analysis of data gathered from publicly available sources to produce actionable intelligence.

PTR – Pointer record. DNS PTR record is used for reverse DNS lookups. It matches domain names with IP addresses and is therefore a security tool that mainly helps to

check if the server's name is actually associated with the IP address from where the connection was initiated.

RAM memory – Random-Access Memory is a form of computer memory that can be read and changed directly. Typically, is used to store working data and machine code.

RAID – Redundant Array of Independent Disks is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both. While RAID arrays can provide enhanced data protection, it should not be considered as a backup.

SD card – Secure Digital non-volatile memory card.

SSL – Secure Sockets Layer is a cryptographic protocol designed to provide communications security over a computer network. It is deprecated from 2015 by TLS – Transport Layer Security, which is also a cryptographic protocol designed to provide cryptography, confidentiality (privacy), integrity, and authenticity using digital certificates, between two or more communicating computer applications.

USB – Universal Serial Bus.

VoIP – Voice over Internet Protocol, also called IP telephony, is a group of technologies for the implementation of voice communications and multimedia sessions over Internet Protocol networks.

VPN – Virtual Private Network.

WHOIS – a database which stores registered users or assignees of Internet resources like domain name, IP address block or autonomous system data.

## References of Annex I

Boone, J. V. & Peterson, R. R. & United States. 2000. *The start of the digital revolution, SIGSALY secure digital voice communications in World War II*. Center for Cryptologic History, National Security Agency. Available at: <https://media.defense.gov/2021/Jul/13/2002761542/-1/-1/0/SIGSALY.PDF>.

Endres Fiona. 2020. Geheimdienstaffäre: Weitere Schweizer Firma rückt in den Fokus. SRF (Schweizer Radio und Fernsehen), 25. 11. 2020, <https://www.srf.ch/news/schweiz/verschluesselungsgeraete-geheimdienstaffaere-weitere-schweizer-firma-rueckt-in-den-fokus>.

ENISA. 2016. ENISA's Threat Taxonomy. Available at: <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view>.

Gaillot, Vincent. 2001. How to use Google to find confidential informations. Posted on BUGTRAQ. Available at: <https://marc.info/?l=bugtraq&m=100619108724992>.

Gardham, Duncan. 2011. Mossad carries out daring London raid on Syrian official. The Daily Telegraph, 15 May 15<sup>th</sup> 2011. Available at: <https://www.telegraph.co.uk/news/worldnews/middleeast/israel/8514919/Mossad-carries-out-daring-London-raid-on-Syrian-official.html>.

Ibrahim Sara. 2021. Will Switzerland distance itself from the EU on mass surveillance? SWI, 8. 7. 2021, <https://www.swissinfo.ch/eng/will-switzerland-distance-itself-from-the-eu-on-mass-surveillance-/46766024>.

Leyden, John. 2009. Russian spy agencies linked to Georgian cyber-attacks. The Register, March 23<sup>rd</sup> 2009. Available at: [https://www.theregister.co.uk/2009/03/23/georgia\\_russia\\_cyberwar\\_analysis/](https://www.theregister.co.uk/2009/03/23/georgia_russia_cyberwar_analysis/).

Long, J. and Skoudis, E. 2005. Google Hacking for Penetration Testers. Syngress, Rockland.

Markoff, John. 2008. Before the Gunfire, Cyberattacks. The New York Times, August 12<sup>th</sup> 2008. Available at: <https://www.nytimes.com/2008/08/13/technology/13cyber.html>.

Miller Greg. 2020. The intelligence coup of the century. The Washington Post, 11. 2. 2020, <https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/>.

Muhammad Ikram, Narseo Vallina-Rodriguez, Suranga Seneviratne, Mohamed Ali Kaafar and Vern Paxson. 2016. An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps. Published in IMC '16: Proceedings of the 2016 Internet Measurement Conference, November 2016, p. 349 - 364. ISBN: 9781450345262, DOI: 10.1145/2987443.

Prince, Brian. 2009. Cyber-attacks on Georgia Show Need for International Cooperation, Report States. eWeek, August 18<sup>th</sup> 2009. Available at: <https://www.eweek.com/security/cyber-attacks-on-georgia-show-need-for-international-cooperation-report-states/>.

Rutkowska, Joanna. 2009. The Invisible Things Lab's blog: Evil Maid goes after TrueCrypt!. The Invisible Things Lab's blog. Available at: <http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html>.

Schönenberger Erik. 2016. Faktenblatt und Illustration zur «Kabelaufklärung». Digitale Gesellschaft, 1. 9. 2016, <https://www.digitale-gesellschaft.ch/2016/09/01/faktenblatt-und-illustration-zur-kabelaufklaerung/>.

Schönenberger Erik. 2018. Faktenblatt zur «Vorratsdatenspeicherung». Digitale Gesellschaft, 27. 9. 2018, <https://www.digitale-gesellschaft.ch/2018/09/27/faktenblatt-zur-vorratsdatenspeicherung-uebersichtlich-erklaert/>

Vancouver, Rick. 2021. What is the 3-2-1 backup rule? Veeam blog, <https://www.veeam.com/blog/321-backup-rule.html>.

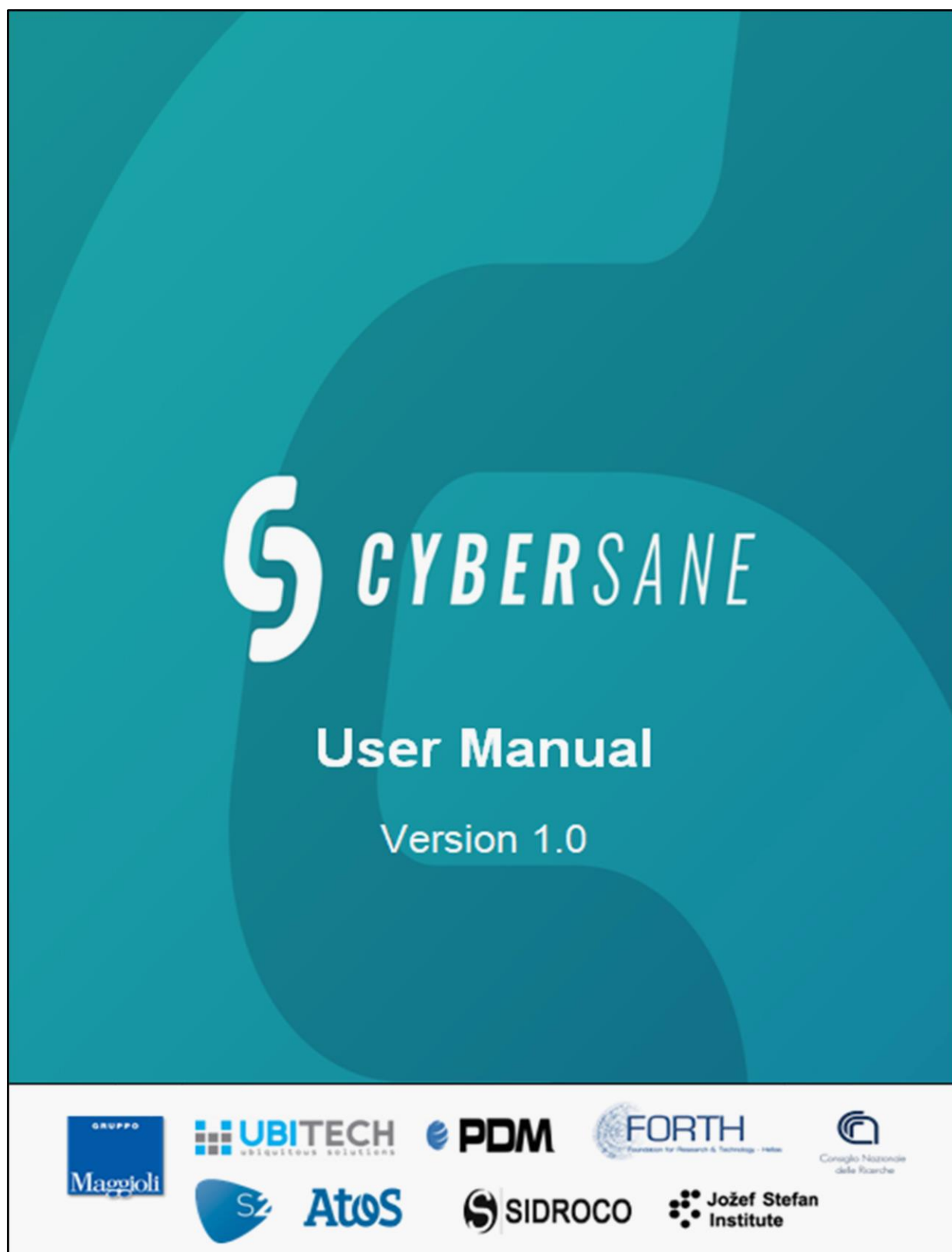
Voiskounsky, E. Alexander, Babveva D. Julia and Smyslova, V. Olga. 2000. Attitudes towards computer hacking in Russia. In Thomas, Douglas in Loader D. Brian, (ed.). 2000. Cybercrime, p. 56–84. London, New York: Routledge.

Zalewski, Michal. 2001. Against the System: Rise of the Robots. Phrack magazine, Volume 0x0b, Issue 0x39, Phile #0x0a of 0x12. Available at: <http://phrack.org/issues/57/10.html>.

Youngren, Jan. 2021. Hidden VPN owners unveiled: 104 VPN products run by just 24 companies. <https://vpnpro.com/blog/hidden-vpn-owners-unveiled-97-vpns-23-companies/>, April 19th, 2021.

World map of encryption laws and policies. Global Partners Digital, <https://www.gp-digital.org/world-map-of-encryption/>

## **Annex II. CyberSANE System User Manual**





Project co-funded by the European Union within the Horizon 2020 Programme

This document has been produced under Grant Agreement 833683. This document and its contents remain the property of the beneficiaries of the CyberSANE Consortium and may not be distributed or reproduced without the express written approval of the Project-Coordinator

# 1. Introduction

The current User Manual presents the user journey to the CyberSANE platform. It describes all the user interface of the CyberSANE system and explains how a user (e.g. Security Professional, Security Analyst) is able to take advantage of the CyberSANE components to:

- identify risks, threats and vulnerabilities upon risk assessment performance
- detect anomalies and incidents and recognize attack patterns within the organisation's Critical Information Infrastructure (CII)
- explore possible attack paths to better comprehend the attacker's course
- develop strategies and share it with organisation's users
- utilize the knowledge gained gradually during the incident handling process to make proper decisions for eradication and recovery
- create lessons learned and communicate the results to external parties upon selected privacy policy(-ies)

The CyberSANE user journey follows subsequently the phases of the incident handling process based on NIST (cf. NIST SP 800-61<sup>46</sup>). The CyberSANE dashboard provides services for Security Professionals and Security Analysts to support the incident handling process. A user that does not have information security expertise or experience would not be able to analyze and deeply comprehend the evidences and information provided by the CyberSANE system.

## 1.1 Incident Handling Phases at a glance

Incident response capabilities are realized in four distinct phases:

### **Preparation Phase**

It refers to the establishment and Training of the Incident Response Team acquiring the necessary tools and responses. Within this phase the organisation aims to limit proactively the number of incidents that could possibly occur by adopting and implementing a set of security controls on the organisations' s assets driven by risk assessment results.

### **Detection and Analysis Phase**

It aims to indicate that Residual Risk persists to the assets of the organisations, regardless the implementation of security controls in the previous phase. The current phase detects security bridges (e.g. suspicious traffic, anomalies) and provides alerts to the organisation whenever a security incident occurs.

---

<sup>46</sup> <http://dx.doi.org/10.6028/NIST.SP.800-61r2>

### **Containment, Eradication and Recovery Phase**

During this phase, the Security Professional/Security Analyst along with the Critical Information Infrastructure (CII) operator undertake proper decisions about mitigation actions and incident handling to encounter what has been detected in the previous phase. The CyberSANE system supports only the containment process of this phase. Within this phase, the Security Professional/Security Analyst can use the CyberSANE system to capture all the evidences generated in the “Detection and Analysis” phase and articulate them in an organized manner for further analysis to help the user undertake proper eradication and recovery actions.

### **Post Incident Activity Phase**

After the incident has been handled properly or corresponding mitigation actions have been undertaken, the organisation can document on the adopted incident handling process and the lessons learned (according to the information and evidence gathered from all previous phases) to raise the security awareness and indicate what could be worth replicating and what could be omitted in a future incident handling process. Within this phase, the organisation has the option to disseminate the entire or a part of the produced documentation with external parties at will.

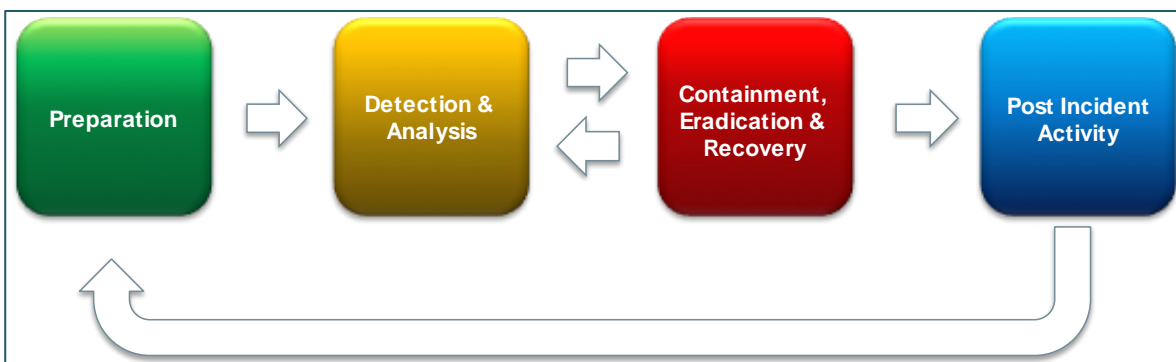


Figure 1: The four phases of the incident handling process in CyberSANE based on NIST.

## **1.2 Structure of the manual**

The current manual is structured as follows: Section 2 presents the horizontal services of the CyberSANE system (i.e. Self-Registration, Support and Profiling), Section 3 presents an overview of the incident handling phases within the CyberSANE system, Section 4 presents the Preparation Phase, Section 5 describes the Detection and Analysis Phase, Section 6 illustrates the Containment, Eradication and Recovery Phase, Section 7 reflects the Post Incident Activity phase and eventually Section 8 presents briefly the CyberSANE system components LiveNet, DarkNet, HybridNet, ShareNet and PrivacyNet and the tools that operate behind the incident handling phases of the CyberSANE dashboard.

## 2. Self-Registration, Support and Profiling

The CyberSANE platform can be accessed through the following web address:

<https://platform.cybersane-project.eu/cybersane>

### 2.1 Create Account

To create an account, select “Sign Up” from the CyberSANE homepage.

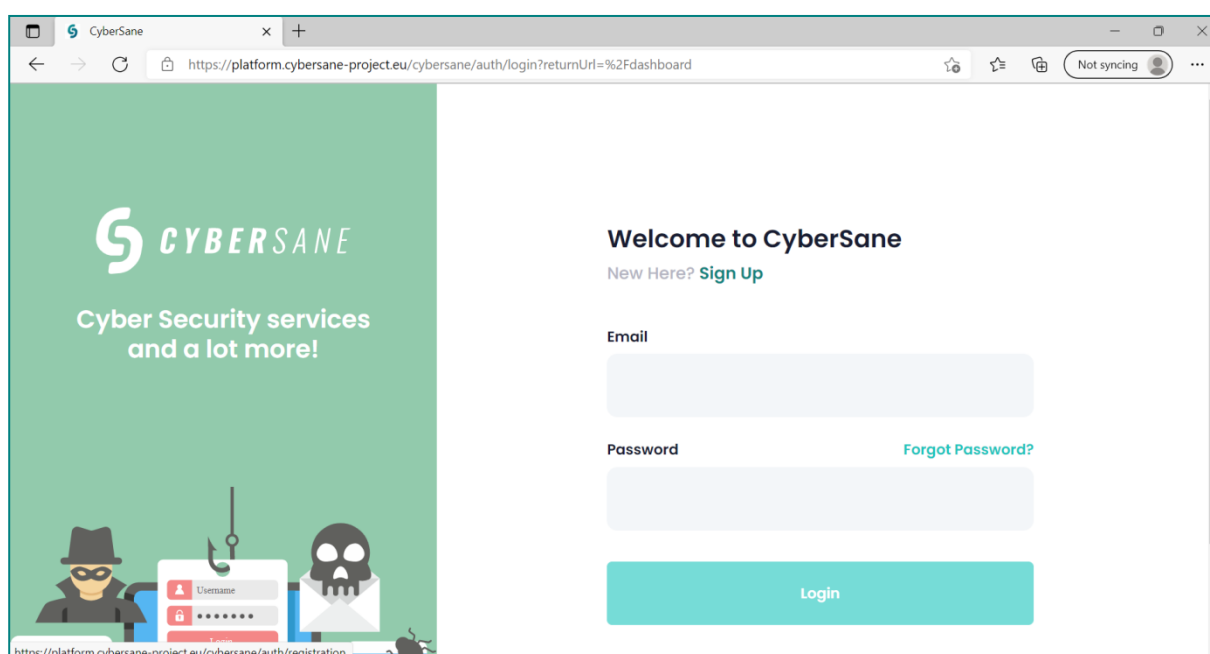


Figure 2 –CyberSANE homepage.

Then, enter details, accept terms and conditions and click on the “Register” button.

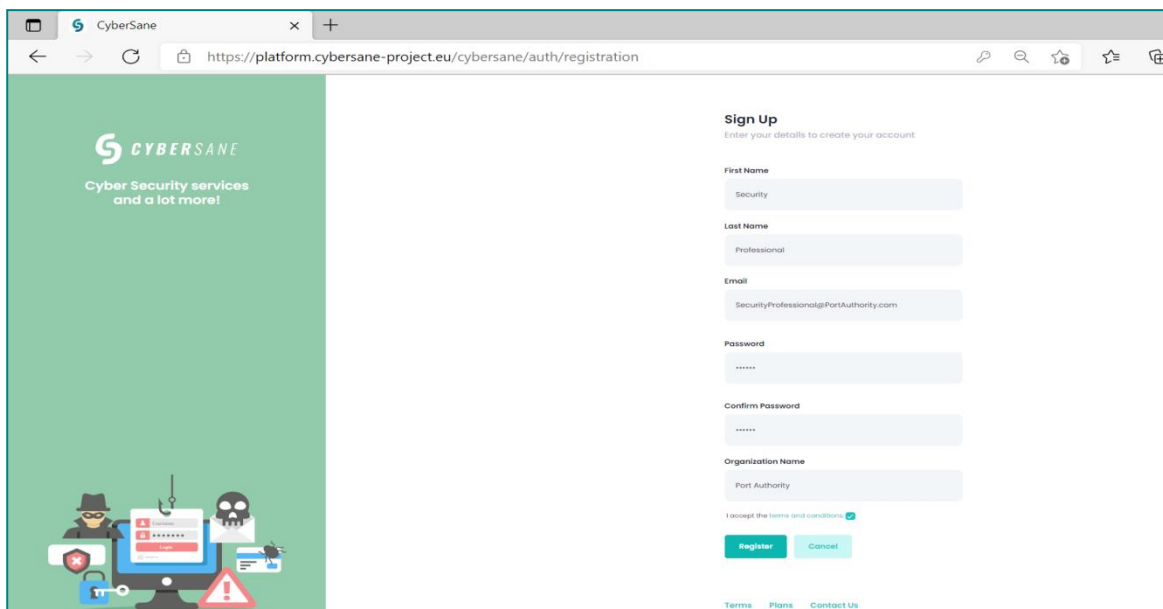
A screenshot of a web browser showing the CyberSane registration page. The browser's address bar displays the URL: https://platform.cybersane-project.eu/cybersane/auth/registration. The page is split into two main sections. On the left, there is a green vertical banner with the CyberSane logo at the top, followed by the text "Cyber Security services and a lot more!". At the bottom of the banner is an illustration of a person in a black hat and mask sitting at a desk with a computer monitor, with various security-related icons like a skull, a shield, and a key. On the right, the "Sign Up" form is displayed. It includes the heading "Sign Up" and a subtext "Enter your details to create your account". The form fields are: "First Name" (with "Security" entered), "Last Name" (with "Professional" entered), "Email" (with "SecurityProfessional@PortAuthority.com" entered), "Password" (with "\*\*\*\*\*" entered), "Confirm Password" (with "\*\*\*\*\*" entered), and "Organization Name" (with "Port Authority" entered). Below these fields is a checkbox labeled "I accept the terms and conditions" which is checked. At the bottom of the form are two buttons: "Register" (in green) and "Cancel" (in light blue). At the very bottom of the page, there are links for "Terms", "Plans", and "Contact Us".

Figure 3: Sign up the CyberSANE platform.

After signing up, a verification e-mail is sent to the new user's provided e-mail address. The new CyberSANE user must access the verification link, included in the e-mail. The user's account has been created successfully.

## 2.2 Login

To login to the CyberSANE platform, the CyberSANE user must access the CyberSANE homepage <https://platform.cybersane-project.eu/cybersane>, insert his/her credentials and press the "Login" button.

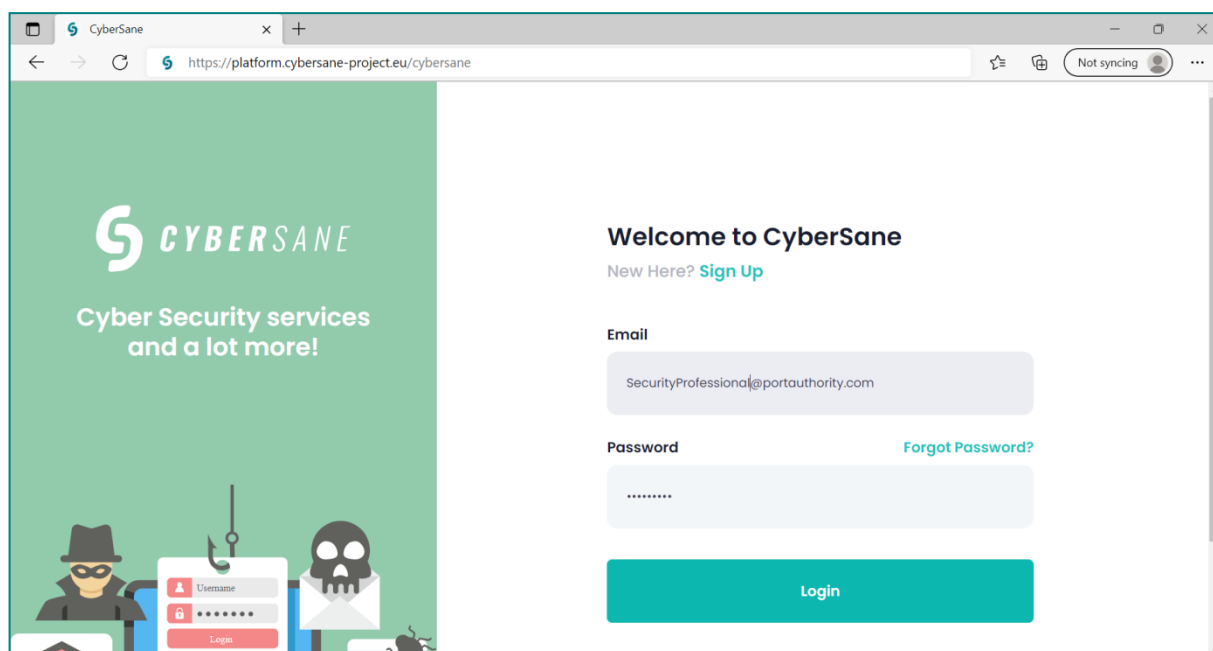


Figure 4: Login the CyberSANE.

Upon successful authentication the following screen appears showing the Dashboard menu.

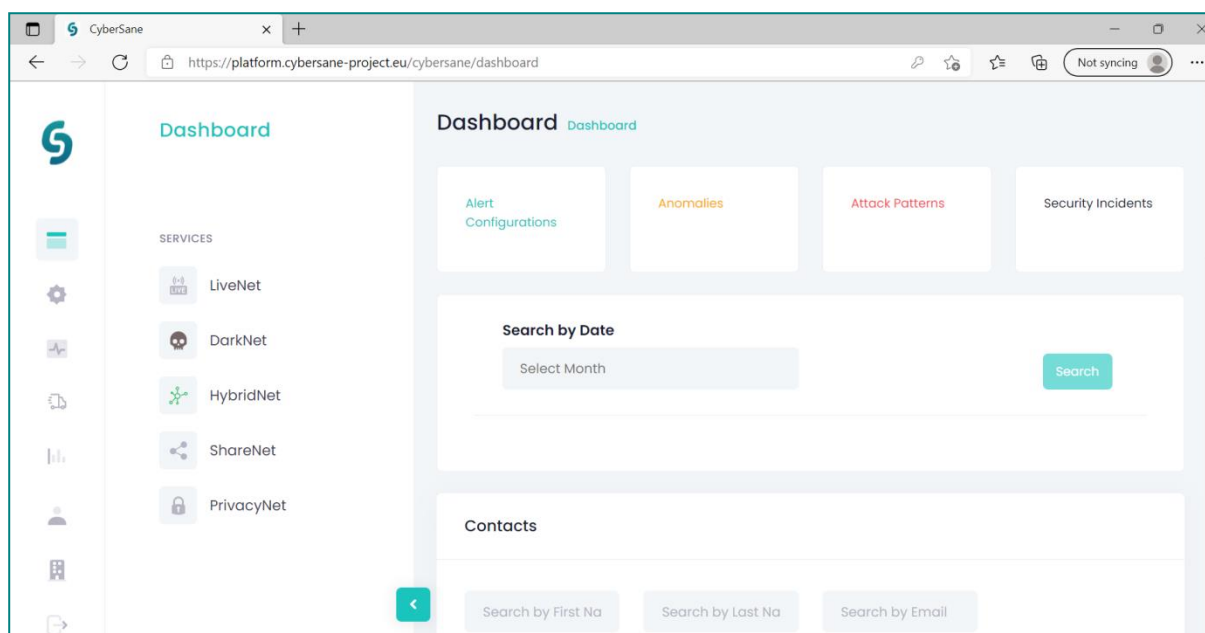


Figure 5: CyberSANE Dashboard menu.

## 2.3 Logout

To logout from CyberSANE press the “Logout” button.

## D9.2 – Training Materials and Report on Training Processes

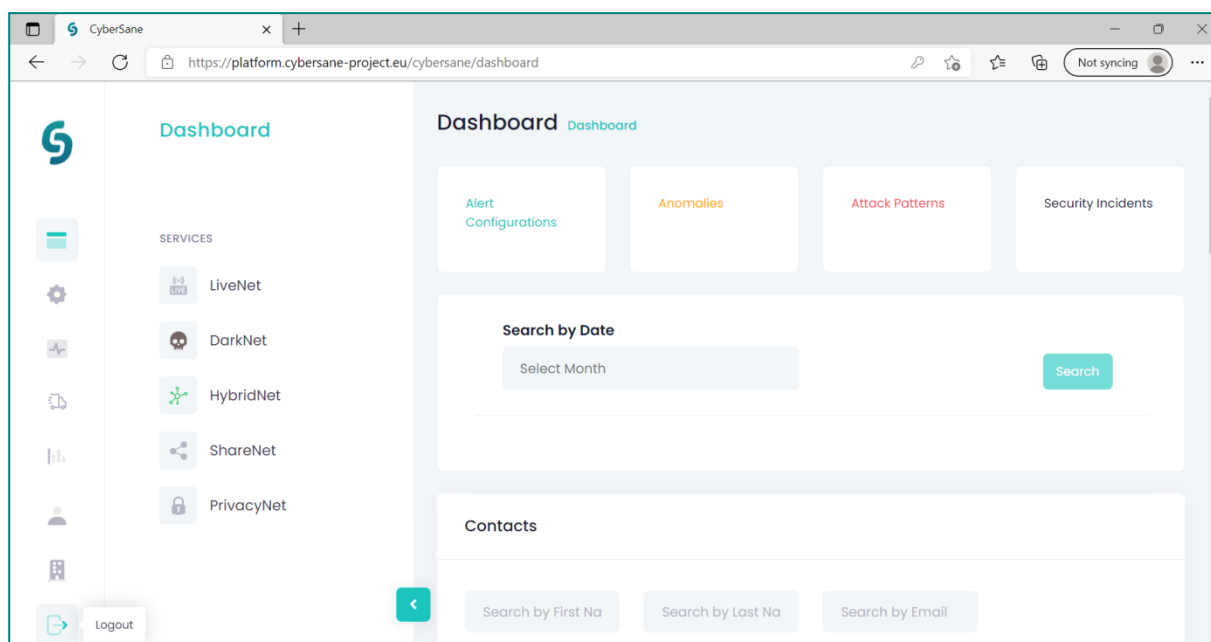


Figure 6: Logout from CyberSANE.

Upon successful logout the following screen appears.

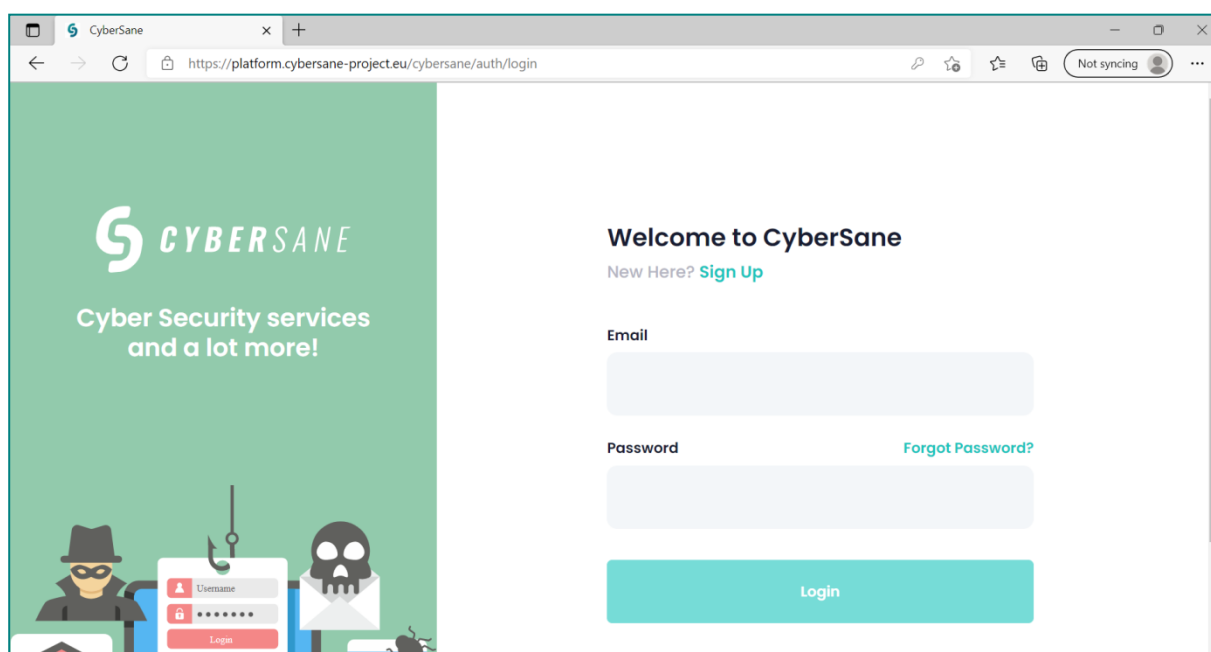


Figure 7: Screen after CyberSANE successful logout.

## 2.4 Support

In case a CyberSANE user faces any issues, he/she can contact to the CyberSANE support technical team by sending the enquiries via the platform. To do so, the CyberSANE user shall click on the “Contact Us” indication which can be found at the bottom-right of the main homepage.

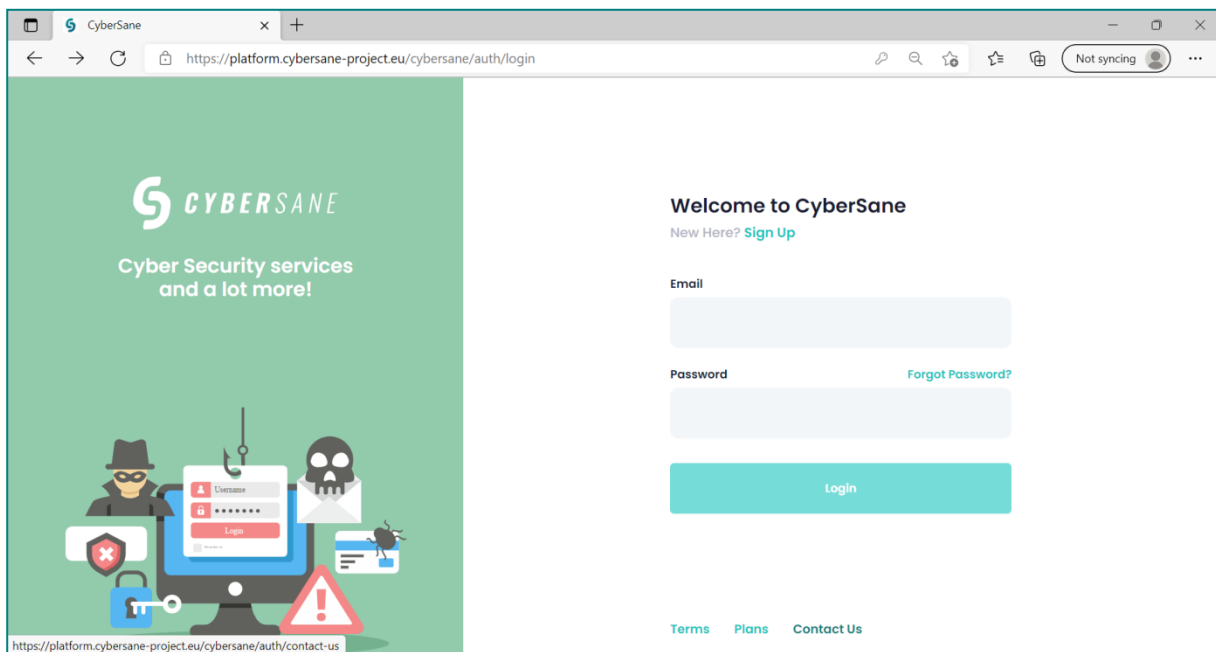


Figure 8: Contact with the CyberSANE support team in case of issues.

Then, an inquiry form appears as depicted in the following figure. The CyberSANE user shall fill the inquiry form and press the “Submit” button.

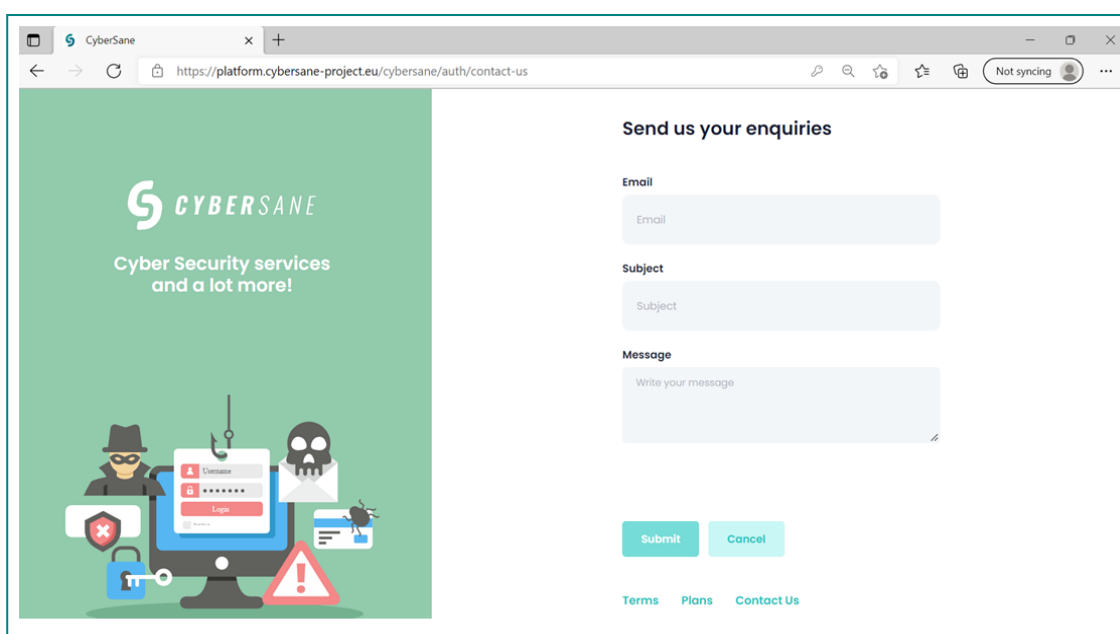




Figure 9: Send an inquiry to the CyberSANE support team.

## 2.5 Profiling (User and Organisation)

The profiling related activities are supported by the user and organisation management which can be achieved from the CyberSANE dashboard menu icon (Figure 10). User profile can be easily configured from the following options:

- Profile Overview
- Change Password

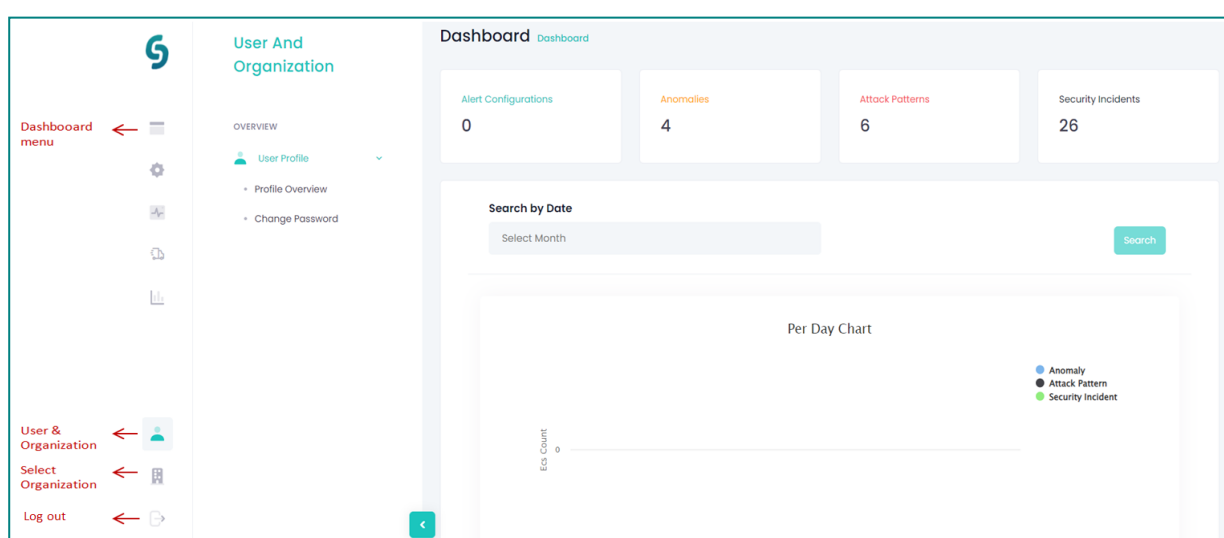


Figure 10: CyberSANE user management options.

### 2.5.1 Profile Overview

User & Organisation -> User Profile -> Profile Overview

To insert user's profile and add or change information click the "User & Organisation" icon and then select "User Profile" and "Profile Overview" options (Figure 10), make the desired configurations and then click "Save".

### 2.5.2 Change Password

User & Organisation -> User Profile -> Change Password

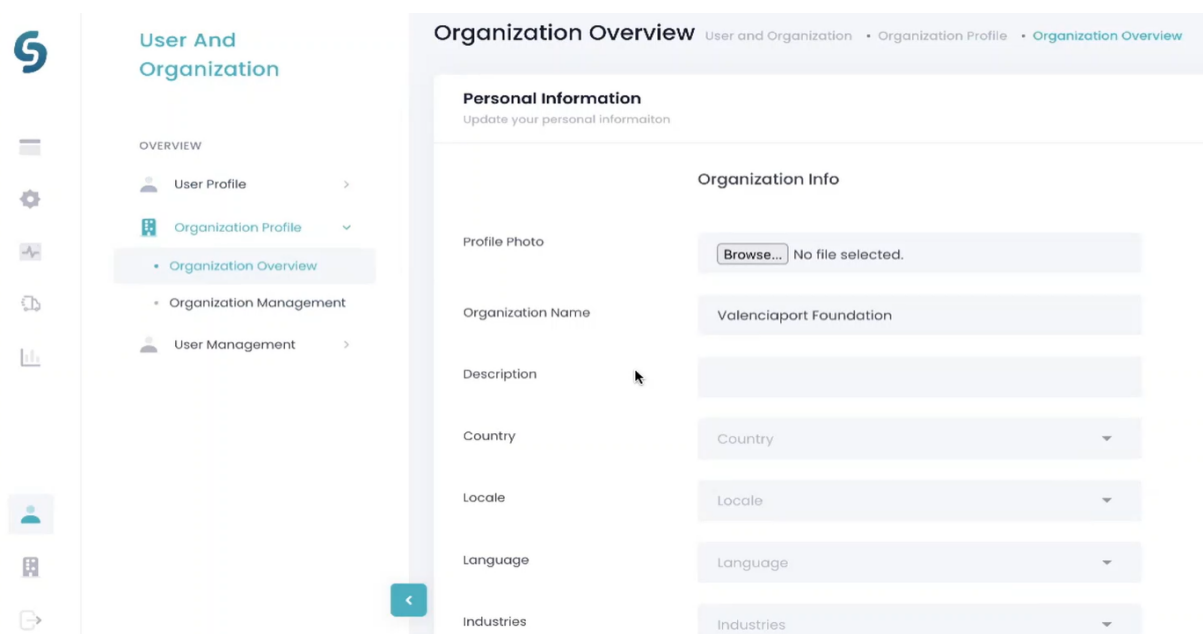
To change password, the user shall click on the User & Organisation" icon and then select "User Profile" and "Change Password" (Figure 10) options, fill in the requested fields (Current Password/New Password/Verify Password) and press "Save". Upon successful verification the user's password is changed.

### 2.5.3 Organisation Profile

## D9.2 – Training Materials and Report on Training Processes

This functionality can be accessed only by the administrator user. It contains the following two capabilities (Figure 11):

- Organisation Overview
- Organisation Management



The screenshot displays the 'Organization Overview' interface. On the left, a sidebar shows the navigation menu under 'User And Organization', with 'Organization Overview' selected. The main panel is titled 'Organization Overview' and contains two main sections: 'Personal Information' (with a sub-header 'Update your personal information') and 'Organization Info'. The 'Organization Info' section includes fields for 'Profile Photo' (with a 'Browse...' button and 'No file selected.' text), 'Organization Name' (filled with 'Valenciaport Foundation'), 'Description' (empty text area), 'Country' (dropdown menu), 'Locale' (dropdown menu), 'Language' (dropdown menu), and 'Industries' (dropdown menu).

Figure 11: CyberSANE organisation profile options.

### 2.5.3.1 Organization Overview

User & Organisation -> Organisation Profile -> Organisation Overview

The “Organisation Overview” option (Figure 11) can be accessed only by the administrator user upon clicking on the “Organisation Profile” from the “User and Organisation” category. Information about the organisation can be used to automatically search for the reputation of this organisation in the Deep and Dark Web (cf. section 5.4 “Deep Web Threat Intelligence”)

### 2.5.3.2 Organisation Management

User & Organisation -> Organisation Profile -> Organisation Management

The “Organisation Management” option (Figure 11) provides to the administrator user a list of details of all the different users of the organisation (full names/e-mail addresses) and their roles.

In addition, the e-mail addresses can be searched in the Deep and Dark Web to know whether an organisation user’s or an internal contact’s e-mail is breached in the Deep and Dark Web. No breach identified is indicated with “False” notification, whereas an identified breach on an e-mail address denotes “True” notification in the “Organisation Management” page. The exact information for a breached e-mail address can be further explored.

### 3. Overview of the Phases of the Incident

## Handling Process in the CyberSANE system

The CyberSANE capabilities of the incident handling process phases can be accessed in the platform through the following icons, depicted in Figure 12.

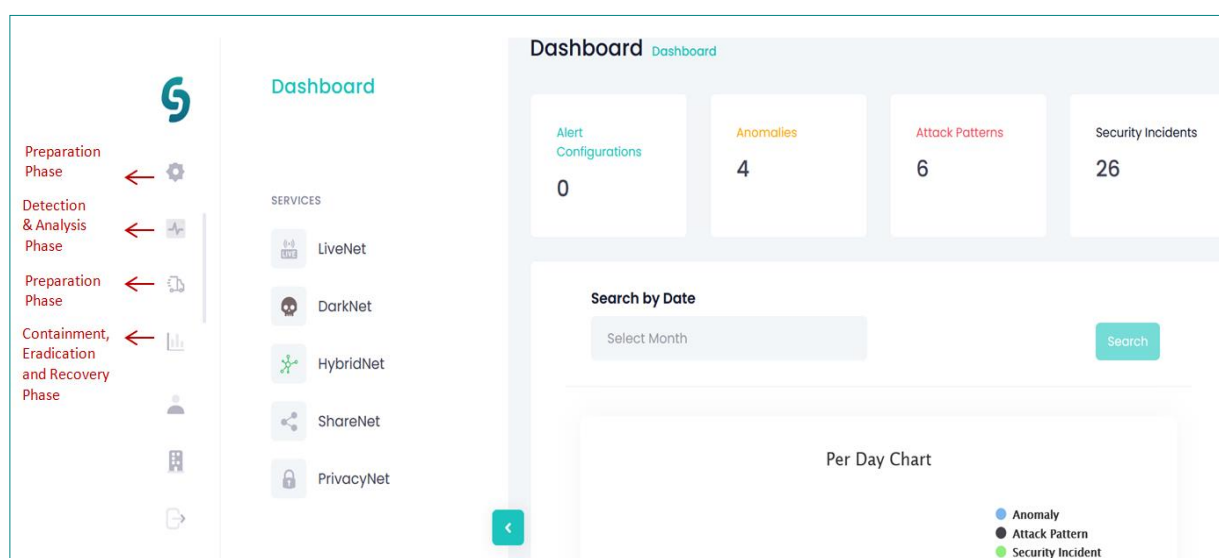


Figure 12: Incident handling phases in CyberSANE

Each incident handling phase provides the following main functionalities:

#### Preparation Phase

- Communication
- Asset Inventory
- Threat Intelligence
- Prevention

#### Detection & Analysis Phase

- Security Incidents
- Alerts and Notifications
- Deep Web Threat Intelligence
- Open Web Threat Intelligence

## D9.2 – Training Materials and Report on Training Processes

---

### Containment, Eradication & Recovery Phase

- Simulation Environment

### Post Incident Activity Phase

- Data Sharing Agreements

## 4. Preparation Phase

The Preparation Phase functionalities can be accessed by the dashboard menu by clicking on the “Preparation” icon (Figure 13).

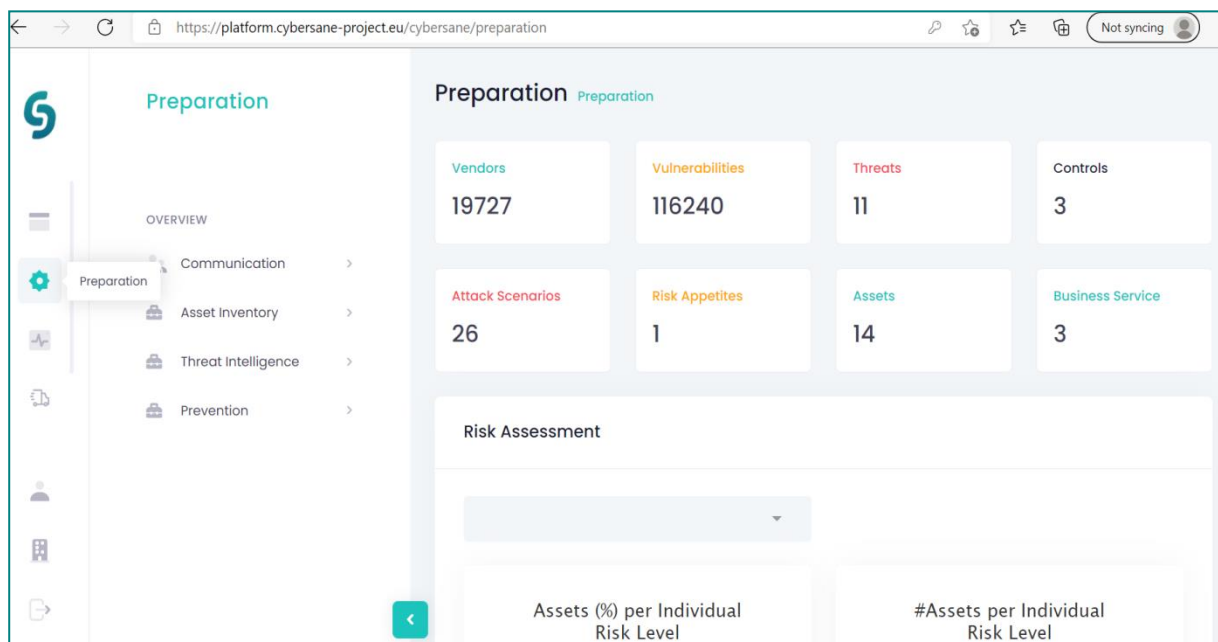


Figure 13: CyberSANE Preparation phase functionalities.

The Preparation Phase of the CyberSANE system falls into the below functionalities which are analyzed in the following sections:

- Communication
- Asset Inventory
- Threat Intelligence
- Prevention

### 4.1 Communication

The organisation shall deal with the internal and external contacts that will participate in the incident handling process (e.g. get notified for an incident that involves the CII they operate by receiving security alerts). In particular, the CyberSANE user can register, edit, search whether there is a breach of the e-mail in the Deep and Dark Web, deactivate or delete organisation’s internal and external contacts by clicking on the following icons of the respective contacts management editor accordingly:

+ Create new

Create a new internal or external contact



Edit an internal or external contact



Check for potential e-mail breach of an existing internal or external contact in the Deep and Dark Web



Delete an existing internal or external contact

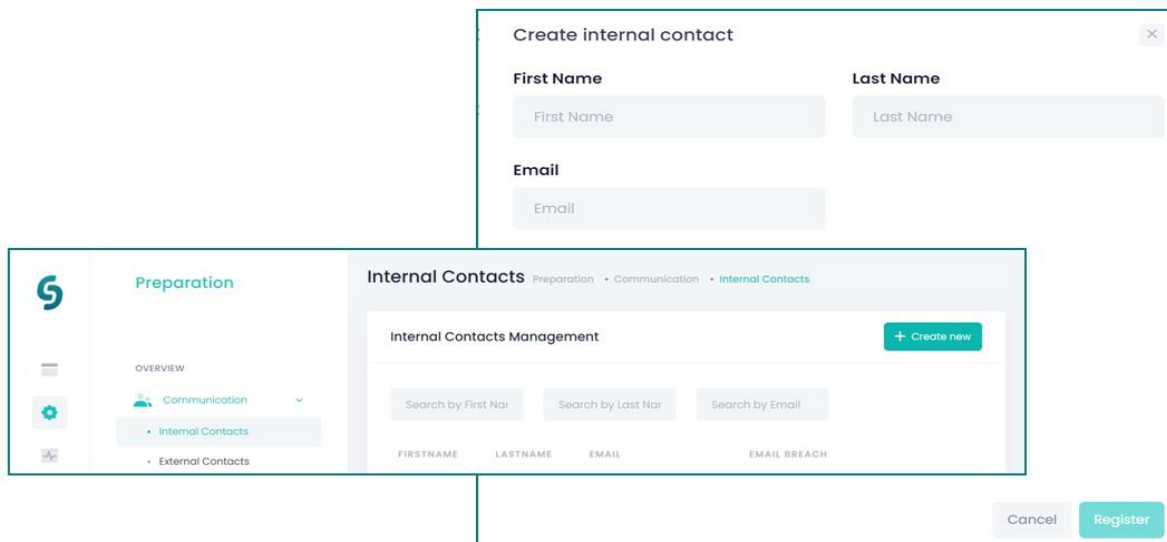
In addition, existing contacts can be searched from the contacts management editor.

#### 4.1.1 Create Internal Contacts

Preparation -> Communication -> Internal Contacts

The CyberSANE user can register new users in an organisation that will participate in the incident handling process. At a later stage, the CyberSANE system will create alerts for these contacts whenever it identifies a security incident/an anomaly/an attack. Contacts may receive or not automatic alerts and notifications depending on the user will.

To create an internal contact (for a person that belongs in the same organisation), the CyberSANE user shall select “Communication” from the “Preparation” phase icon of the dashboard menu and then click on the “Internal Contacts”, “Internal contacts Management” and “Create new” options subsequently. Then, the contact editor appears and the CyberSANE user shall fill in the requested fields and press the “Register” button. The internal contact creation process is shown in the following figure.



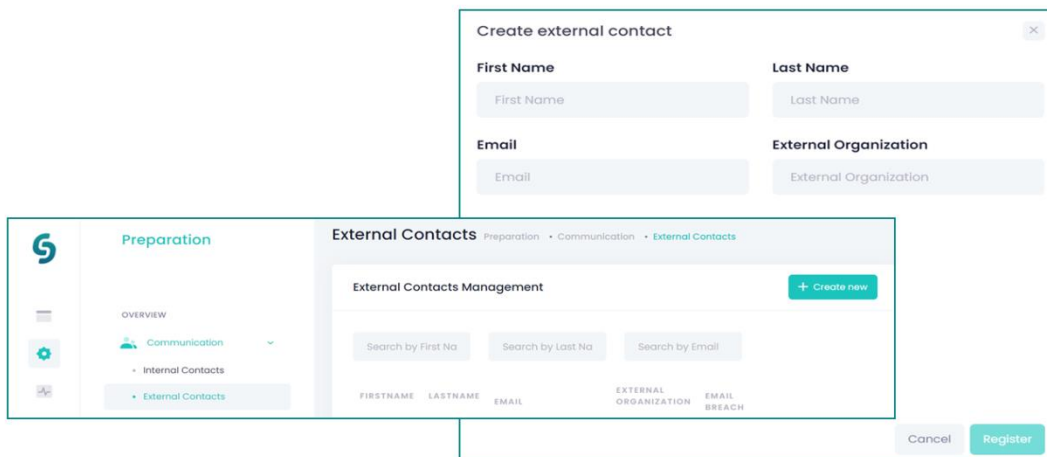
The screenshot displays the CyberSANE interface. On the left, a sidebar menu shows the navigation path: Preparation > Communication > Internal Contacts. The main content area is titled 'Internal Contacts Management' and includes a '+ Create new' button. Below this, there are search filters: 'Search by First Name', 'Search by Last Name', and 'Search by Email'. A table with columns 'FIRSTNAME', 'LASTNAME', 'EMAIL', and 'EMAIL BREACH' is visible. Overlaid on top of the main content is a 'Create internal contact' form with fields for 'First Name', 'Last Name', and 'Email'. At the bottom right of the form, there are 'Cancel' and 'Register' buttons.

Figure 14: Creation of an internal contact.

### 4.1.2 Create External Contacts

Preparation -> Communication -> External Contacts

The CyberSANE user can register, be aware and maintain a full list of all the external contacts that will support the incident handling process. At a later stage, the CyberSANE system will create alerts for these contacts whenever it identifies a security incident/an anomaly/an attack. Contacts may receive or not automatic alerts and notifications depending on the administrator's will. To create an external contact (for a person that does not belong in the organisation), the CyberSANE user shall select "Communication" from the "Preparation" phase icon of the dashboard menu and then click on the "External Contacts", "External contacts Management" and "Create new" options subsequently. Then, contact editor appears and the CyberSANE user shall fill in the requested fields in and press the "Register" button. The external contact creation process is shown in the following figure.



The figure shows two overlapping screenshots of the CyberSANE interface. The background screenshot displays the 'Preparation' phase menu with 'Communication' selected, leading to 'External Contacts' and then 'External Contacts Management'. The foreground screenshot is a modal form titled 'Create external contact' with the following fields: 'First Name', 'Last Name', 'Email', and 'External Organization'. A '+ Create new' button is visible in the background dashboard. At the bottom right of the modal, there are 'Cancel' and 'Register' buttons.

Figure 15: Creation of an external contact.

## 4.2 Asset Inventory

The organisation can hold within the CyberSANE system an asset inventory of its CII. The asset inventory must be developed during the Preparation phase of the incident handling process which can be viewed by selecting the corresponding options from the dashboard menu (Figure 16). It provides the following three functionalities:

- Asset Management
- Controls Management
- Vendors Management

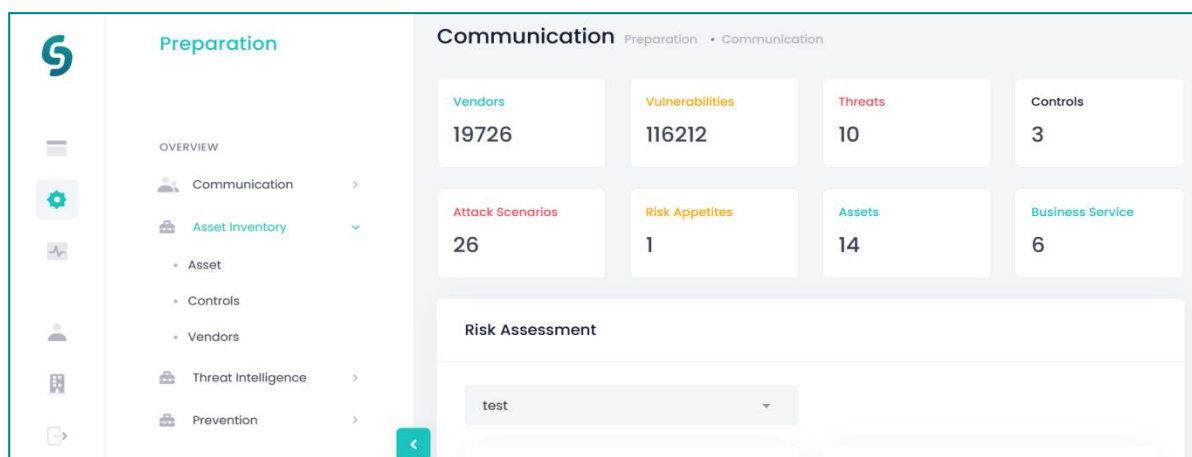


Figure 16: Browse the Asset Inventory and its capabilities.

## 4.2.1 Asset Management

Asset management is a CyberSANE functionality that allows the Security Professional to register the organisation's assets and review and manage them within an asset repository. Moreover, the functionality offers the capability to explore asset graphs and review identified threats and vulnerabilities from online repositories.

### 4.2.1.1 Manage Assets

Preparation -> Asset Inventory -> Asset

To manage assets, select the "Asset Inventory" from the "Preparation" phase of the dashboard menu and then click on the "Asset" category. A list of all the registered assets appears as it is shown in Figure 17.

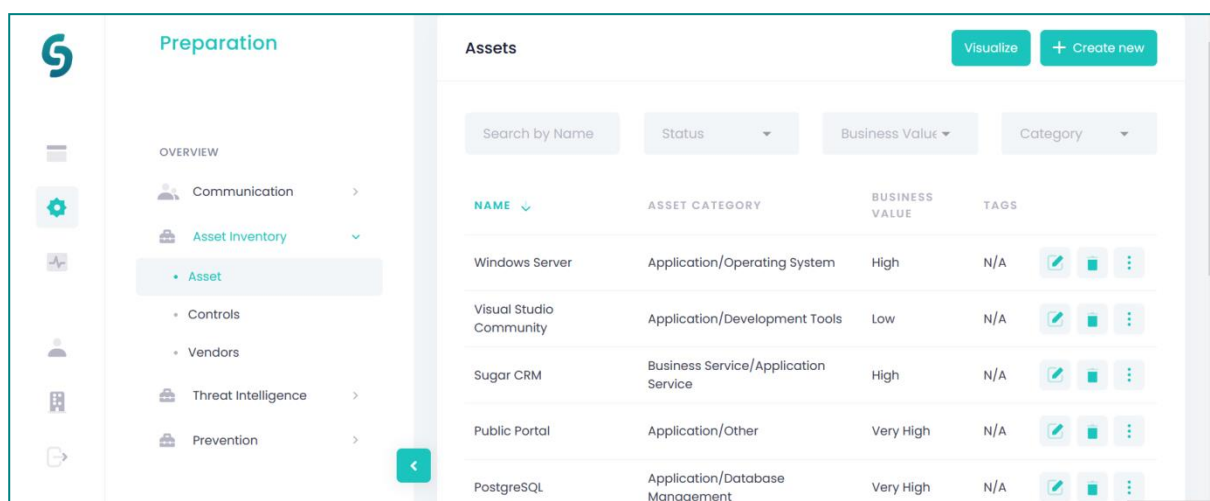


Figure 17: A list of the registered asset is depicted from the Asset menu.



Assets can be searched from the “Assets” menu either by their declared “Name” or “Business Value” (through a nominal scale providing labels from “Very Low” to “Very High”) or “Category” (Asset category from default list) (Figure 17).

**Example:** Suppose that the organisation seeks for its registered portals, the keyword “Portal” can be inserted in the “Search by Name” field and a list of all the assets including the word “Portal” are presented as shown in Figure 18.

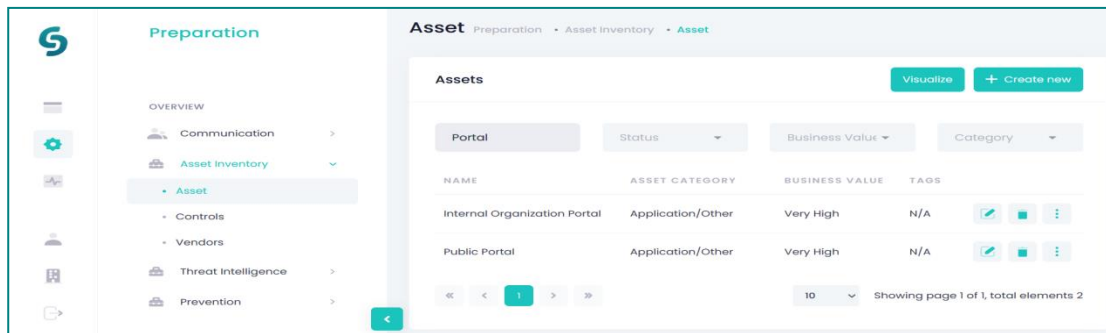





Figure 18: Assets can be searched from the Asset menu.

Assets can be either edited or deleted by selecting the  (pen) icon or the  (bin) icon respectively from the asset management editor (Figure 18). The Security Professional can browse additional asset functionalities by clicking on the  (three dots) icon (Figure 19):

- Footprint: Review a Threat Probability Vulnerability Heatmap depicting all identified threats and vulnerabilities for each asset
- Clone: Creating an asset clone allows the Security Professional to replicate an asset's attributes to a new asset
- Vulnerabilities: Shows all identified vulnerabilities for each asset along with their attributes

#### 4.2.1.2 Register Asset

Preparation -> Asset Inventory -> Asset

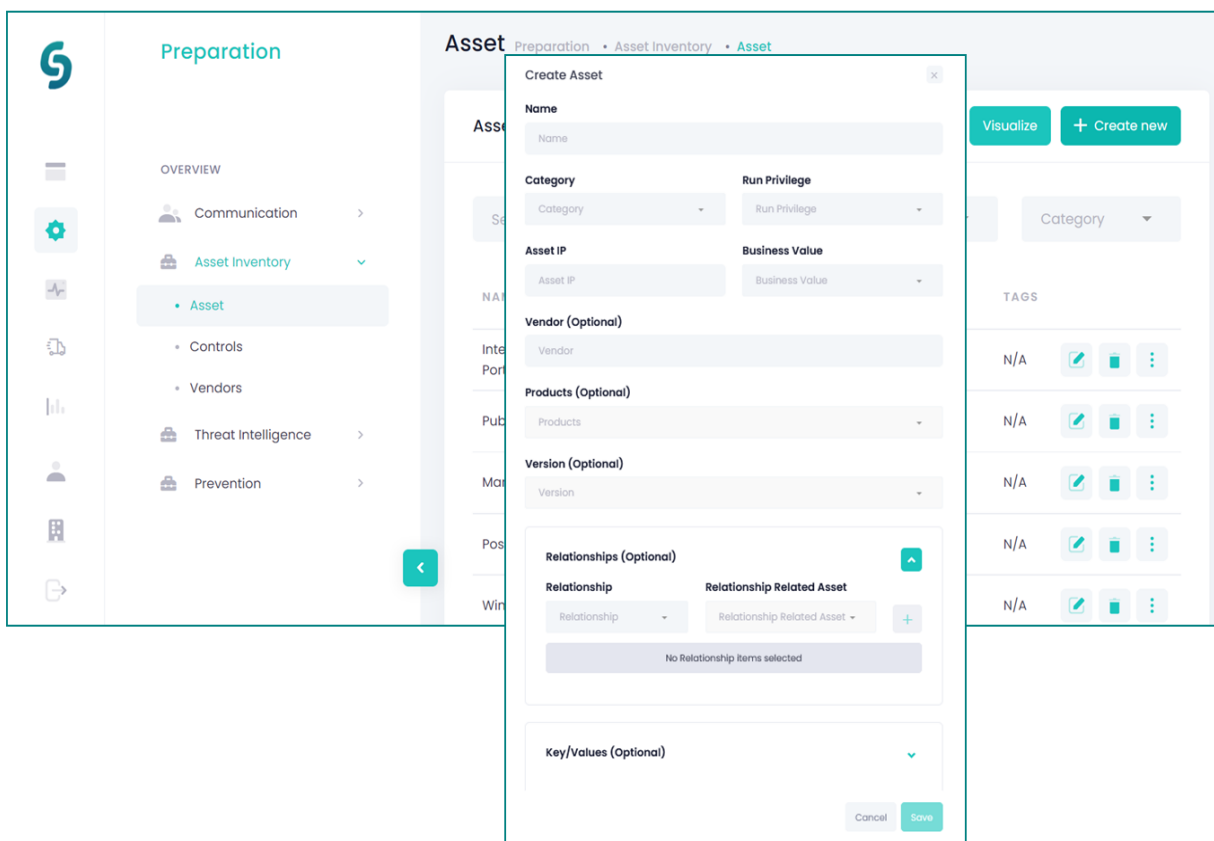
To create an asset, select “Asset Inventory” from the “Preparation” phase of the dashboard menu and then in the “Assets” page select “Create new” option. A “Create Asset” editor appears where the Security Professional can add several attributes of the asset:

- Asset Name: Provide the name of the asset
- Asset Category: Declare the asset category from a default dropdown list (e.g. Application/Operating System, Data/Database, Application/Business, etc)
- Run Privilege: Indicate privilege on the asset (Domain admin, Domain user, Local admin, local user)
- Asset IP: Provide asset's IP (Optional)
- Business value: estimate asset's value to the organisation from dropdown qualitative values (required for the risk assessment process)
- Vendor: Select a vendor from a dropdown list. In case a new vendor must be edited, the vendor must be declared before the asset's creation following the process in section 4.2.3.2 (Optional)
- Products: Declare asset's product type from a dropdown list (Optional)

## D9.2 – Training Materials and Report on Training Processes

- Version: Declare the version of the asset's product type from a dropdown list (Optional)
- Relationships: Set a relationship between the asset and another asset of the organisation by providing the type of the relationship and the related asset (Optional)

After providing the proper information, click on the “Save” button. By filling the above asset attributes, the CyberSANE system is able to identify the asset's Common Platform Enumeration (CPE)<sup>47</sup> in order to use it to automatically recognize asset's vulnerabilities from open repositories, e.g. Common Vulnerabilities and Exposure (CVE) of MITRE<sup>48</sup>. Thereby, the Security Professional can get a generic idea of the security status for each asset (non-real-time).



The screenshot displays the CyberSANE user interface for asset registration. On the left, a sidebar contains a navigation menu with icons for Overview, Communication, Asset Inventory, Controls, Vendors, Threat Intelligence, and Prevention. The 'Asset Inventory' section is expanded, showing a list of assets. The main content area is titled 'Create Asset' and contains several input fields and dropdown menus. These include: Name, Category, Asset IP, Vendor (Optional), Products (Optional), Version (Optional), Relationships (Optional), and Key/Values (Optional). The Relationships section shows a table with columns for Relationship and Relationship Related Asset. A 'Visualize' button is located at the top right of the main area, and a 'Create new' button is at the bottom right. The interface is clean and modern, with a light blue and white color scheme.

Figure 19: Screens from the Asset registration process in CyberSANE.

### 4.2.1.3 Assets visualization

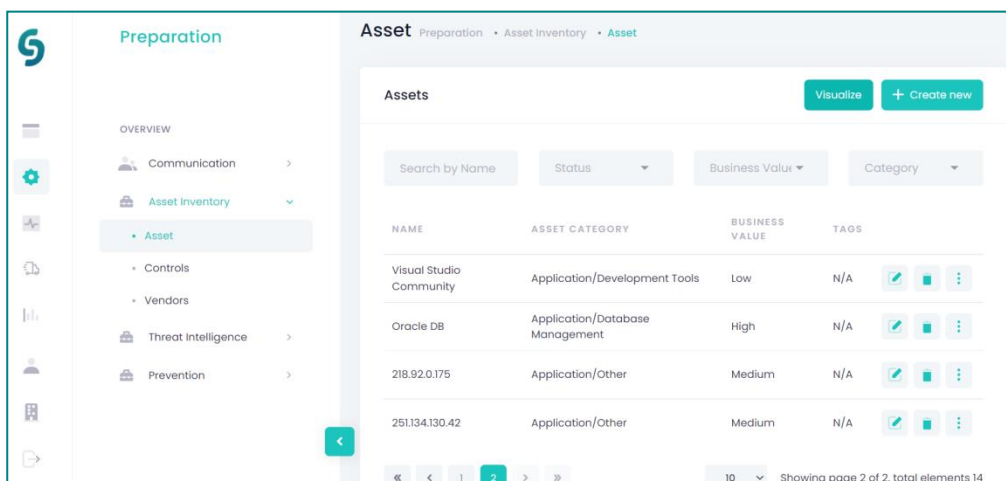
Preparation -> Asset Inventory -> Asset -> Visualize

<sup>47</sup> <https://nvd.nist.gov/products/cpe>

<sup>48</sup> <https://cve.mitre.org/>

## D9.2 – Training Materials and Report on Training Processes

The Security Professional can explore graphs and further security details of the organisation's registered assets by selecting the "Asset Inventory" from the Preparation category of the dashboard menu and pressing the button "Visualize" from the "Assets" page (Figure 20). A visualization of the organisation's asset inventory appears illustrating the declared assets relationships in the context of developed asset graphs (Figure 21). Upon clicking on a specific registered asset (asset node), an asset "Footprint" button appears (Figure 22).



NAME	ASSET CATEGORY	BUSINESS VALUE	TAGS
Visual Studio Community	Application/Development Tools	Low	N/A
Oracle DB	Application/Database Management	High	N/A
218.92.0.175	Application/Other	Medium	N/A
251.134.130.42	Application/Other	Medium	N/A

Figure 20: The "Visualize" button produces asset graphs and provides security-related information.

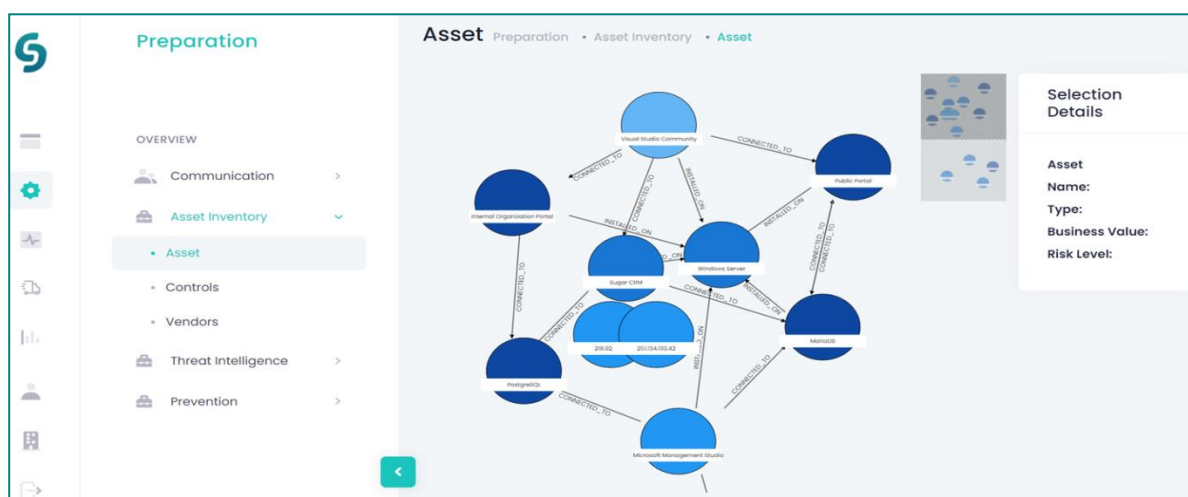


Figure 21: A visualization of an organisation's assets graph.

## D9.2 – Training Materials and Report on Training Processes

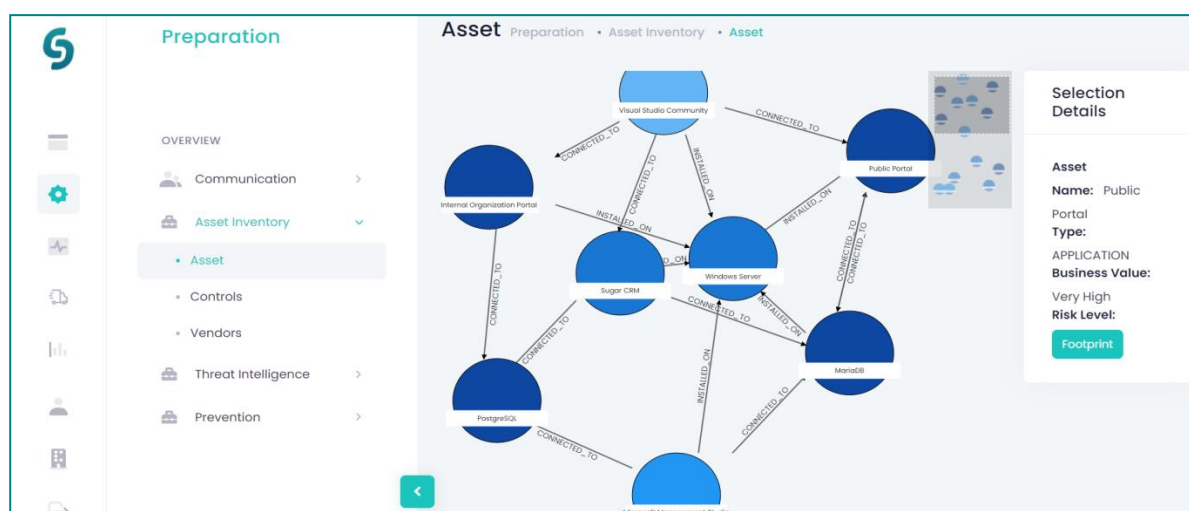


Figure 22: An asset “Footprint” button appears upon clicking on a specific asset, herein on the “Public Portal”.

The asset footprint presents information about the probability of all identified threats and the impact of all identified vulnerabilities on a specific asset displayed through a heatmap. By hitting the asset “Footprint” button, the Security Professional can review this asset’s threats and vulnerabilities matrix (Figure 23). In addition, he/she can explore further options, such as print and saving options, by tapping on the ≡ (three dashes) icon (Figure 23).

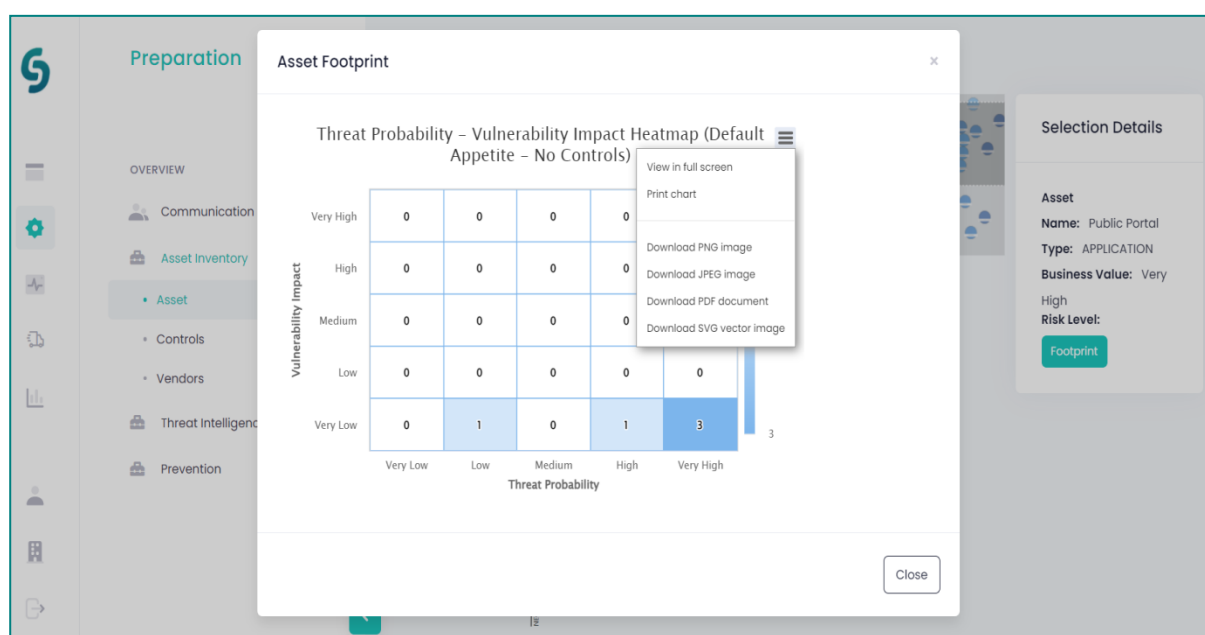


Figure 23: The asset “Public Portal” footprint displaying the asset’s threat probability and vulnerability impact heatmap.

Over a specific value of the developed “Threat Probability – Vulnerability Impact Heatmap” click (Figure 24), the Security Professional can explore tuples of threats and vulnerabilities combinations for the asset (Figure 25).

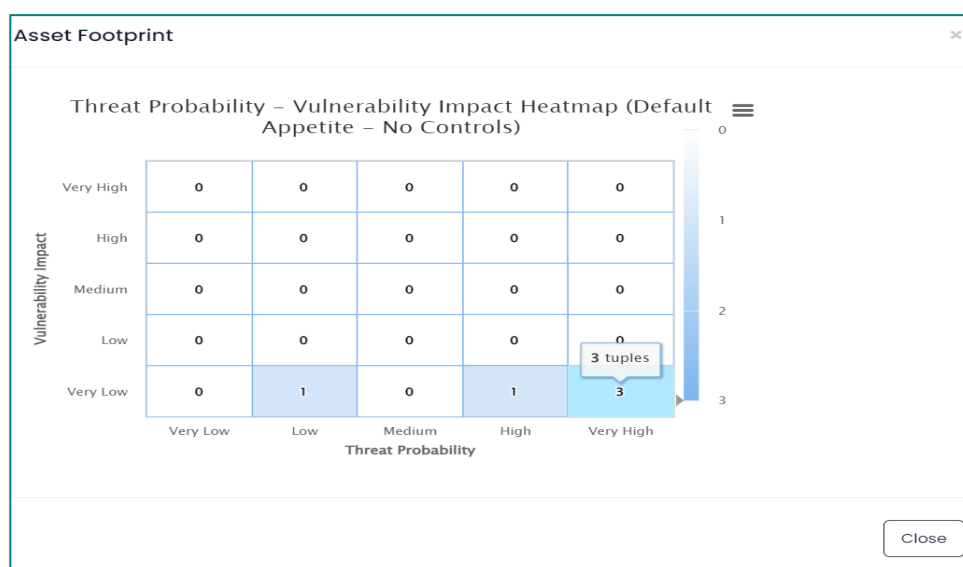


Figure 24: Selection of “Very low” Vulnerability impact and “Very High” threat probability combination to explore the generated tuples for the “Public Portal” asset.

Asset Footprint			
THREAT	PROBABILITY	VULNERABILITY	IMPACT
Flooding-1	VH	CVE-2007-5621	Very Low
HTTP DoS	VH	CVE-2007-5621	Very Low
Authentication Abuse	VH	CVE-2007-5621	Very Low

Figure 25: Tuples of identified threats and vulnerabilities for the “Public Portal” asset.

## 4.2.2 Controls Management

The “Controls Management” functionality of the CyberSANE system provides the opportunity to the Security Professional to add security controls implemented on the organization’s assets, to review and manage them.

### 4.2.2.1 Manage Security Controls

Preparation -> Asset Inventory -> Controls

The Security Professional can view and manage security controls by selecting the “Controls” category from the “Asset Inventory” which can be reached from the “Preparation” phase of the dashboard menu (Figure 26). The controls can be searched by its attributes, i.e. either by “Name” or the “Library” retrieved from (e.g. CyberSANE repository, ISO/IEC 27001, NIST) or “Type” (whether they mitigate threat or vulnerabilities) or their “Description”.

## D9.2 – Training Materials and Report on Training Processes

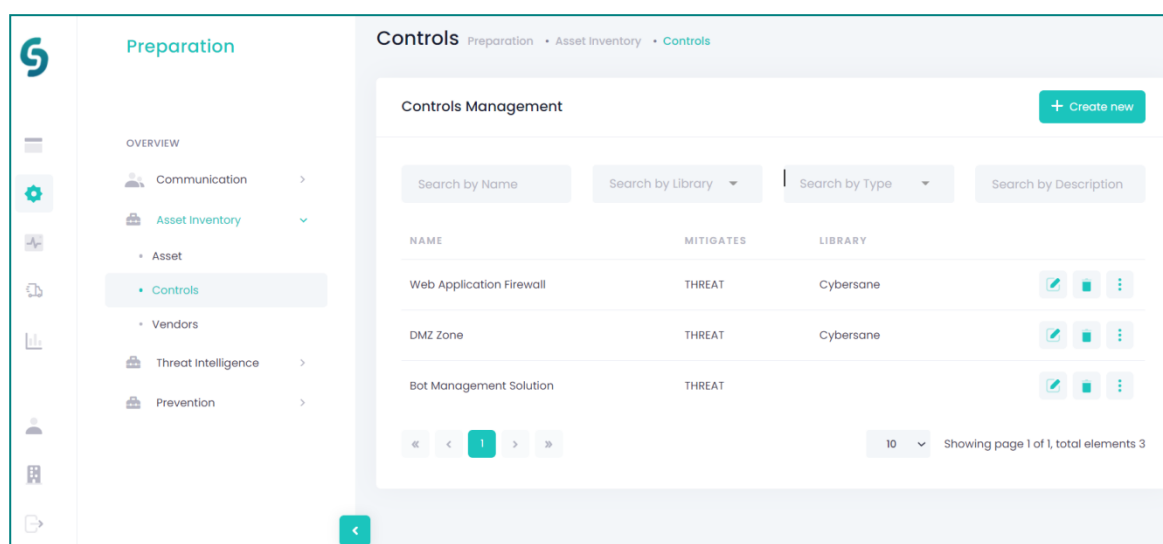


Figure 26: A list of all controls appears in the “Controls Management” page.

Similarly with the assets, the declared controls can be edited or deleted by clicking on the pen icon or bin icon accordingly (cf. section 4.2.1) in the Controls Management page (Figure 27). Information about the threats or vulnerabilities that are mitigated by the specific control can be viewed and managed (add new or delete existing ones) (Figure 28) by clicking on the three dots icon (cf. section 4.2.1) (Figure 26).

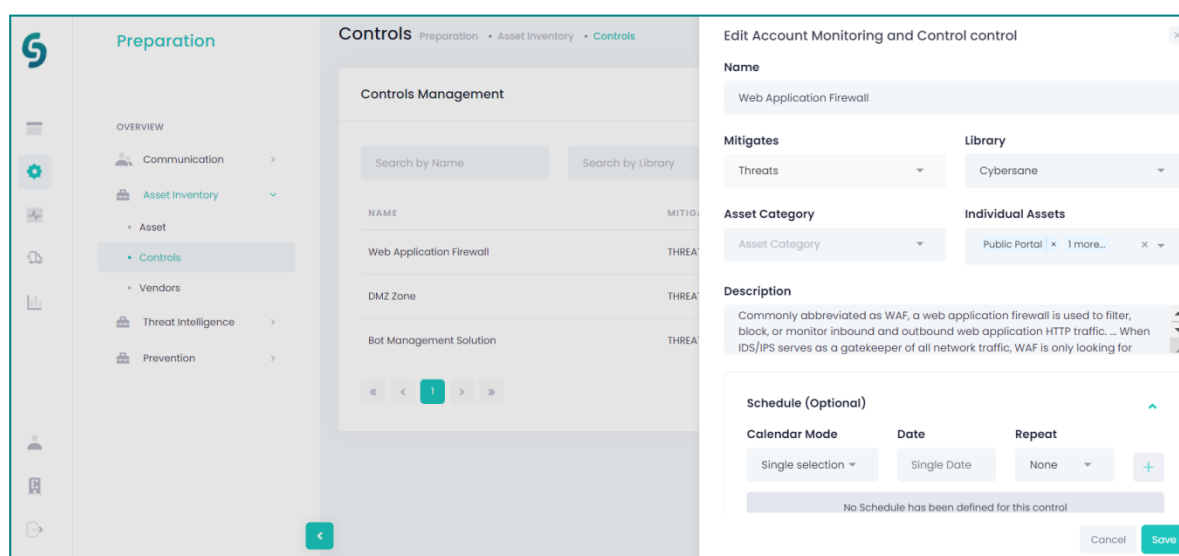


Figure 27: Security controls can be viewed in each details or edited. The current figure shows details for the “Web Application Firewall” security control from the CyberSANE control editor.

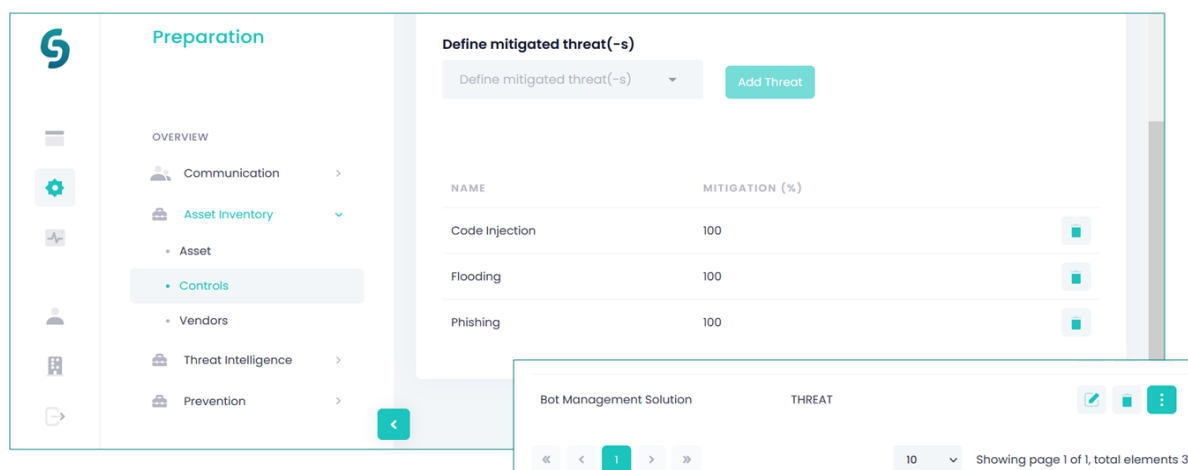


Figure 28: Example of managing threats for the “Bot Management Solution” security control.

#### 4.2.2.2 Create a Security Control

Preparation -> Asset Inventory -> Controls

Organization’s implemented security controls can be registered in the asset inventory and connected to the corresponding asset. To create a security control, select “Asset Inventory” from the “Preparation” category of the dashboard menu and then select “Controls”. Afterwards, press the button “Create New” from the “Controls Management” page (Figure 26). To add a new control and connect it with the specific vulnerabilities and threats that mitigates on the respective asset fill in the requested fields:

- Provide control’s name
- Select the control type in the “Mitigates” field (to indicate whether the control mitigates a vulnerability or threat)
- Refer to the open repository where the vulnerability or threat is recognized in the “Library” field.
- Define the asset type (e.g. Application/Operating System, Data/Database, Application/Business, etc) upon which the specific control is implemented in the “Asset Category” field
- Select the names of the assets upon which the specific control is implemented in the “Individual Assets” field
- Provide a description of the implemented control in the “Description” field
- Create schedule(s) to review and make proper changes/updates on a daily/weekly/monthly/annual basis (optional)

After providing the proper information, click on the “Save” button. The following Figure 29 shows the editor for creating a new security control and connecting it with assets and threats or vulnerabilities.

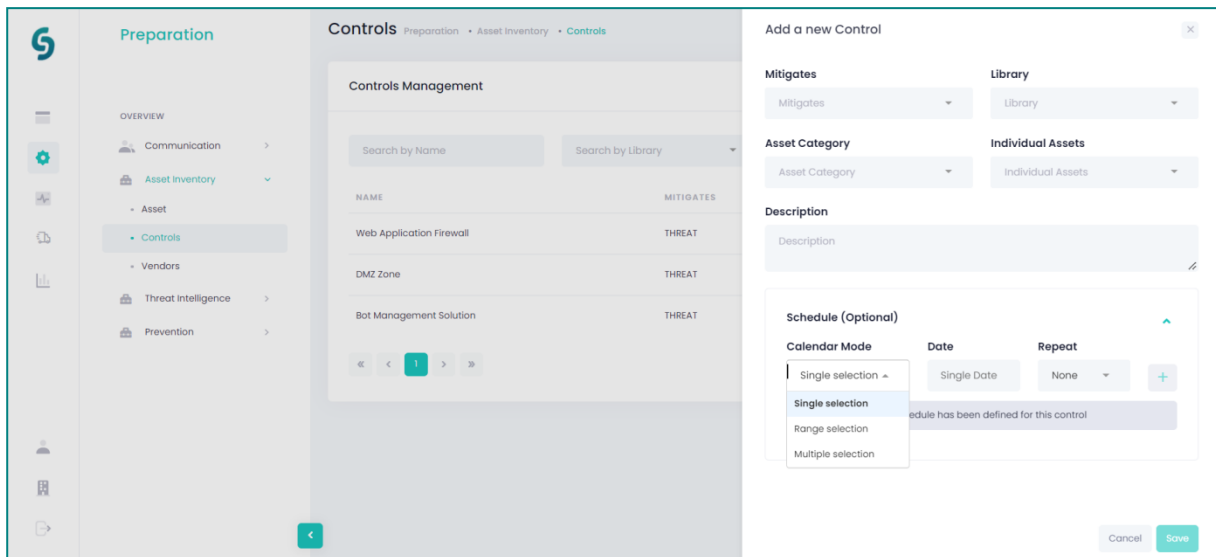


Figure 29: A view of the “Add a new Control” editor

### 4.2.3 Vendors Management

The “Vendors Management” CyberSANE functionality delivers an asset vendor repository allowing the Security Professional to explore and manage existing asset vendors or add new asset vendors that are not included in the vendors list (e.g. in case of custom/inhouse assets).

#### 4.2.3.1 Manage Vendors

Preparation -> Asset Inventory -> Vendors

Asset vendors can be managed by selecting the “Vendors” category from the “Asset Inventory” which can be found in the “Preparation” phase from the dashboard menu (Figure 31).

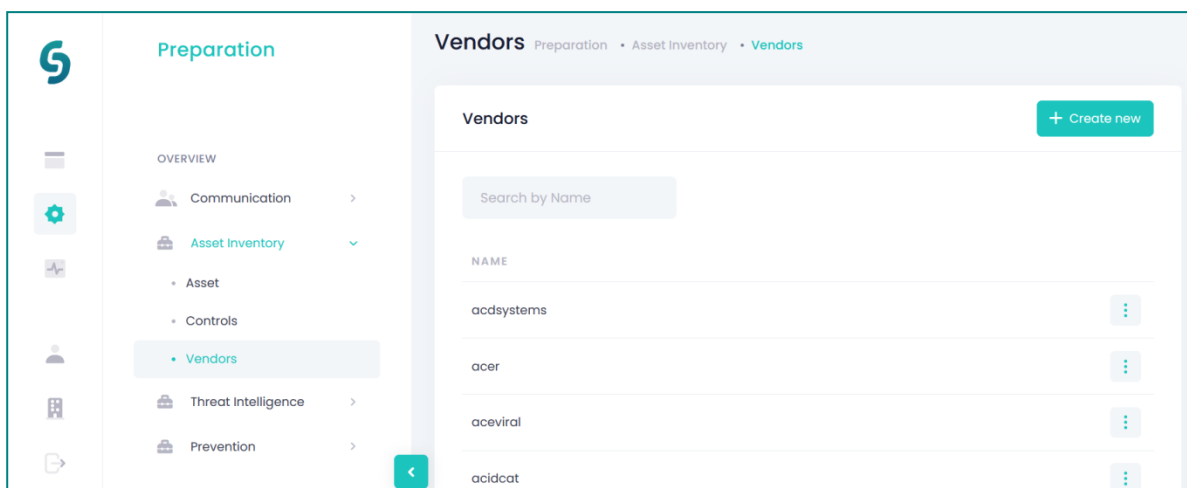


Figure 30: Vendors Management menu.



## D9.2 – Training Materials and Report on Training Processes

Vendors can be searched by their Name as shown in Figure 32. Please notice that only manually added vendors can be edited or deleted by clicking on the pen icon or bin icon accordingly from the Vendors Management menu (Figure 31).

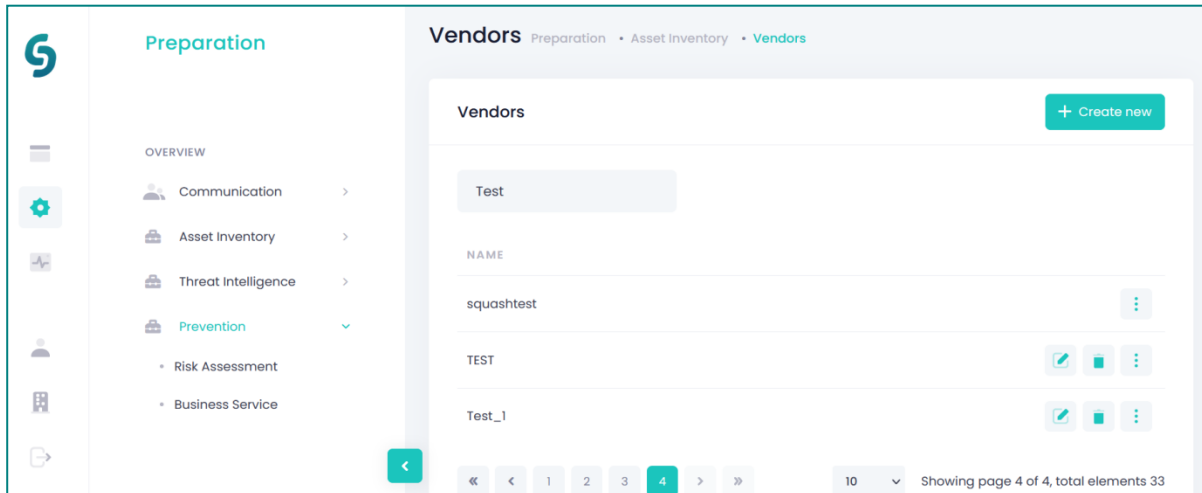


Figure 31: Manually created vendors can be edited or deleted.

Information about the products that reside in a vendor can be viewed by clicking the three dots icon from the Vendors Management menu.

**Example:** Figure 32 shows how to search and view the respective products of the Vendor "Microsoft".

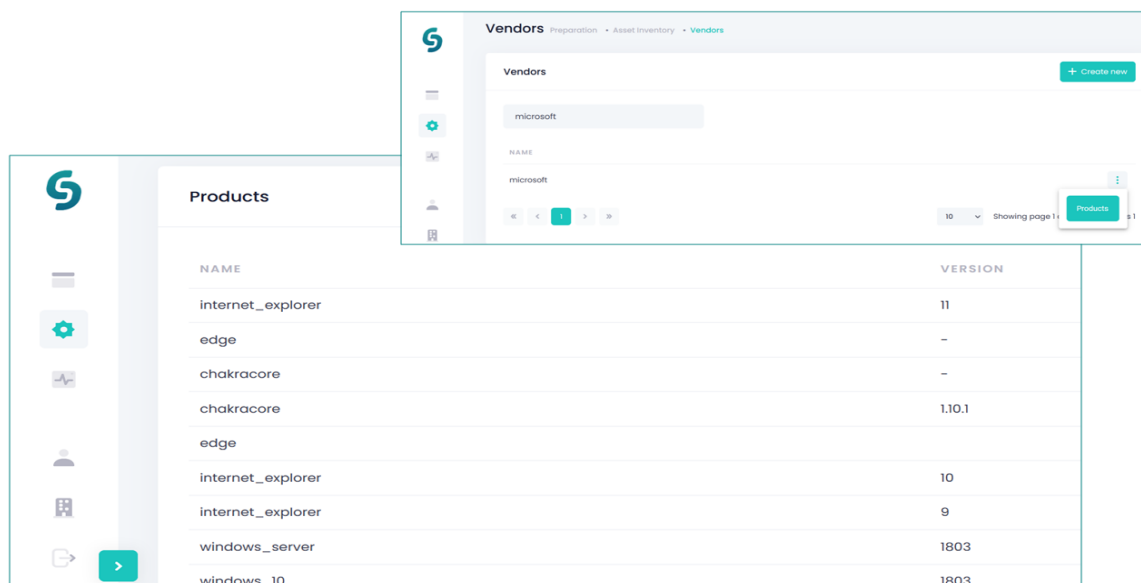


Figure 32: View of a vendor's products.

### 4.2.3.2 Declare a new Vendor

Preparation -> Asset Inventory -> Vendors

To add a new vendor, click on the “Vendors” category from the “Asset Inventory” which is in the “Preparation” phase of the dashboard menu and press the “Create New” button (Figure 31).

## 4.3 Threat Intelligence

Threat Intelligence is a category of the “Preparation” phase which can be reached from the dashboard menu (Figure 33). It provides the following four functionalities:

- Vulnerabilities Management
- Threats Management
- Attack Scenarios Management
- Risk Appetites Management

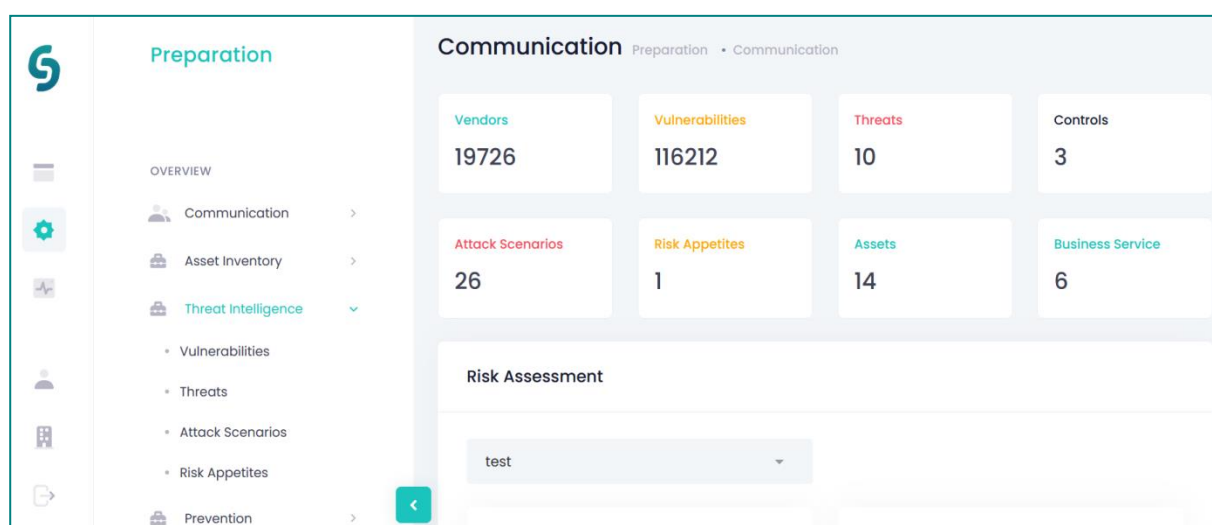


Figure 33: Threat Intelligence functionalities.

### 4.3.1 Vulnerabilities Management

The “Vulnerabilities Management” functionality of CyberSANE provides to the Security Professional a vulnerability repository of confirmed vulnerabilities, which he/she can explore along with their attributes. In addition, the CyberSANE system gives the opportunity to the Security Professional to manually add vulnerabilities (i.e. unknown/zero-day).

#### 4.3.1.1 Manage Vulnerabilities

Preparation -> Threat Intelligence -> Vulnerabilities

Vulnerabilities can be managed from the Vulnerabilities Management menu, which can be viewed by selecting “Vulnerabilities” from the “Threat Intelligence” options of the “Preparation” phase from the dashboard menu. The CyberSANE system provides an

## D9.2 – Training Materials and Report on Training Processes

exhaustive list of vulnerabilities and their details based on CVSS 2.0 of FIRST<sup>49</sup> derived from the open repository of NIST Vulnerabilities Database<sup>50</sup> (Figure 34).

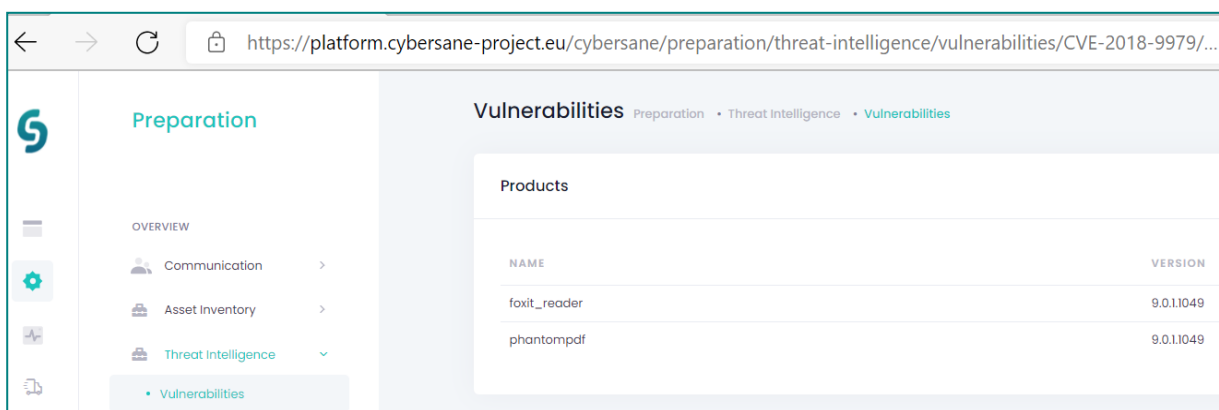


ID	BASE SCORE	EXPLOITABILITY	IMPACT	PUBLISHED	LIBRARY
CVE-2021-34629	5	10	2.9		NIST
CVE-2021-38714	9.3	8.6	10		NIST
CVE-2021-41039	5	10	2.9		NIST
CVE-2021-41099	6.8	8.6	6.4		NIST
CVE-2021-42097	9.3	8.6	10		NIST
CVE-2021-42771	10	10	10		NIST
CVE-2021-44026	7.5	10	6.4		NIST
CVE-2021-44143	7.5	10	6.4		NIST
CVE-2021-44228	9.3	8.6	10		NIST
CVE-2021-44847	5	10	2.9		NIST

Figure 34: A screen from the “Vulnerabilities Management List”.

Vulnerabilities can be searched by their ID or description from the “Vulnerabilities Management List”. Only manually created vulnerabilities (unknown/zero-day) can be edited or deleted by clicking on the pen and bin icons respectively. The known affected products (without considering potential implemented security controls on assets within the organisation) can be viewed upon clicking on the three dots icon from the “Vulnerabilities Management List” (Figure 34).

**Example:** An illustrative example of the known affected products in view of the exploitation of vulnerability CVE-2018-9979 is provided in Figure 35.



NAME	VERSION
foxit_reader	9.0.1.1049
phantompdf	9.0.1.1049

Figure 35: Known affected products from the vulnerability CVE-2018-9979 exploitation.

<sup>49</sup> <https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator>

<sup>50</sup> <https://nvd.nist.gov/vuln>

### 4.3.1.2 Create a Vulnerability (Unknown/Zero-day)

Preparation -> Threat Intelligence -> Vulnerabilities

The Security Professional can create unknown/zero-day vulnerabilities by entering the “Vulnerabilities” category from “Threat Intelligence” of the “Preparation” phase of the dashboard menu and tap on the “Create new” button in the “Vulnerabilities Management List” page (Figure 36). An editor to create the vulnerability appears (Figure 36).

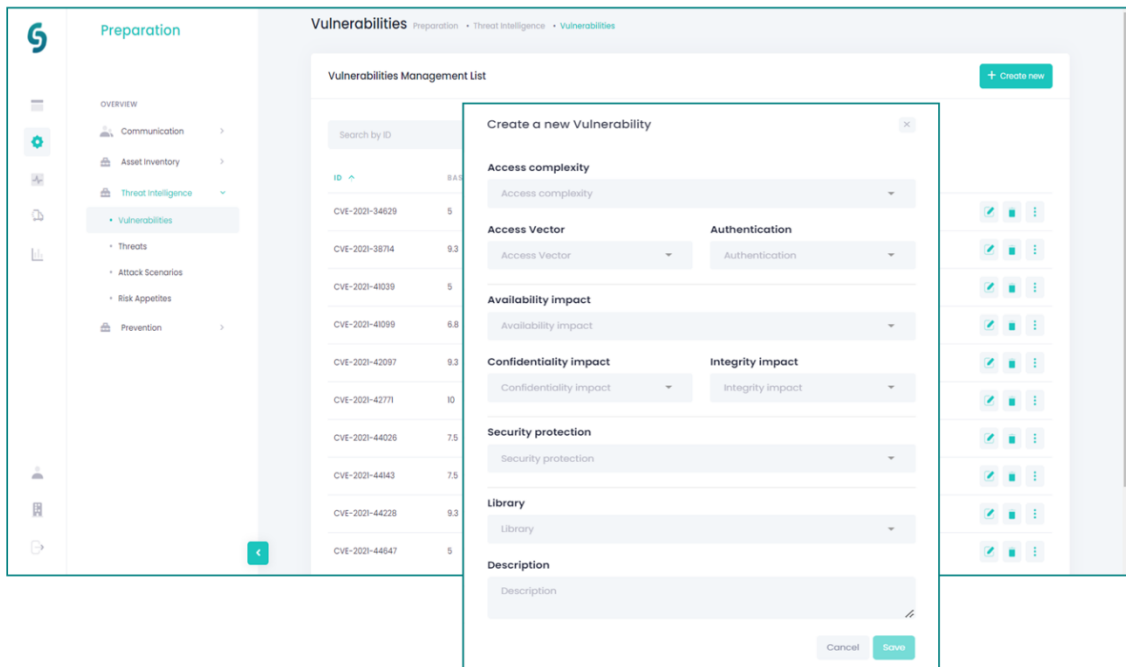


Figure 36: Screens to create an unknown/zero-day vulnerability.

## 4.3.2 Threats Management

The “Threat Management” functionality of CyberSANE offers to the Security Professional the capability to review, manage or register security threats.

### 4.3.2.1 Manage Threats

Preparation -> Threat Intelligence -> Threats

Threats can be managed from the Threats Management menu, which can be viewed by selecting “Threats” option from “Threat Intelligence” which is under the “Preparation” phase of the dashboard menu (Figure 37). The CyberSANE system provides an exhaustive list of threats derived from open threat repositories (i.e. ISO/IEC 27001, NIST). Threats can be searched either by threat identifier or name or library or description in the “Threats Management” page. Only manually developed threats can be edited or deleted by the pen and bin icons respectively (Figure 37).

## D9.2 – Training Materials and Report on Training Processes

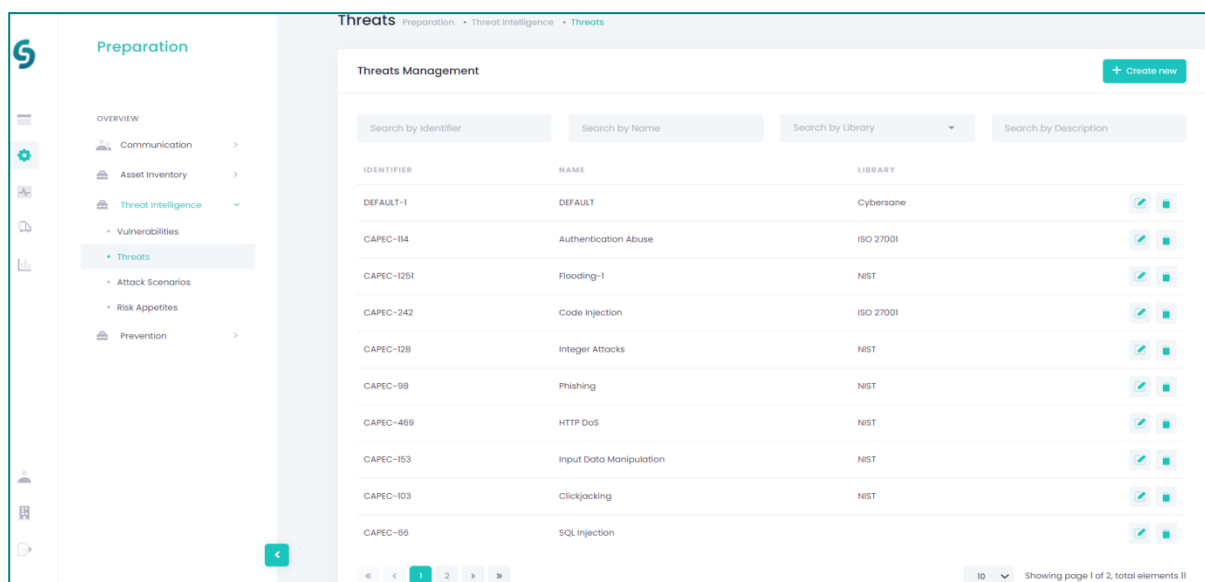


Figure 37: A screen of threats list from the “Threats Management” page.

### 4.3.2.2 Register a threat

The Security Professional can register specific threats that could affect one or more assets within the organisation. To do so, he/she shall enter the “Preparation” phase from the dashboard menu, select “Threats Intelligence” and then “Threats”. The “Threats Management” page appears and a new threat can be created when hitting the “Create New” button (Figure 37). To register a threat, the Security Professional shall fill in the requested threat information and then press the “Save” button (Figure 38).

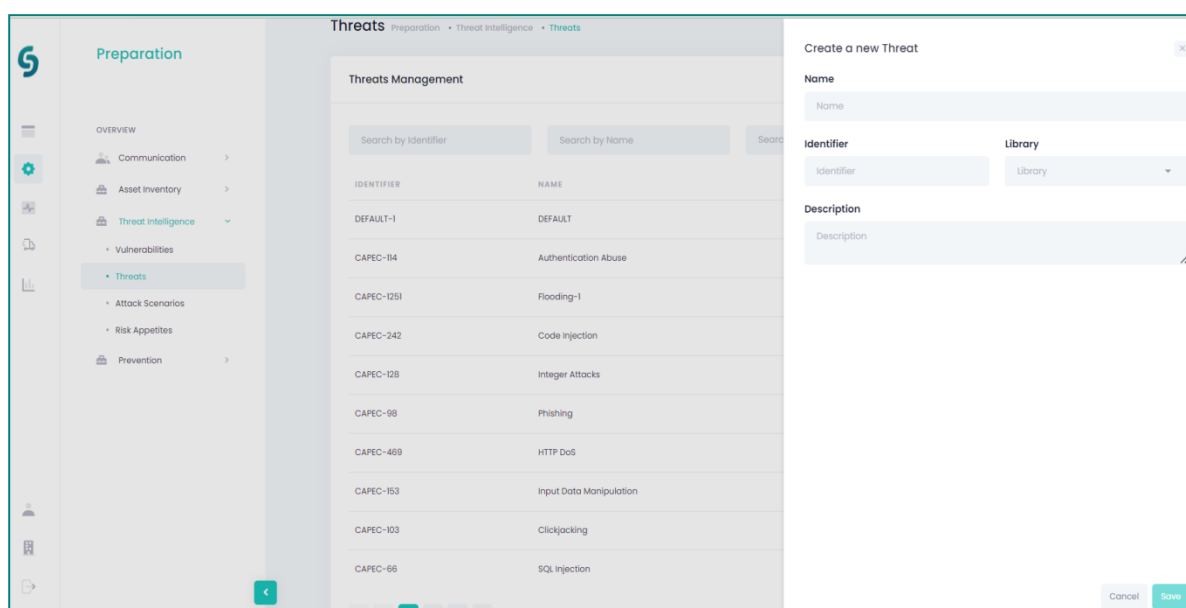


Figure 38: Register a threat.

### 4.3.3 Attack Scenarios Management

With this functionality the CyberSANE system allows the Security Professional to experiment on threat cases by interrelating threats with corresponding vulnerabilities on specific assets of the organisation.

#### 4.3.3.1 Manage Attack Scenarios

Preparation -> Threat Intelligence -> Attack Scenarios

Attack scenarios Management functionality gives the opportunity to the Security Professional to develop, view or manage threat cases of threats interrelations with given vulnerabilities and with specific assets of the organisation. Attack scenarios can be searched upon their denoted category, threat, corresponding vulnerability(ies) or provided scenario description. Threat scenarios can be deleted from the bin icon (Figure 39).

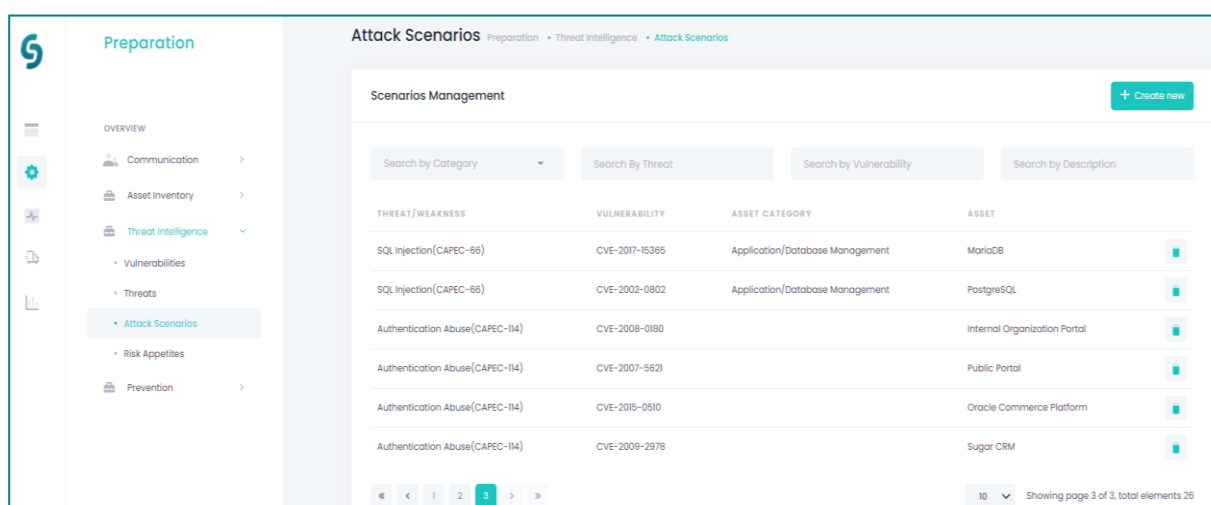


Figure 39: Attack scenarios Management screen.

#### 4.3.3.2 Create an Attack Scenario

Preparation -> Threat Intelligence -> Attack Scenarios

The Security Professional can create a new attack scenario when choosing from the “Preparation” phase of the CyberSANE dashboard menu the “Threats Intelligence” and “Attack Scenarios” options subsequently. Afterwards, from the “Scenarios Management” page he/she shall push the “Create new” button (Figure 39) and fill in the requested fields (Figure 40).

## D9.2 – Training Materials and Report on Training Processes

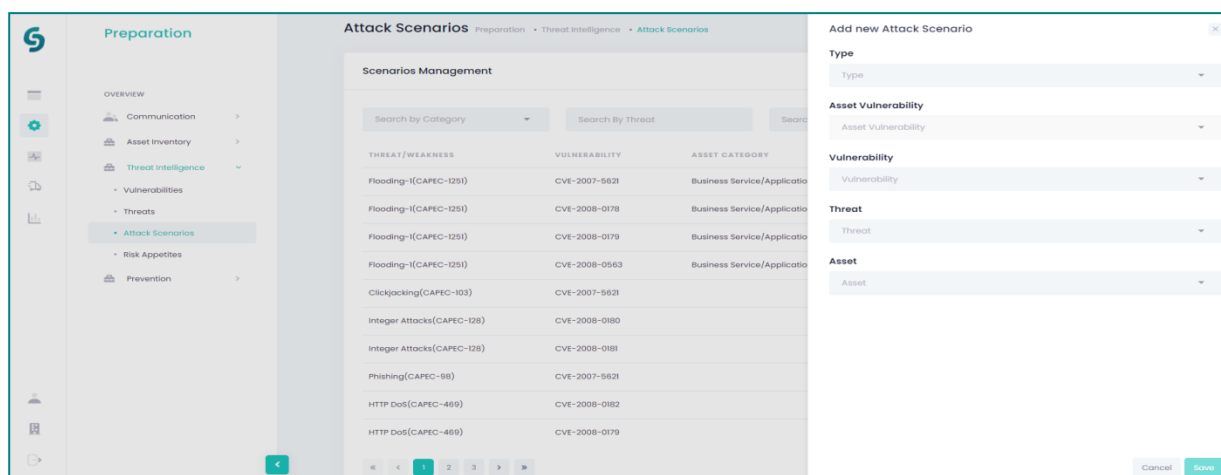


Figure 40: Attack scenario development.

### 4.3.4 Risk Appetites Management

The Risk Appetite functionality can provide the capability to the Security Professional to define risk appetites. The risk appetite is considered the likelihood of occurrence of a given threat. This functionality gives to the Security Professional configurable options to adjust the threat probability according to organisation's conditional expectations and preferences. These configurations will be considered in the risk assessment process (cf. section 4.4.1).

#### 4.3.4.1 Manage Risk Appetites

Preparation -> Threat Intelligence -> Risk Appetites

To manage risk appetites, the Security Professional shall enter the "Preparation" phase from the dashboard menu and select "Threat Intelligence" and "Risk Appetites" categories subsequently. The "Risk Appetites Management" page appears (Figure 41).

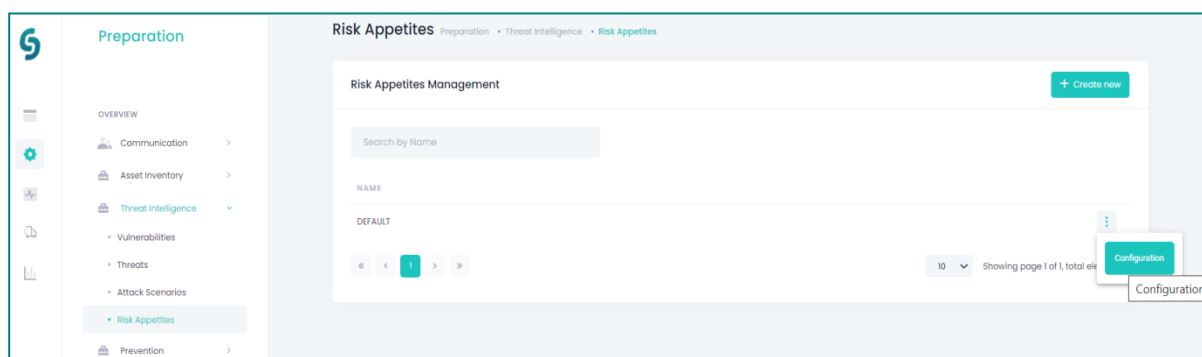


Figure 41: A screen of the "Risk Appetite Management" page.

By clicking on the three dots icon (Figure 41) and hitting the configuration button a list of threat probability appears (Figure 42). The default threat probability values are retrieved

from the MITRE threat catalogue<sup>51</sup>. The Security Professional can review and adjust the probability values according to organisation's conditions and preferences (Figure 42). The defined threat probability values will be considered for the risk assessment (cf. section 4.4.1).

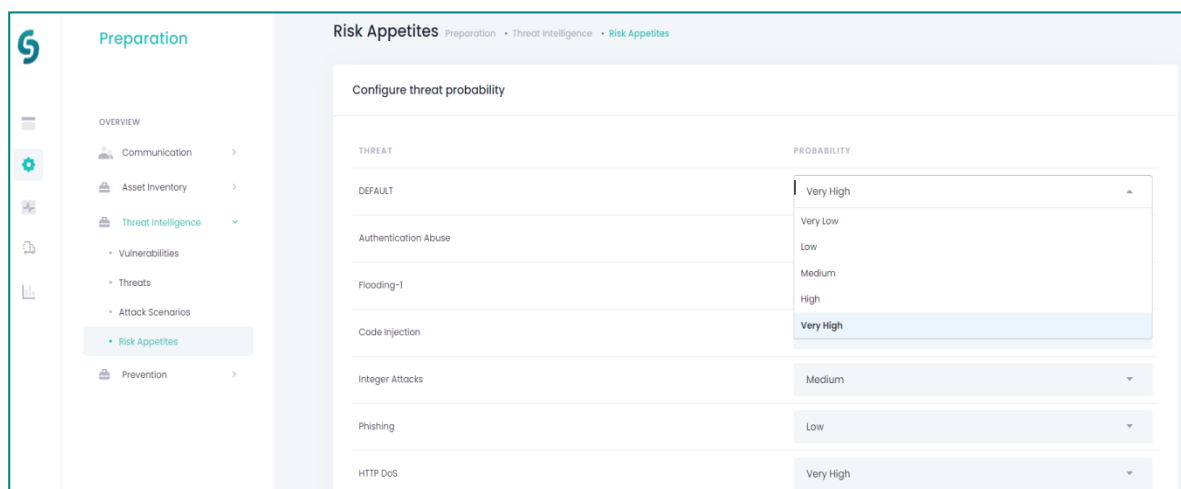


Figure 42: Configure threat probability capability to define risk appetite.

#### 4.3.4.2 Create a Risk Appetite

To create a new risk appetite, the Security Professional shall go to the “Preparation” phase from the dashboard menu and select “Threat Intelligence” and “Risk Appetites” categories successively. Afterwards, by tapping on the “Create new” button (Figure 42) in the “Risk Appetites Management” page, the Security Professional shall add a new risk appetite and press “Save” (Figure 43).

<sup>51</sup> <https://capec.mitre.org/>



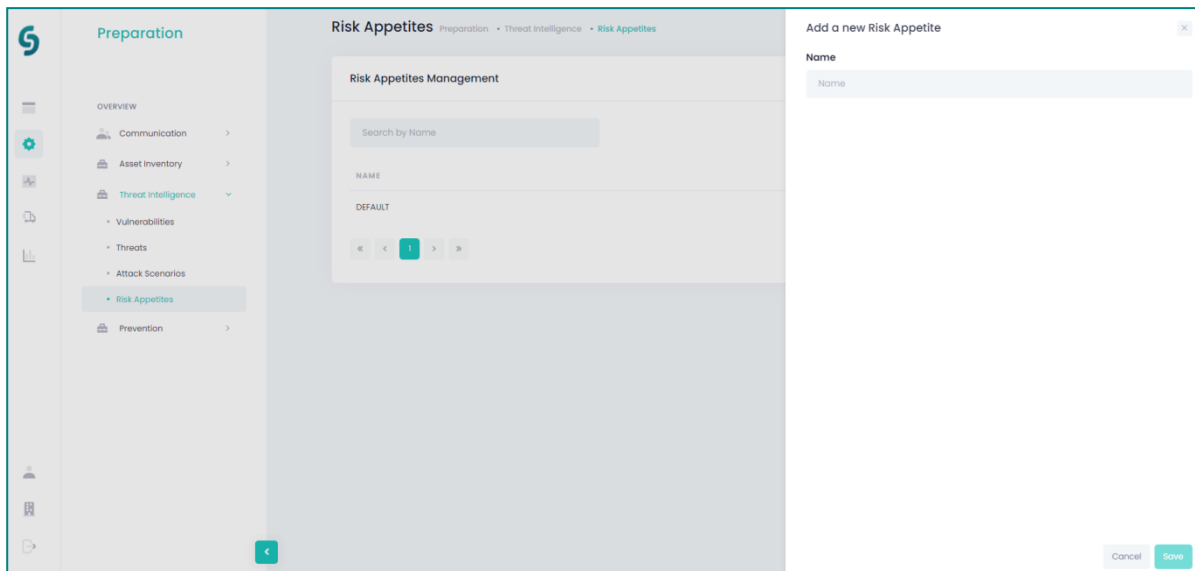


Figure 43: Add a new risk appetite.

The default threat probability values are retrieved from the CAPEC threat catalogue of MITRE (cf. 4.3.4.1). The Security Professional can set a new scenario by adjusting the threat probability values according to his/her preferences (e.g. how often a threat is likely to appear to the organisation's corresponding assets) following the process in Section 4.3.4.1.

## 4.4 Prevention

Prevention is a category of the “Preparation” phase which can be reached from the dashboard menu (Figure 44). It provides the following two functionalities:

- Risk Assessment
- Business Service

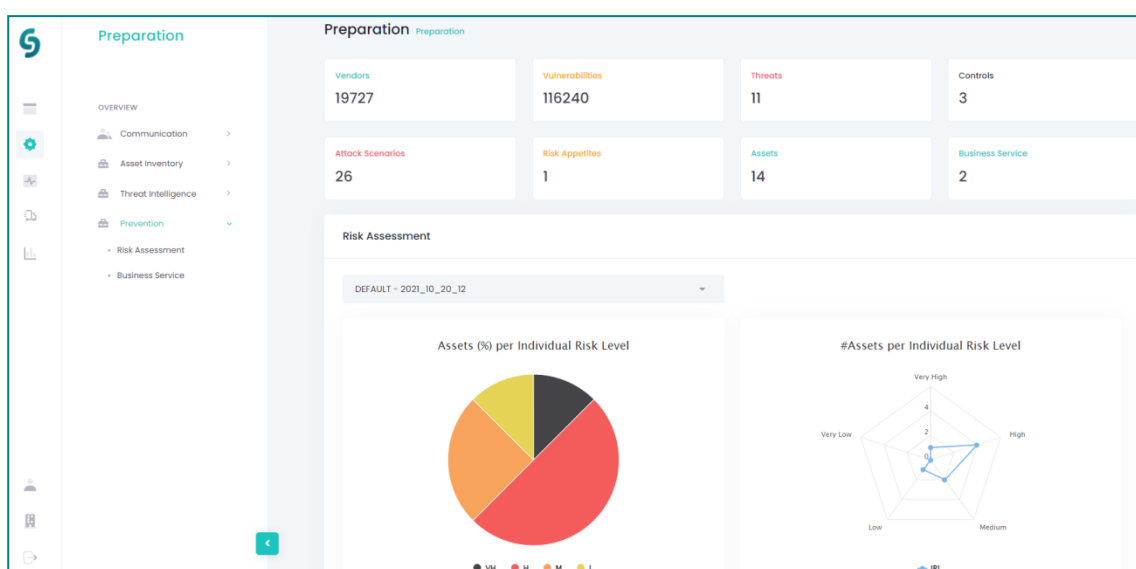


Figure 44: Prevention functionalities of the Preparation phase.

#### **4.4.1 Risk Assessment**

Risk Assessment functionality allows the Security Professional to manage or conduct a risk assessment process at the preparation phase of incident handling and review risks, threats and vulnerabilities results on declared assets of an organisation's Business Service (cf. section 4.4.2). The risk assessment functionality takes into account all the configurations set by the Security Professional (e.g. security controls, risk appetite, zero-day vulnerabilities). All assets and additional security-related configurations must be set before the "Detection and Analysis" phase of the incident handling process. Nevertheless, after performing the "Detection and Analysis" phase operations (cf. section 5), the Security Professional can optionally go back to the "Preparation" phase of the CyberSANE system and from the "Threat Intelligence" and "Risk Appetite" options create a new threat or change a threat's level respectively based on the real evidence provided. Once completing adjusting security options on the organisation's assets upon real evidence, the Security Professional can perform a new risk assessment on the assets to be more concrete on the results.

##### **4.4.1.1 Initiate a Risk Assessment**

Preparation -> Prevention -> Risk Assessment

To initiate a Risk Assessment, the Security Professional shall select from the "Preparation" phase of the dashboard menu the "Prevention" category, then click on the "Risk Assessment" functionality and press the "Create new" button from the "Risk Assessment" main page (Figure 45). The "Create Risk Assessment" tab appears (Figure 46). The Security Professional shall fill the requested fields (Figure 46):

- Name: a descriptive name of the Risk Assessment has to be provided
- Process: a Business Service, including all the assets related on this service must be selected from the default list. To create a new Business Service, the Security Professional shall register the Business Service in CyberSANE from the "Business Service" functionality of the "Prevention" category of the "Preparation" phase (see section 4.4.2) before the risk assessment. The CyberSANE system will perform risk assessment on the assets of the selected Business Service
- Type (Real/No Controls): indicate the type of the risk assessment. In case of selecting the "Real" risk assessment type, all configurations concerning implemented security controls on assets declared by the Security Professional are considered during the calculations of the risk assessment performance. Upon selecting "No Controls" type, the risk assessment calculations ignore the security controls that may have been declared on the organisation's assets.
- Risk Appetite: indicate the Risk Appetite (see section 4.3.4) from a dropdown list.

After fulfilling all the proper information, the Security Professional shall press "Save" (Figure 46). The risk assessment is performed.

## D9.2 – Training Materials and Report on Training Processes

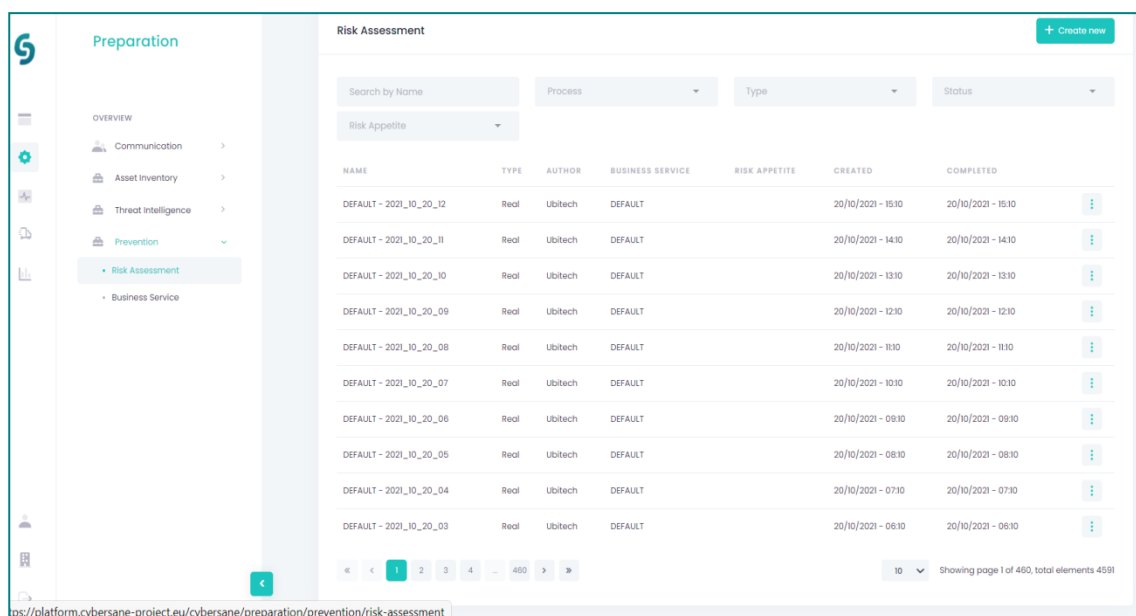


Figure 45: Risk Assessment main page.

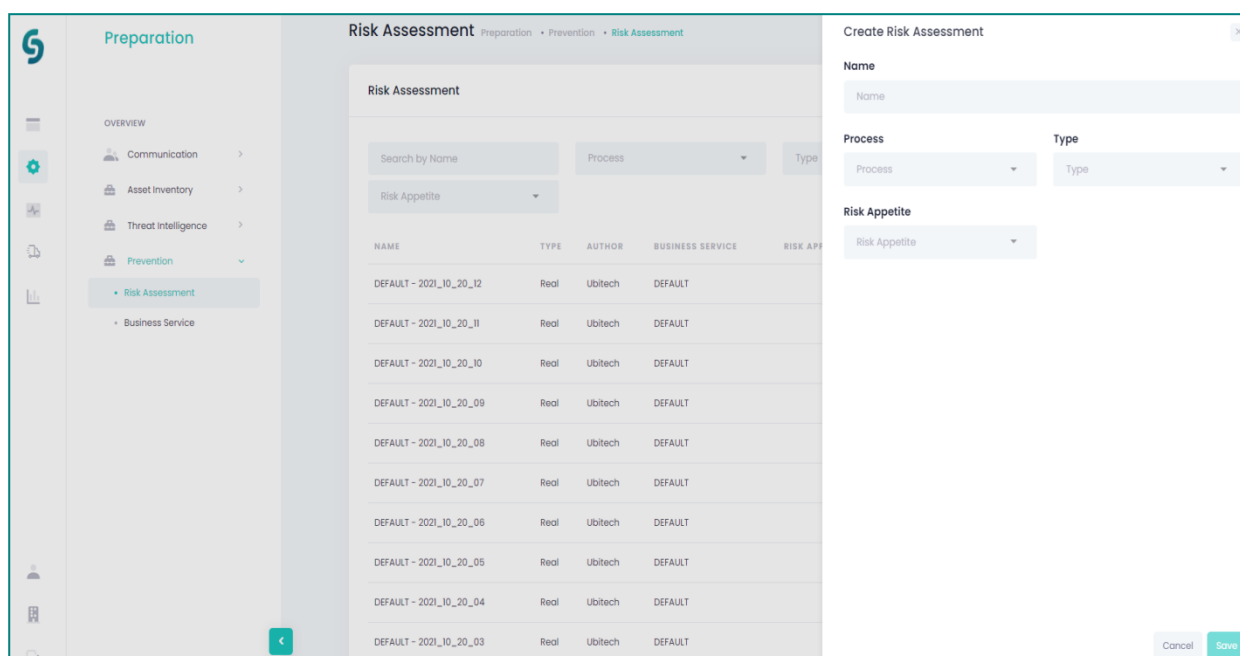


Figure 46: Initiate a Risk Assessment

### 4.4.1.2 Review Risk Assessment results

Preparation -> Prevention -> Risk Assessment

To reach the Risk Assessment functionality, the Security Professional shall select from the “Preparation” phase of the dashboard menu the “Prevention” category and the click on the “Risk Assessment” (Figure 45). Risk Assessment performances can be viewed and searched either by name, process, type or risk appetite from the main Risk Assessment page (Figure 45). The output of a risk assessment performance at the

## D9.2 – Training Materials and Report on Training Processes

preparation phase of the incident handling process can be viewed by clicking on the three dots icon (Figure 47).

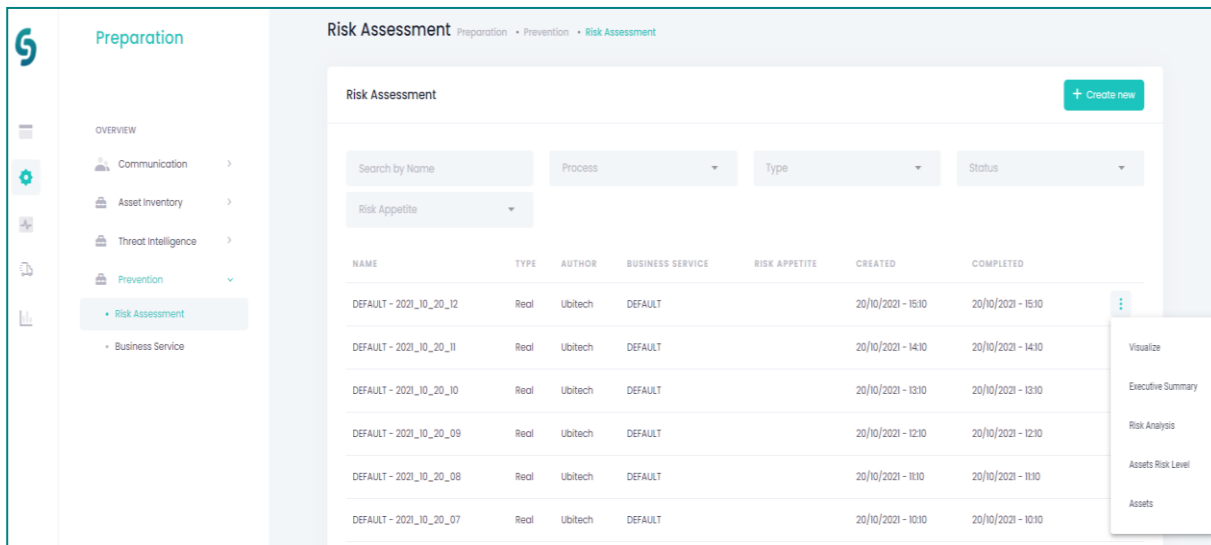


Figure 47: Risk Assessment results different options.

As shown in the figure above, Risk Assessment results can be explored from a variety of different perspectives:

- By selecting “*Visualize*” from the “Risk Assessment” main page the Security Professional can see the status of the CII’s asset inventory (depicted in asset graph structure cf. section 4.2.1.3) after the risk assessment performance. Asset nodes are different colored depending on the identified Risk Level (a grey asset node indicates that no risk is found on an asset/a yellow asset node indicates that asset’s Risk Level is “Low”/ an orange asset node indicates that asset’s Risk Level is “Medium”/a red asset node indicates that asset’s Risk Level is “High”/a black asset node indicates that asset’s Risk Level is “Very High” (Figure 48).

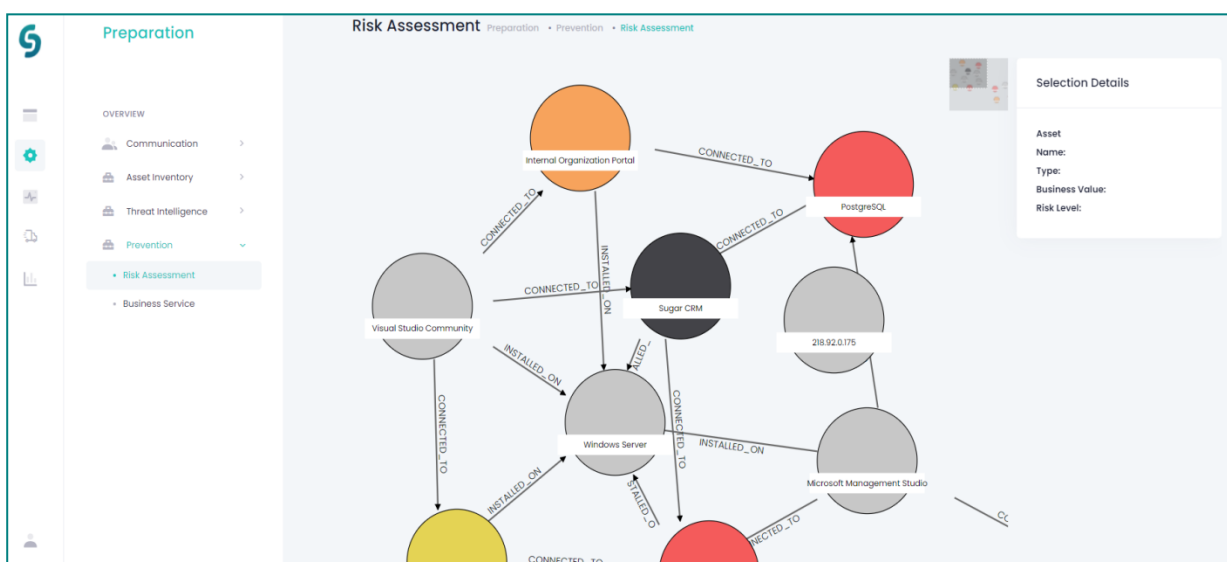


Figure 48: The “Visualize” option depicts the organisation’s assets graph, where asset nodes are coloured by assets risk levels.

## D9.2 – Training Materials and Report on Training Processes

By clicking on a specific asset node, the asset's "Footprint" option appears (cf. 4.2.1.3). The asset "Footprint" option (Figure 49) presents information about the real status of the asset. Herein, it illustrates the probability of all identified threats and the impact of all identified vulnerabilities on a specific asset **after the risk assessment performance**. By hitting the asset's "Footprint" option this information is displayed on a heatmap (Figure 50). In addition, the Security Professional can explore further options, such as print and saving from the "Chart context menu" by tapping on the three dashes icon (Figure 50).

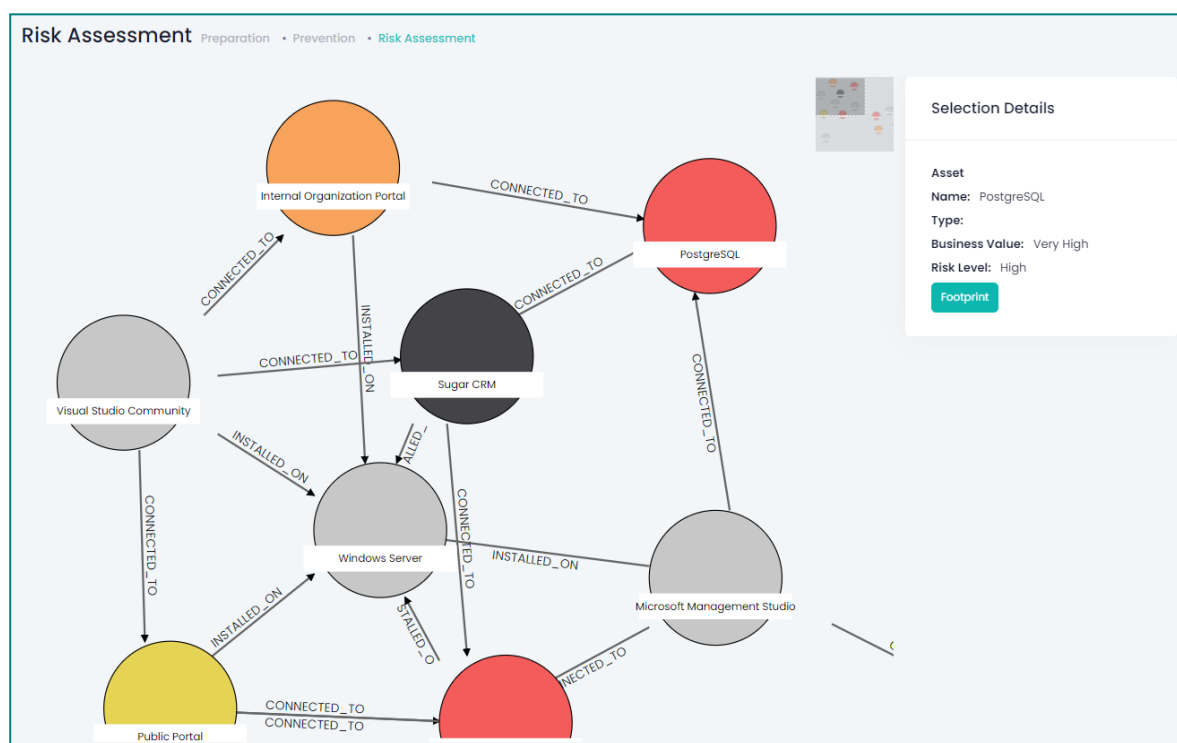


Figure 49: "PostgreSQL" asset Footprint options are activated.

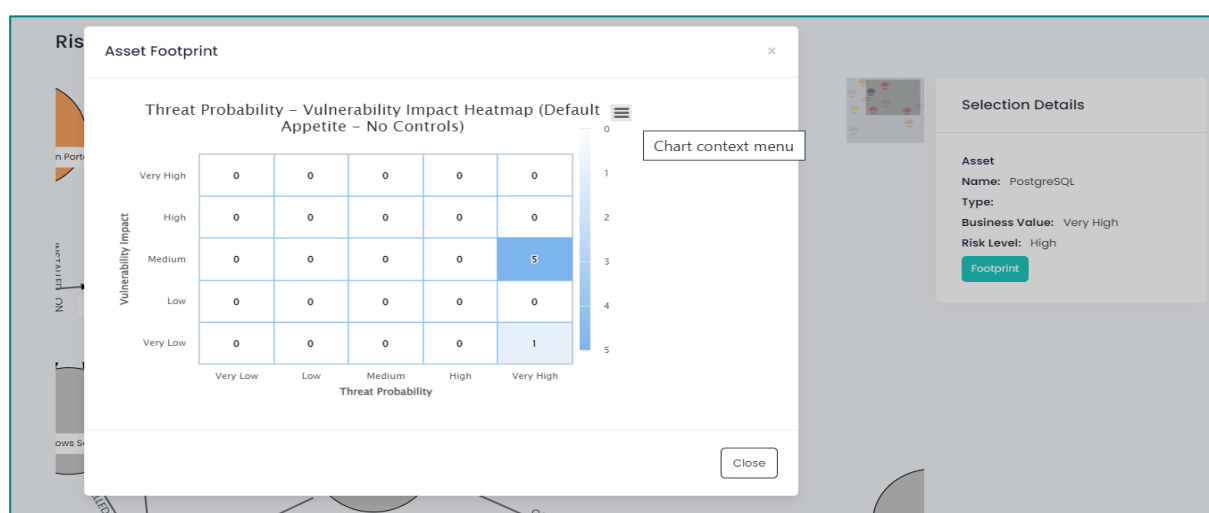


Figure 50: The Asset Footprint depicts the real status of the asset "PostgreSQL" (after risk assessment) in a "Threat Probability-Vulnerability Impact" Heatmap. Additional options can be explored from the "Chart context" menu.

## D9.2 – Training Materials and Report on Training Processes

Upon selecting a specific value in a cell of the matrix, information of the specific threat identified on the asset along with its probability and information of the specific vulnerability with its impact can be explored.

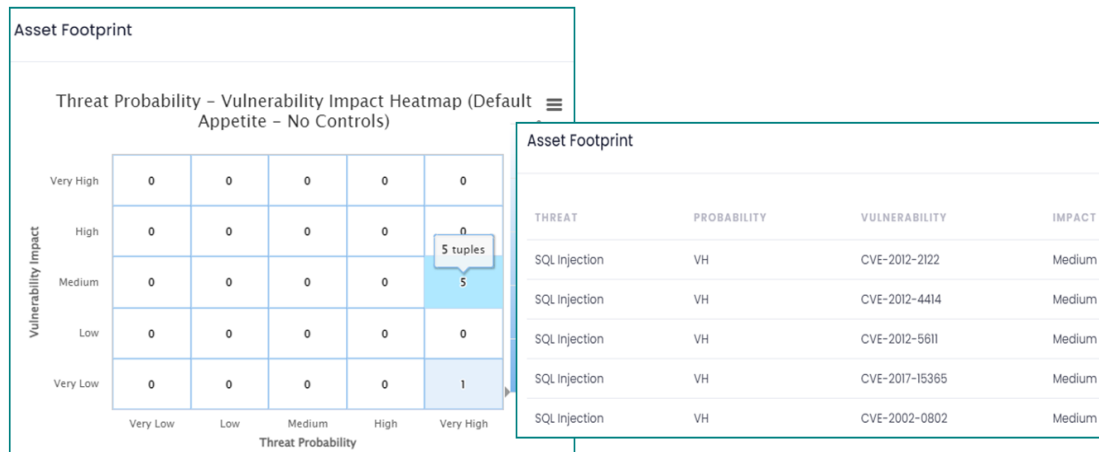


Figure 51: Threat and Vulnerabilities information can be viewed by clicking on a specific value of the “Threat Probability-Vulnerability Impact” Heatmap.

- By selecting “Executive Summary” from the “Risk Assessment” main page, the Security Professional can explore the risk assessment results in different chart types: the Assets Individual Risk Level in pies and radar (spider web) charts (Figure 52), clustered column charts providing the occurrence weighted threats that result in “Very High” upper Individual Risk Level and information on the “critical” assets (Figure 53), a “Threats Probability – Vulnerability Impact” heatmap (Figure 53).

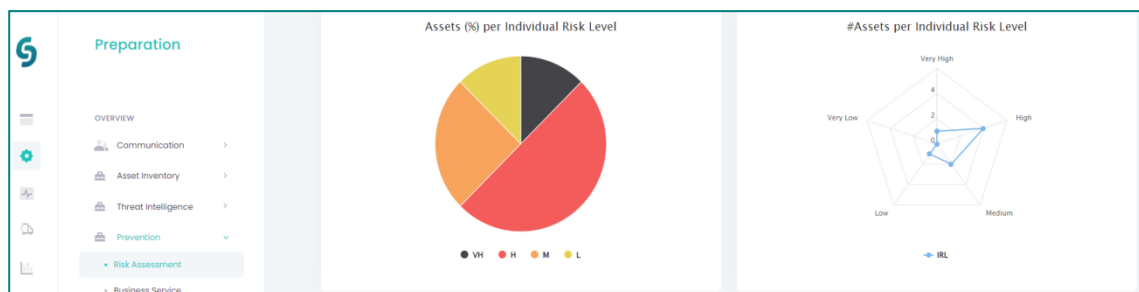


Figure 52: Different charts representing the Individual Risk Level on assets of a specific Business Service.

## D9.2 – Training Materials and Report on Training Processes



Figure 53: Different charts representing the Individual Risk Level on critical assets of a specific Business Service.

- By selecting “*Risk Analysis*” from the “Risk Assessment” main page, the risk assessment results can be viewed per asset and per risk level (Figure 54)

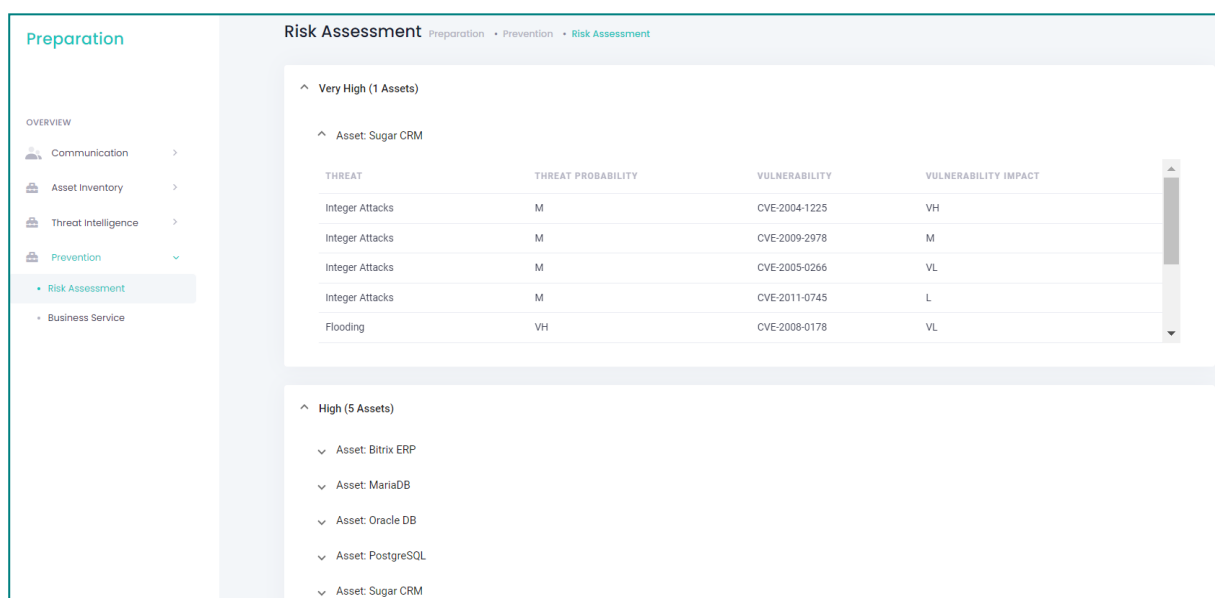


Figure 54: Risk assessment report in table format per asset and per risk level.

- By selecting “*Assets Risk Level*” from the “Risk Assessment” main page, a report in table format appears showing the risk assessment results for each asset per threat, indicating the Dominant Individual Risk Level as well (Figure 55)
- By selecting “*Assets*” from the “Risk Assessment” main page, an asset list appears of all assets that are involved in the risk assessment of the given Business Service (Figure 56). Upon clicking the three dots button (Figure 56) information on detected threats and vulnerabilities (attack scenarios) appears (Figure 57)

## D9.2 – Training Materials and Report on Training Processes

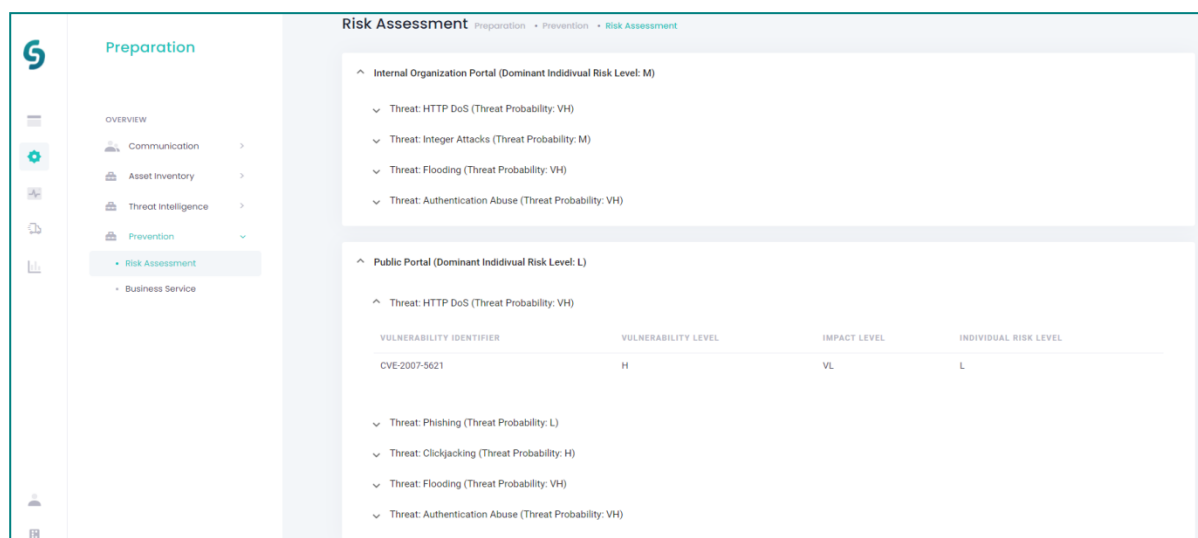


Figure 55: Risk Assessment report showing the Dominant Individual Risk Level per asset and the identified threats with corresponding vulnerabilities.

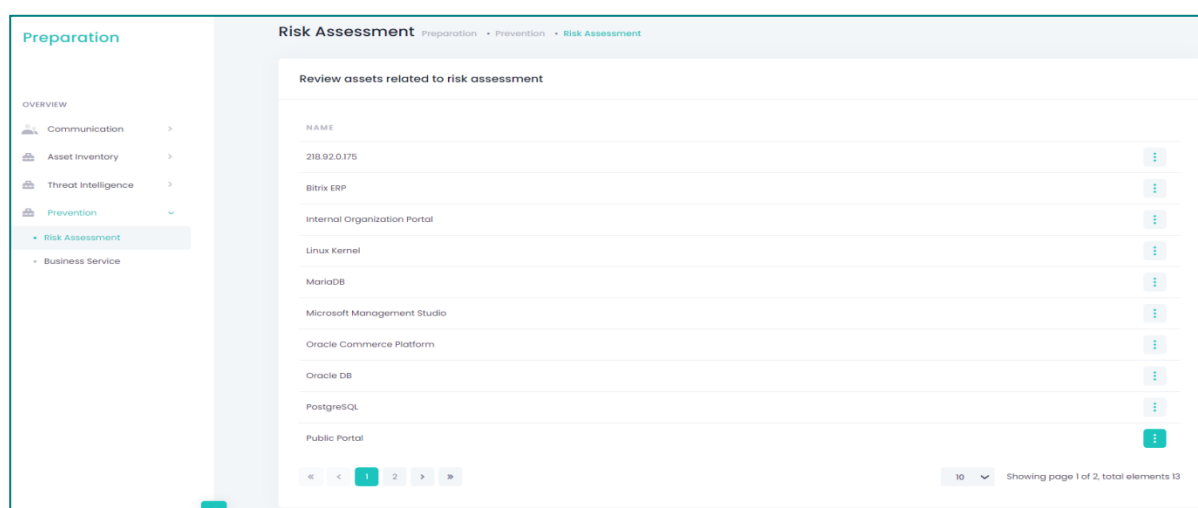


Figure 56: Asset list report related to risk assessment of a given Business Service.

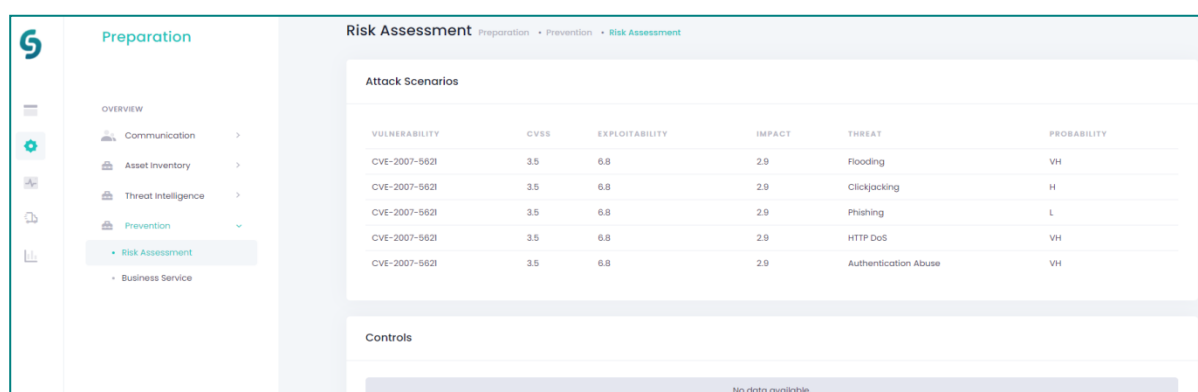


Figure 57 - Attack scenarios information depicted per asset related to the risk assessment.



### 4.4.2 Business Service

The Business Service functionality in CyberSANE refers to an organisation's process which contains all the assets that operate during its execution (assets are retrieved from the Asset Inventory). Risk Assessment in CyberSANE can be performed upon a selected Business Service. Business Services can be either managed or created from the "Business Service" functionality of the "Preparation" phase (Figure 58).

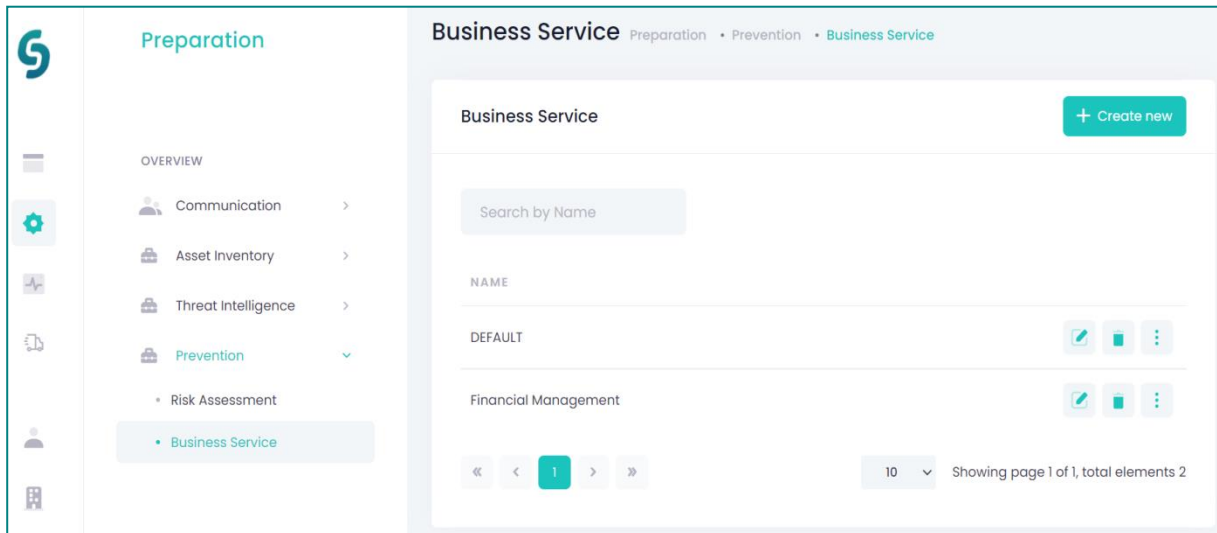


Figure 58: The Business Service functionality in CyberSANE.

#### 4.4.2.1 Business Service Management

Preparation -> Prevention -> Business Service

Declared Business Services can be viewed by selecting from the "Preparation" phase of the dashboard menu the "Prevention" and "Business Service" options subsequently. The declared Business Services can be either searched by name or renamed upon clicking on the pen icon or deleted through hitting the bin icon (Figure 59). Assets included in a Business Service can be either viewed, or managed by clicking on the three dots icon (Figure 59). Afterwards, a list of assets declared to the specific Business Service appears (Figure 60). The declared assets can be deleted by clicking on the bin icon. New assets can be added on the Business Service by selecting the desired asset(s) and tapping on the "Add Asset(-s)" button.

## D9.2 – Training Materials and Report on Training Processes

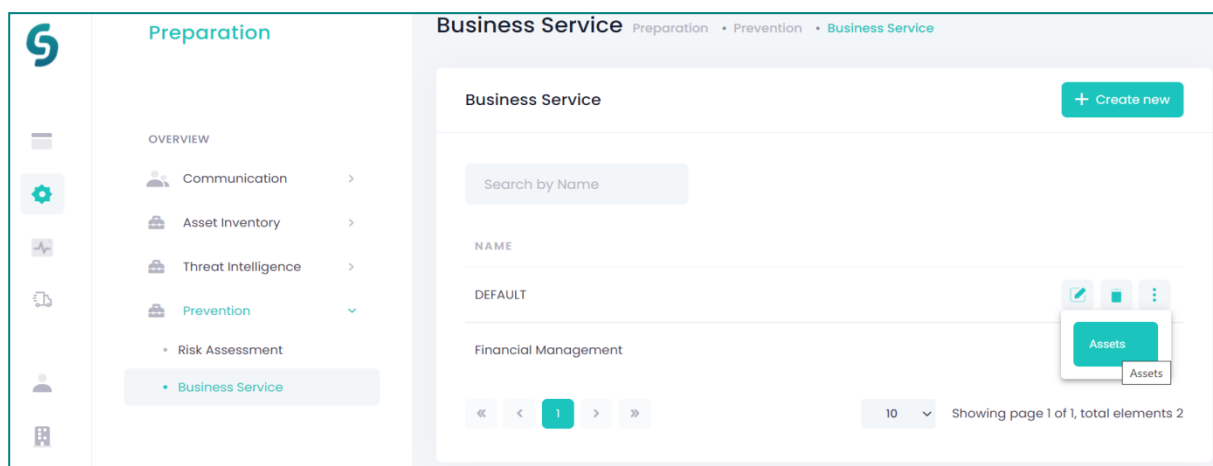


Figure 59: Business Service options.

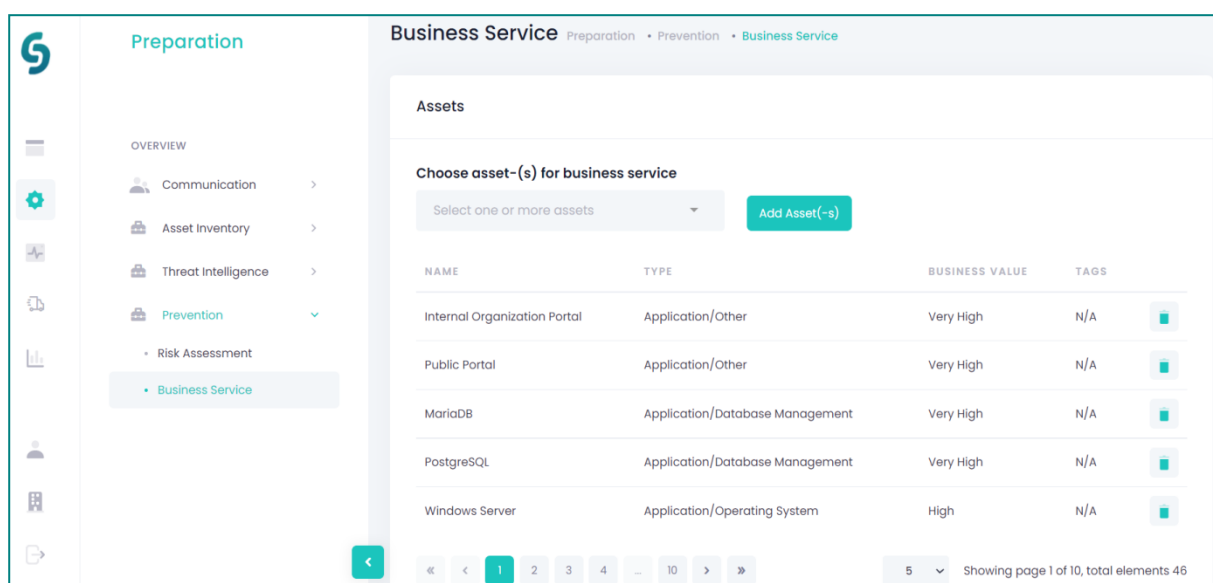


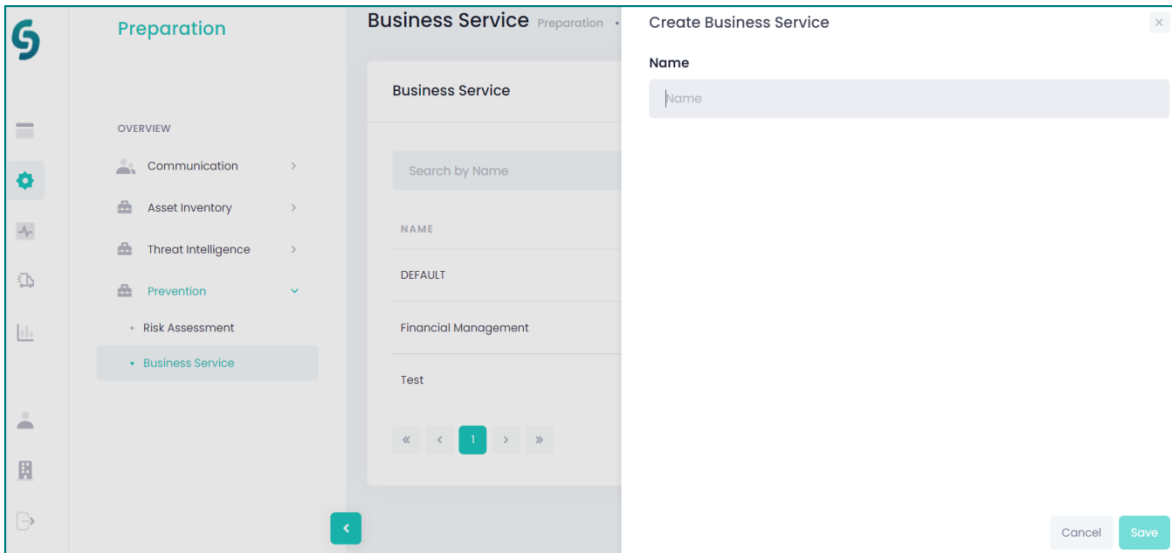
Figure 60: A list of declared assets on a specific Business Service can be viewed or managed from the “Business Service” functionality.

### 4.4.2.2 Create a Business Service

Preparation -> Prevention -> Business Service

To create a new Business Service, The Security Professional shall select “Prevention” from the “Preparation” phase of the dashboard menu and then go to the “Business Service” functionality (Figure 58) and press “Create new”. Then, the “Create Business Service” tab appears and the Security Professional shall enter a descriptive name of the Business Service and press the “Save” button (Figure 61). To add assets on the Business Service, the Security Professional must follow the process of adding assets described in Section 4.4.2.1.

## D9.2 – Training Materials and Report on Training Processes



The screenshot shows the 'Create Business Service' dialog box. The background interface includes a sidebar with a 'Preparation' section containing 'Communication', 'Asset Inventory', 'Threat Intelligence', 'Prevention' (with a dropdown arrow), 'Risk Assessment', and 'Business Service' (highlighted). The main content area is titled 'Business Service' and includes a 'Search by Name' input field, a 'NAME' field, a 'DEFAULT' field, a 'Financial Management' field, and a 'Test' field. At the bottom of the main content area are navigation buttons: '<<', '<', a highlighted '1', '>', and '>>'. The dialog box itself has a title bar 'Create Business Service' with a close button 'x'. It contains a 'Name' label and a text input field with the placeholder 'Name'. At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

Figure 61: Create a Business Service.

## 5. Detection and Analysis Phase

Within the Detection and Analysis Phase, the Security Professional can view and investigate the evidence gathered from the CII. The Detection and Analysis Phase functionalities can be accessed by the dashboard menu by clicking on the “Detection and Analysis” icon (Figure 62).

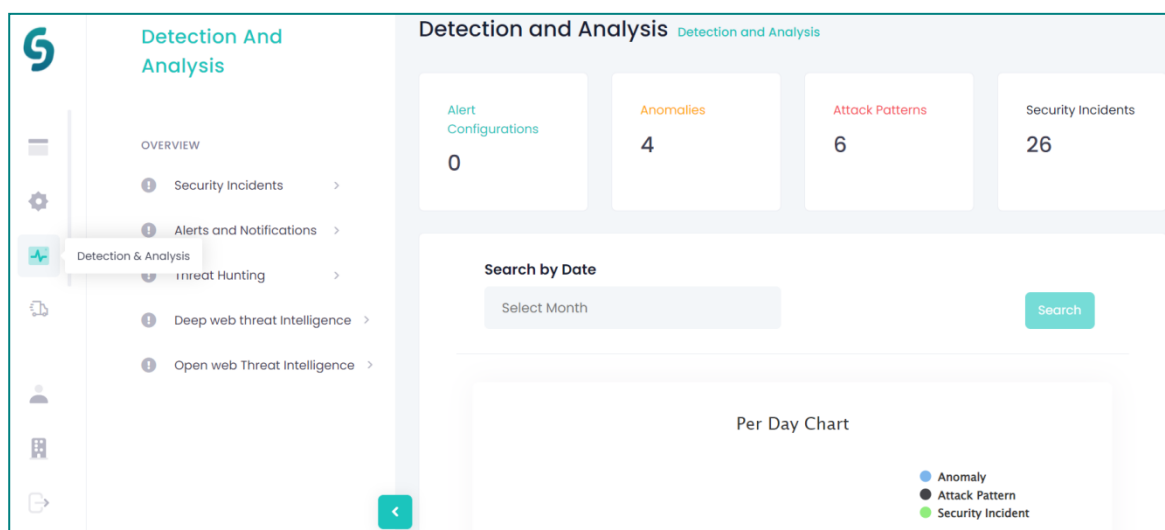


Figure 62: CyberSANE Detection and Analysis phase functionalities.

The Detection and Analysis phase in CyberSANE supports the following functionalities:

- Security Incidents
- Alerts and Notifications
- Threat Hunting
- Deep Web Threat Intelligence
- Open Web Threat Intelligence

### 5.1 Security Incidents

The “Security Incidents” functionality of CyberSANE allows the Security Professional to review in real-time the number of anomalies, attack patterns and incidents detected upon the organisation’s declared assets.

The “Security Incident” functionality can be reached from the “Detection and Analysis” phase icon which is shown from the dashboard menu. The Security Professional by selecting a specific period from the calendar icon and pressing the “Search” button (Figure 63), he/she can explore information on anomalies, attack patterns and incidents

## D9.2 – Training Materials and Report on Training Processes

detected within the organisation through the visualization of daily and overall charts (Figure 64).

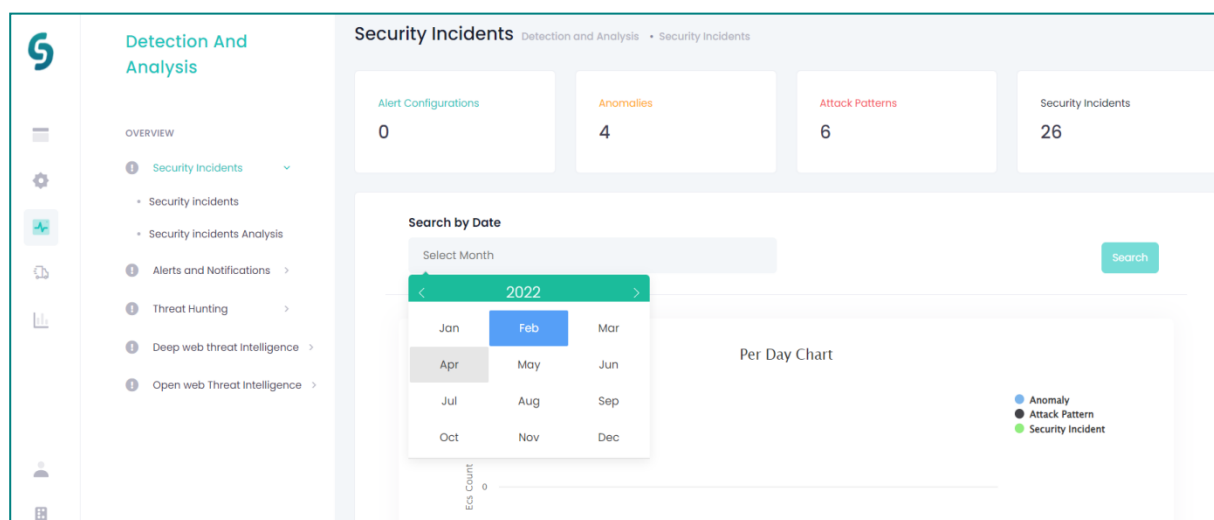


Figure 63: The Security Professional can search for anomalies, attack patterns and security incidents identified within the organisation for a selected period.

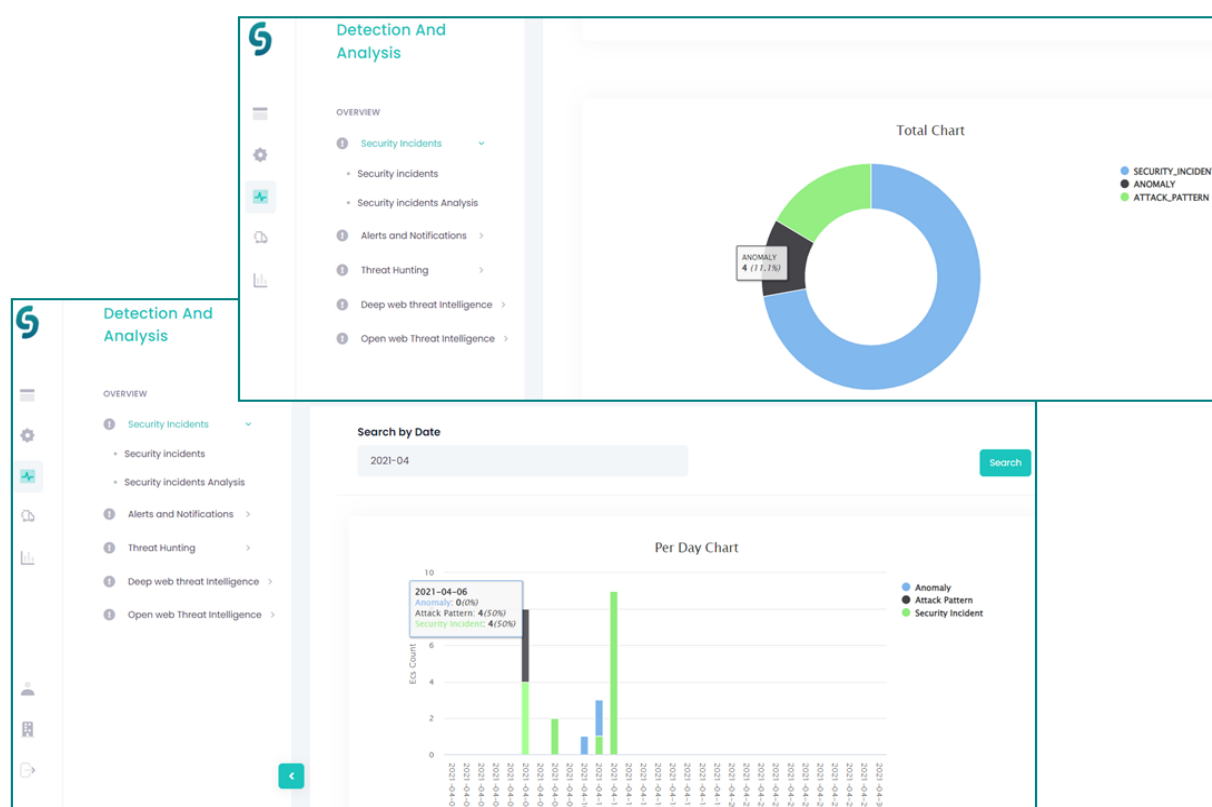
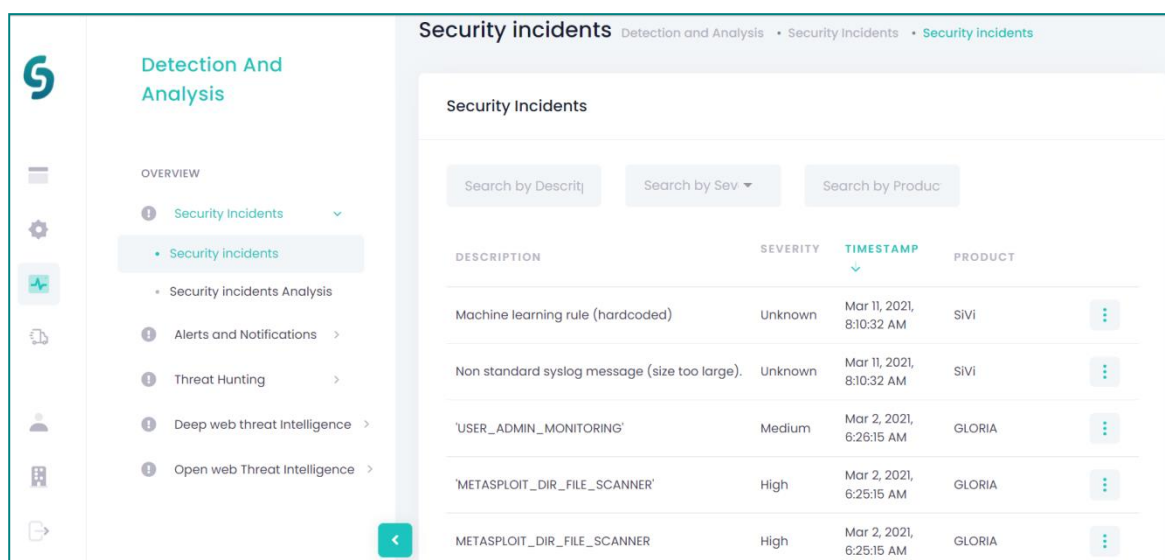


Figure 64: The Security Professional can review analytics on identified anomalies, attack patterns and security incidents within the organisation upon a selected period.

### 5.1.1 Review Security Incidents information

Detection and Analysis -> Security Incidents -> Security Incidents

By clicking on the “Security Incident” options in the “Detection and Analysis” phase which can be reached from the dashboard menu, the Security Professional can explore further information on the identified incidents (Description/Severity/Timestamp/Product that generated the detected item) (Figure 65). They can be searched either by each description or severity or product. Information about the “Product” that produced the detection of these items is provided in case the Security Professional wishes to track more information by visiting the dashboard menu of the specific product.



DESCRIPTION	SEVERITY	TIMESTAMP	PRODUCT
Machine learning rule (hardcoded)	Unknown	Mar 11, 2021, 8:10:32 AM	SIVI
Non standard syslog message (size too large).	Unknown	Mar 11, 2021, 8:10:32 AM	SIVI
'USER_ADMIN_MONITORING'	Medium	Mar 2, 2021, 6:26:15 AM	GLORIA
'METASPLOIT_DIR_FILE_SCANNER'	High	Mar 2, 2021, 6:25:15 AM	GLORIA
METASPLOIT_DIR_FILE_SCANNER	High	Mar 2, 2021, 6:25:15 AM	GLORIA

Figure 65: Security Incidents functionality offers a detailed list of security incidents, attack patterns and anomalies detected within the organisation.

Nevertheless, by clicking on the three dots icon and pressing the “View Info” option (Figure 66), the Security Professional can review a concrete analysis of the security incident identified on a specific asset of the organisation through a large-scale list of attributes, (an excerpt of it is depicted in Figure 67).

## D9.2 – Training Materials and Report on Training Processes

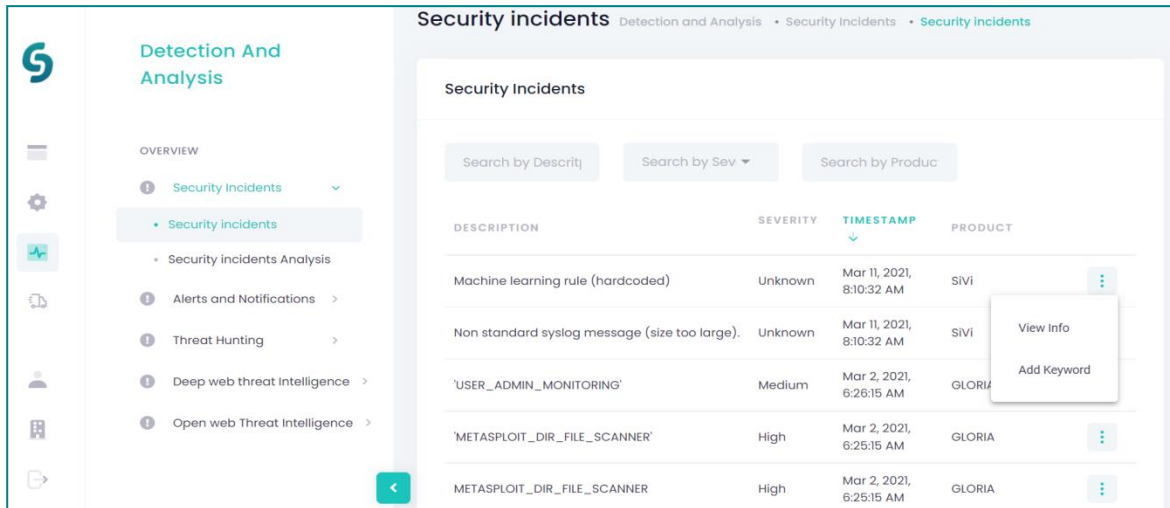


Figure 66: Security Incident page of the Detection and Analysis phase.

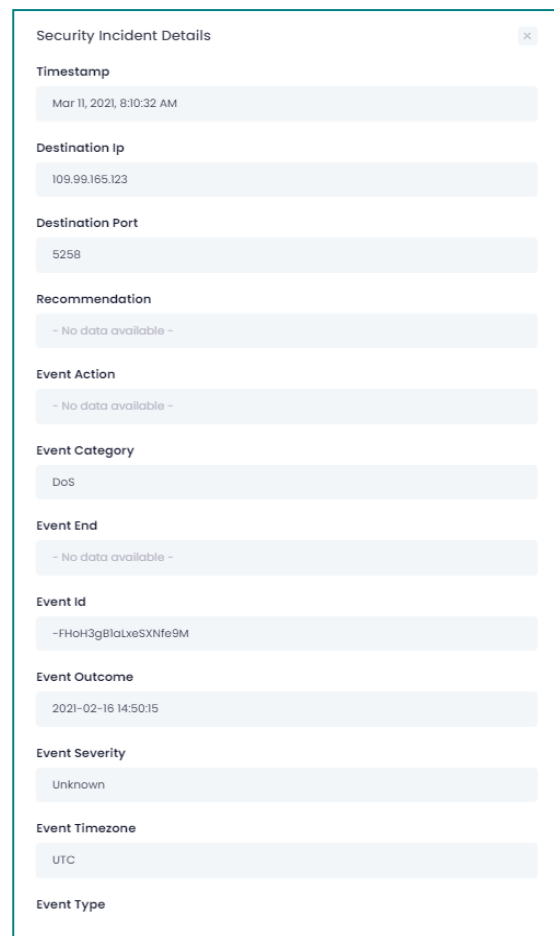


Figure 67: CyberSANE system provides a large-scale of attributes of a security incident identified on a specific asset.

The “Security Incident” list is derived from the CyberSANE “LiveNet” component.

### 5.1.2 Security Incidents Analysis

Detection and Analysis -> Security Incidents -> Security Incidents Analysis

The “Security Incident Analysis” option can be reached from the “Security Incidents” functionality of the “Detection and Analysis” phase, which is shown from the dashboard menu. The Security Professional by selecting a specific period from the calendar icon and pressing the “Search” button (Figure 68), he/she can explore analytics on the security incidents and their criticality through visualizations of daily and overall charts (Figure 69).

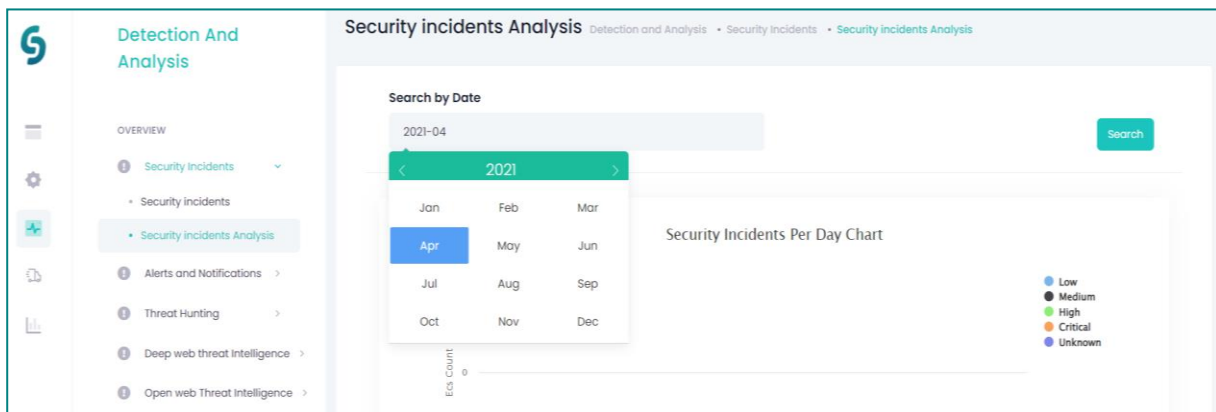


Figure 68: The Security Professional can search for anomalies, attack patterns and security incidents identified within the organisation for a selected period.

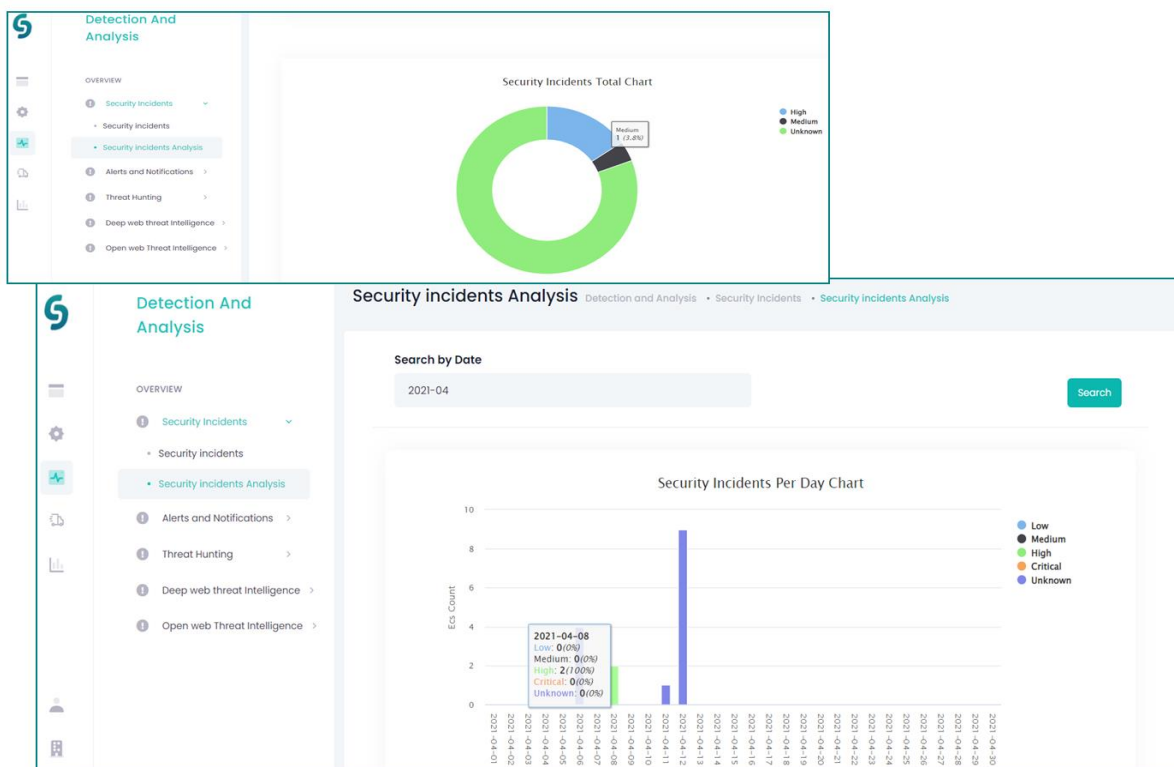


Figure 69: The Security Professional can review analytics on the security incidents and their criticality identified on the declared assets of the organisation upon a selected period.



## 5.2 Alerts and Notifications

The “Alerts and Notifications” functionality of CyberSANE allows the Security Professional to review in real-time security alerts that have been raised and corresponding notifications generated because of the security incident or anomaly detection and attack patterns identification (cf. section 5.1).

“Alerts and Notifications” can be created or managed from the “Alerts” option further described in the next sections.

### 5.2.1 View and Manage Alerts

Detection and Analysis -> Alerts and Notifications -> Alerts

Alerts can be viewed and managed by the “Alerts” option from the “Alerts and Notifications” functionality of the “Detection and Analysis” phase of the dashboard menu (Figure 70). The Security Professional can view and edit information on security alerts or delete security alerts by selecting the pen icon or bin icon accordingly.

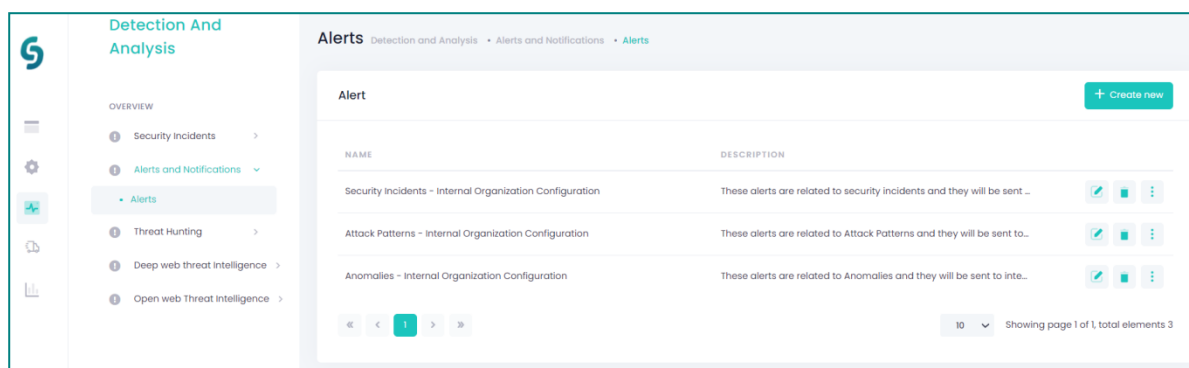


Figure 70: Raised alerts can be viewed and managed from the “Alerts and Notifications” functionality.

From the “Edit Alert” editor reached by the pen icon, the Security Professional can review and edit the alert’s information (Figure 71).

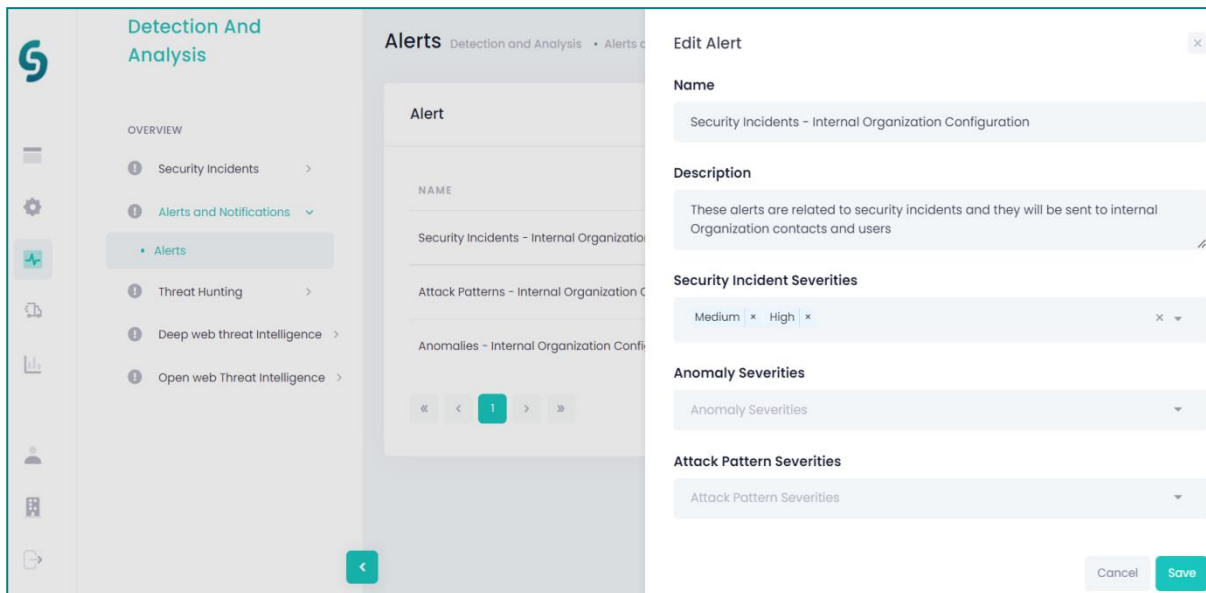


Figure 71: The “Edit Alert” tab from the “Alerts and Notifications” functionality.

Once the three dots button is clicked from the “Alerts” page (Figure 70), the Security Professional can explore information about alert loggers (Figure 72).

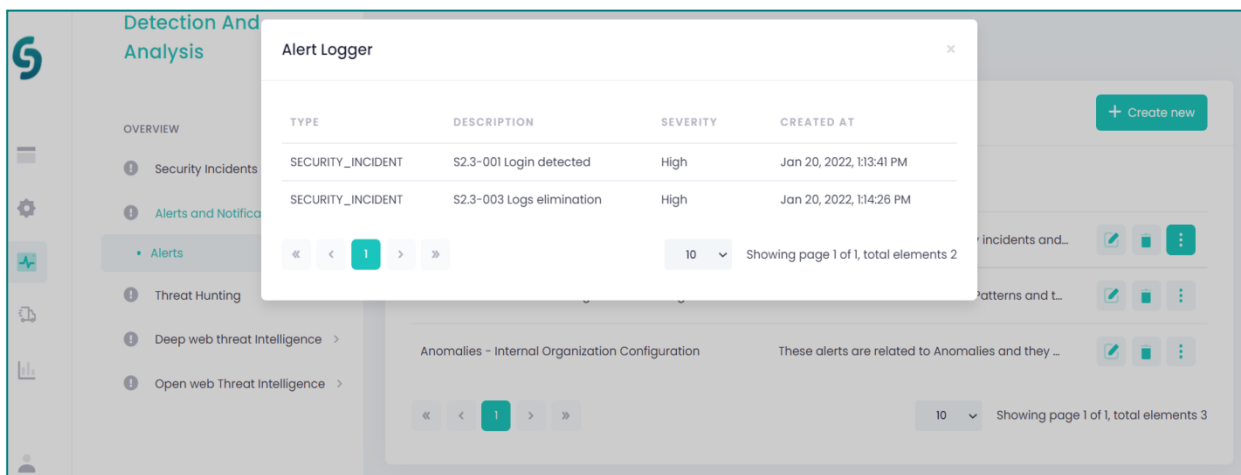


Figure 72: Information on Loggers can be viewed for each alert from the “Alerts and Notifications” functionality.

### 5.2.2 Create an alert

Detection and Analysis -> Alerts and Notifications -> Alerts

To create an alert, the Security Professional shall go to the “Alerts” option from the “Alerts and Notifications” functionality of the “Detection and Analysis” phase which can be reached from the dashboard menu and press the “Create new” button (Figure 70). Then, the “Create Alert” tab appears and the Security Professional shall fill the requested fields (Figure 73):

- Alert name: provide a name related to the alert raised
- Alert Description: provide a descriptive text of the generated alert

- Security Incident Severities: assess the severity of the detected security incident from a dropdown nominal scale list
- Anomaly Severities: assess the severity of the detected anomaly from a dropdown nominal scale list
- Attack Pattern Severities: assess the severity of recognized attack patterns from a dropdown nominal scale list)
- Organisation users: select organisation users to get notified for the alert
- Internal contacts: select internal contacts (see “Communication” section; cf. section 4.1 of the “Preparation” phase) to get notified for the alert
- External contacts: select external contacts (see “Communication” section; cf. section 4.1 of the “Preparation” phase) to get notified for the alert

After providing the proper information, the Security Professional shall press the “Save” button. The security alert has been created.

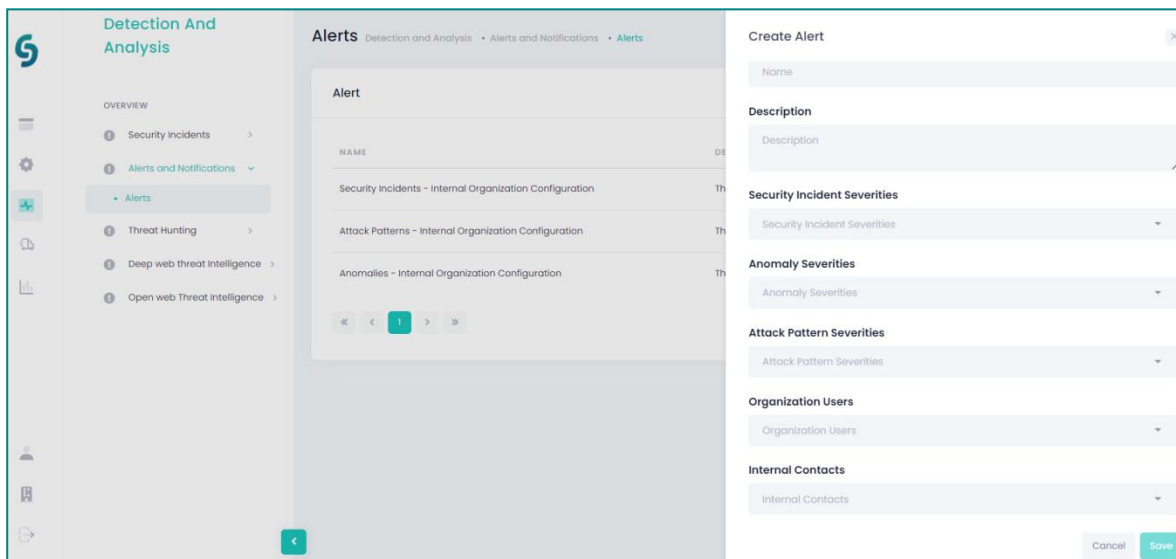


Figure 73: The “Create alert” tab from the “Alerts and Notifications” functionality.

## 5.3 Threat Hunting

The “Threat Hunting” functionality of the CyberSANE system allows the Security Professional to review in real-time the number of anomalies detected upon the organisation’s declared assets and the corresponding attack patterns. “Threat Hunting” supports the following options described in the following sections:

- Attack Patterns
- Attack Patterns Analysis
- Anomaly Detection
- Anomaly Detection Analysis

### 5.3.1 Attack Patterns

## D9.2 – Training Materials and Report on Training Processes

### Detection and Analysis -> Threat Hunting -> Attack Patterns

“Attack Patterns” can be reached from the “Threat Hunting” functionality of the “Detection and Analysis” phase of the dashboard menu. Within this option, the Security Professional can review a list of attack patterns along with detailed information for each attack pattern (Description/Severity/Timestamp/Product that generated the detected item) (Figure 74). “Attack Patterns” can be searched either by their description or severity or product (cf. section 5.1.1). By pressing the three dots icon, the Security Professional can delve into further detail for each attack pattern. An excerpt of an Attack Pattern’s attributes is shown in Figure 75.

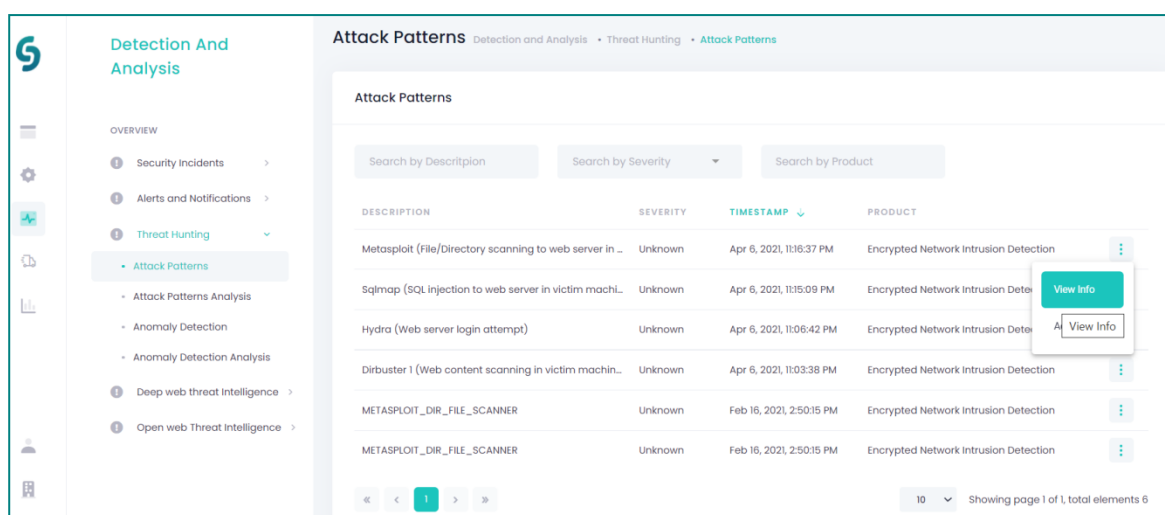


Figure 74: Attack Patterns page of the Detection and Analysis phase.

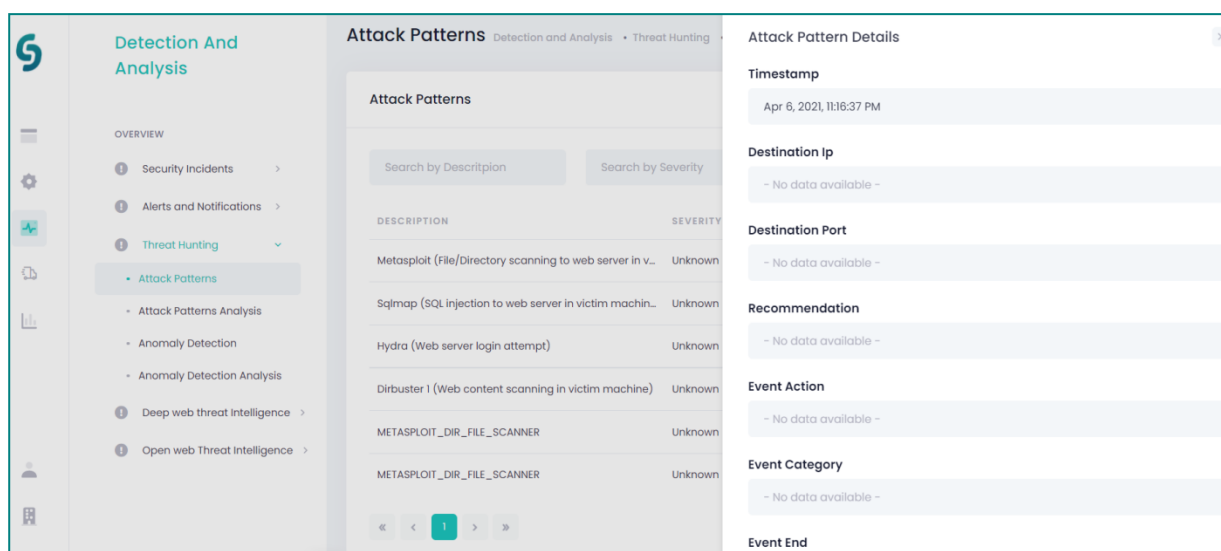


Figure 75: An excerpt of the provided attributes of an Attack Pattern.

The Attack Patterns list is derived from the CyberSANE “LiveNet” component.

### 5.3.2 Attack Patterns Analysis

## D9.2 – Training Materials and Report on Training Processes

### Detection and Analysis -> Threat Hunting -> Attack Patterns Analysis

The “Attack Patterns Analysis” option can be reached from the “Threat Hunting” functionality of the “Detection and Analysis” phase, which is displayed from the dashboard menu. Similarly, with the “Security Incident Analysis” (cf. section 5.1.2), the Security Professional can explore detailed information about the attack patterns and their criticality through visualizations of daily and overall charts upon selecting a specific period (Figure 76).

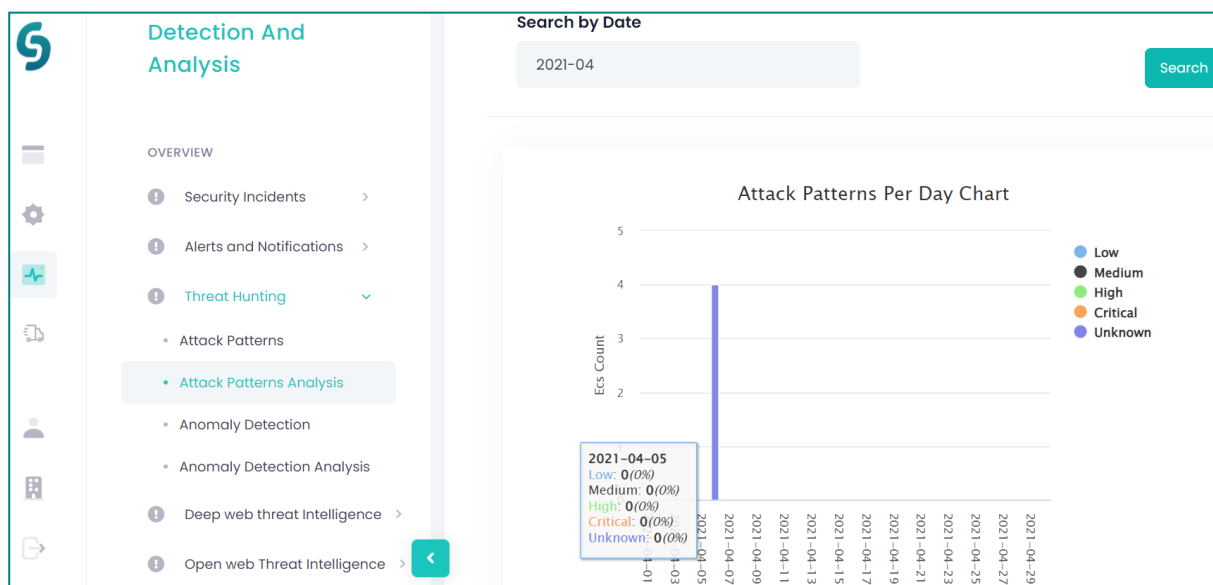
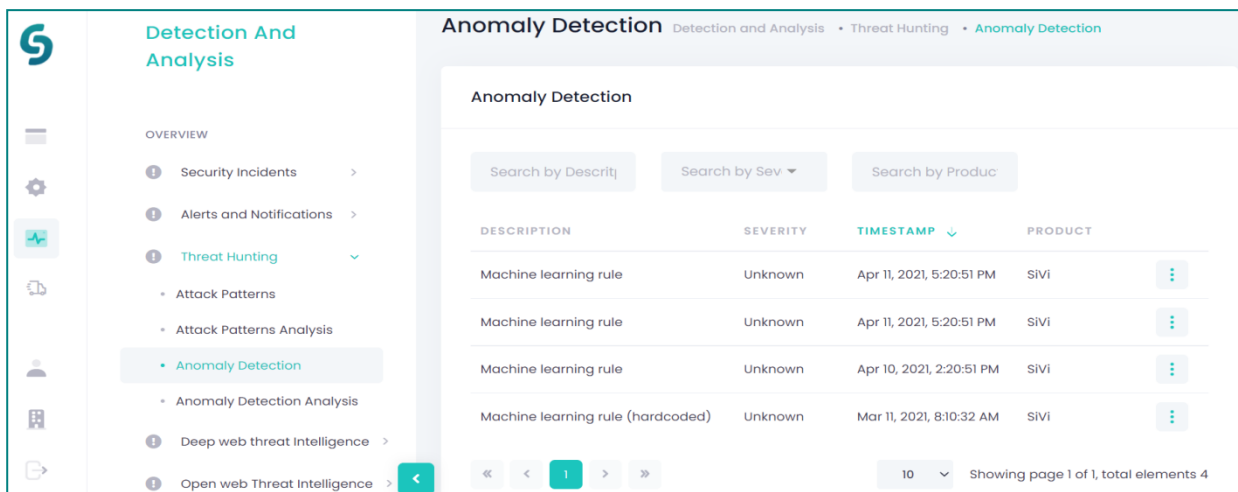


Figure 76: Attack Patterns Analysis page of the Detection and Analysis phase.

### 5.3.3 Anomaly Detection

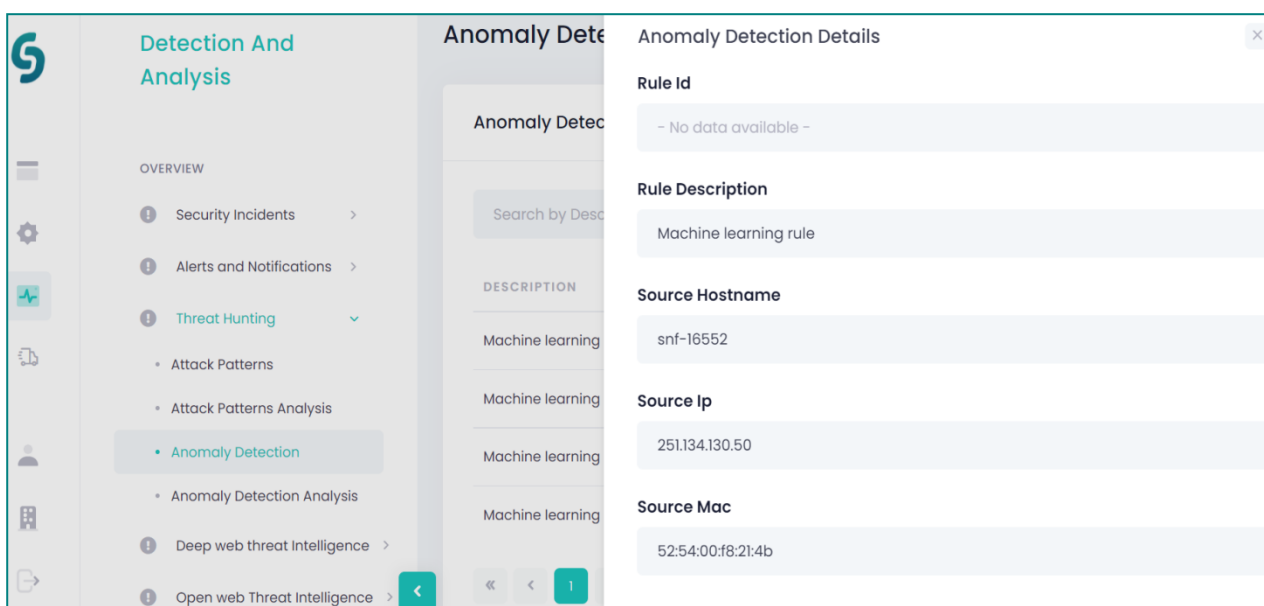
#### Detection and Analysis -> Threat Hunting -> Anomaly Detection

“Anomaly Detection” can be approached by the “Threat Hunting” functionality from the “Detection and Analysis” phase of the dashboard menu. Within this option, the Security Professional can review a list of anomalies together with detailed information for each detected anomaly (Description/Severity/Timestamp/Product that generated the detected item) (Figure 77). Anomalies can be searched either by their description or severity or product (cf. section 5.1.1). By pressing the three dots icon, the Security Professional can browse further details for each detected anomaly. An excerpt of the provided attributes for a detected anomaly is shown in Figure 78.



DESCRIPTION	SEVERITY	TIMESTAMP	PRODUCT
Machine learning rule	Unknown	Apr 11, 2021, 5:20:51 PM	SIVI
Machine learning rule	Unknown	Apr 11, 2021, 5:20:51 PM	SIVI
Machine learning rule	Unknown	Apr 10, 2021, 2:20:51 PM	SIVI
Machine learning rule (hardcoded)	Unknown	Mar 11, 2021, 8:10:32 AM	SIVI

Figure 77: Anomaly Detection list of the Detection and Analysis phase.



DESCRIPTION	SEVERITY	TIMESTAMP	PRODUCT
Machine learning	Unknown	Apr 11, 2021, 5:20:51 PM	SIVI
Machine learning	Unknown	Apr 11, 2021, 5:20:51 PM	SIVI
Machine learning	Unknown	Apr 10, 2021, 2:20:51 PM	SIVI
Machine learning	Unknown	Mar 11, 2021, 8:10:32 AM	SIVI

Figure 78: An excerpt of the provided attributes for a detected anomaly.

The Anomaly Detection list is derived from the CyberSANE “HybridNet” component.

### 5.3.4 Anomaly Detection Analysis

Detection and Analysis -> Threat Hunting -> Anomaly Detection Analysis

The “Anomaly Detection Analysis” option can be approached by the “Threat Hunting” functionality of the “Detection and Analysis” phase, which is reached from the dashboard menu. Similarly with the “Security Incident Analysis” and “Attack Patterns Analysis” functionalities (cf. sections 5.1.2, 5.3.2), the Security Professional can review detailed information about the anomalies detected on organisation’s assets and their criticality through visualizations of daily and overall charts upon selecting a specific period (Figure 79).

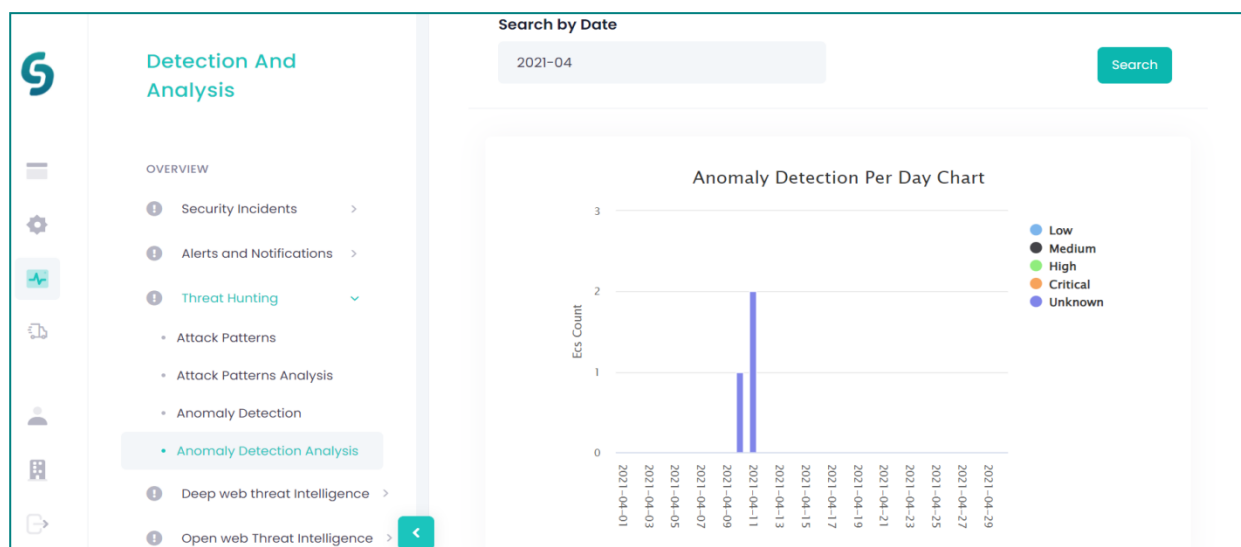


Figure 79: Anomaly Detection Analysis page of the Detection and Analysis phase.

## 5.4 Deep Web Threat Intelligence

The “Deep Web Threat Intelligence” functionality of the CyberSANE system allows the Security Professional to further investigate the real evidence gathered from the CII and get better prepared and make proper decisions at a later stage of the incident handling process for eradication and recovery actions towards the detected evidence. In particular, the current functionality produces a variety of web articles that CyberSANE crawled and retrieved from the Deep and Dark Web upon specific search set by the Security Professional. Thereby, the Security Professional can search for further information about the identified evidence on the organisations’ CII. Moreover, the CyberSANE system produces a variety of graphs relying on different perspectives to give to the Security Professional a more concrete view of the results. “Deep Web Threat Intelligence” delivers the following options, which are described in the next sections (Figure 80):

- Deep Web Articles
- Categories and Concepts
- Tag Cloud and Concept Graphs
- Graph Analytics
- Graph Significant

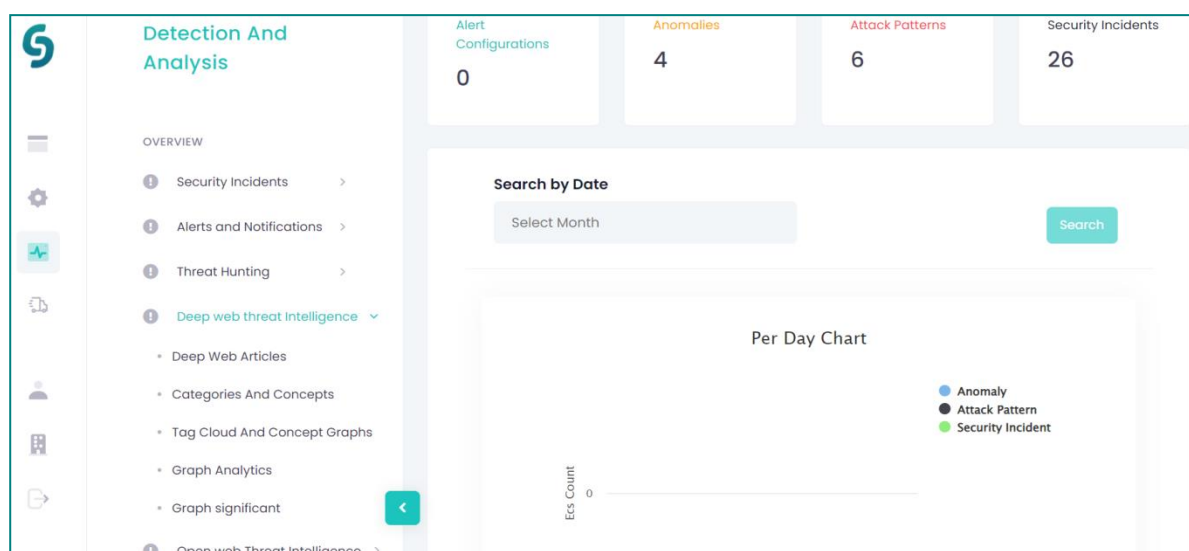


Figure 80: The Deep Web Threat Intelligence functionality of the Detection and Analysis phase.

### 5.4.1 Deep Web Articles

Detection and Analysis -> Deep Web Threat Intelligence -> Deep Web Articles

The “Deep Web Articles” option can be viewed from the “Deep Web Threat Intelligence” functionality of the “Detection and Analysis” phase of the dashboard menu (Figure 81). Here, the Security Professional can see the reputation of his/her organisation in the Deep and Dark Web. In addition, the crawling mechanism has searched for number of articles related to the provided evidence (Total Documents).

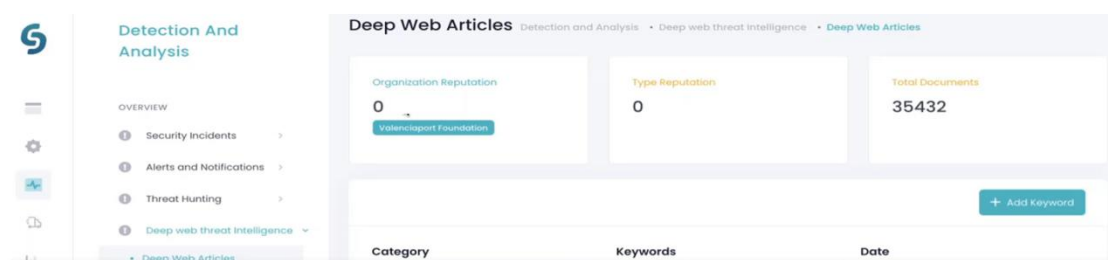


Figure 81: Deep Web Articles illustrate whether there is a reputation for the organisation in the Deep and Dark Web and crawls for documents related to the detected evidence.

The Security Professional can search among these articles to elicit specific security information by defining the desired category, related keywords, selecting a specific time and pressing the “Save” button (Figure 82). In this manner the Security Professional can review what have been discussed in relation to these keywords in the Deep and Dark Web.



## D9.2 – Training Materials and Report on Training Processes

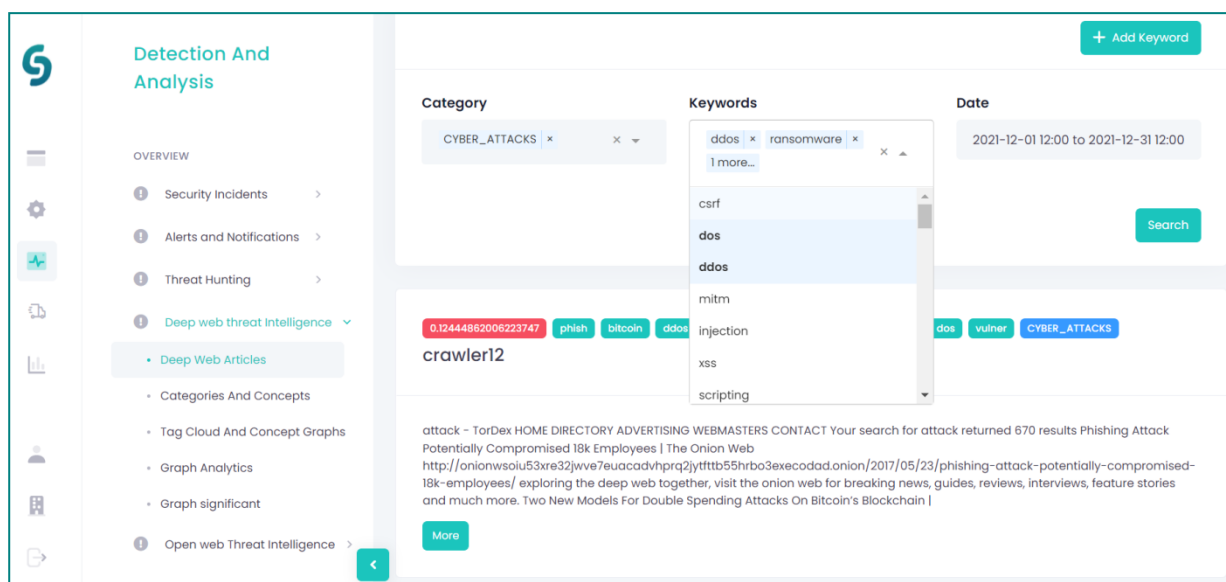


Figure 82: Documents retrieved from the Deep and Dark Web can be searched to gather specific information.

The following figures show the variety of findings related to the previous search. By selecting the “More” button under an article (Figure 83), the Security Professional can view the entire information of a Deep Web Article (Figure 84).

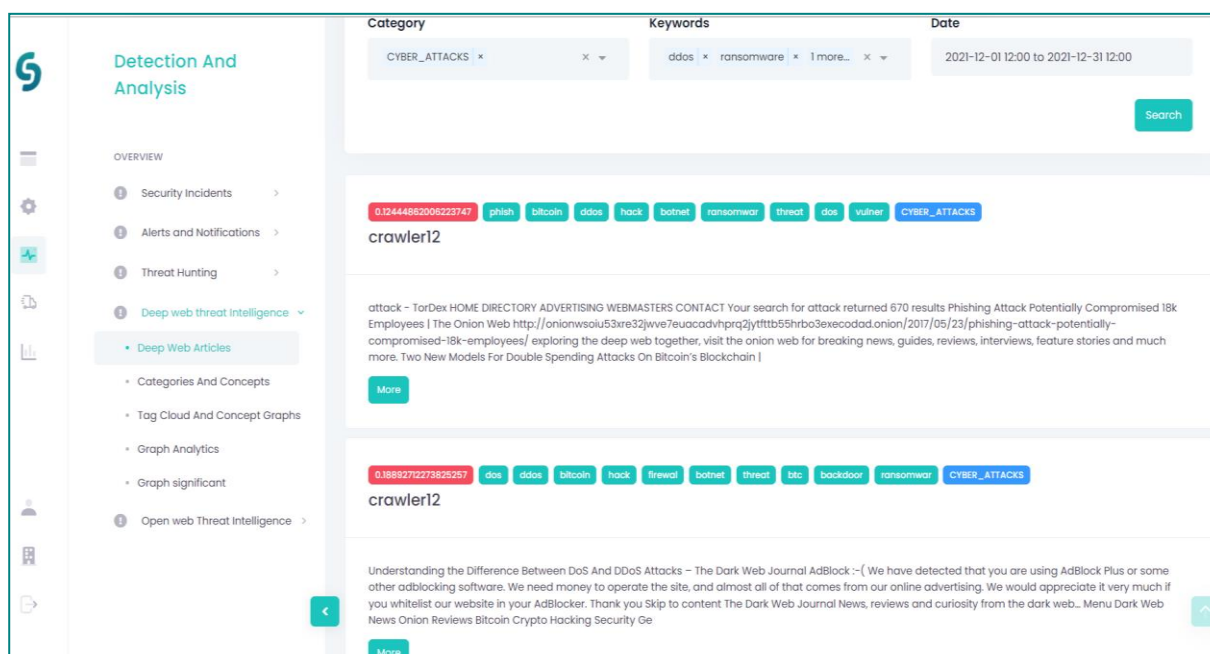


Figure 83: A list of documents can be viewed upon search.

## D9.2 – Training Materials and Report on Training Processes

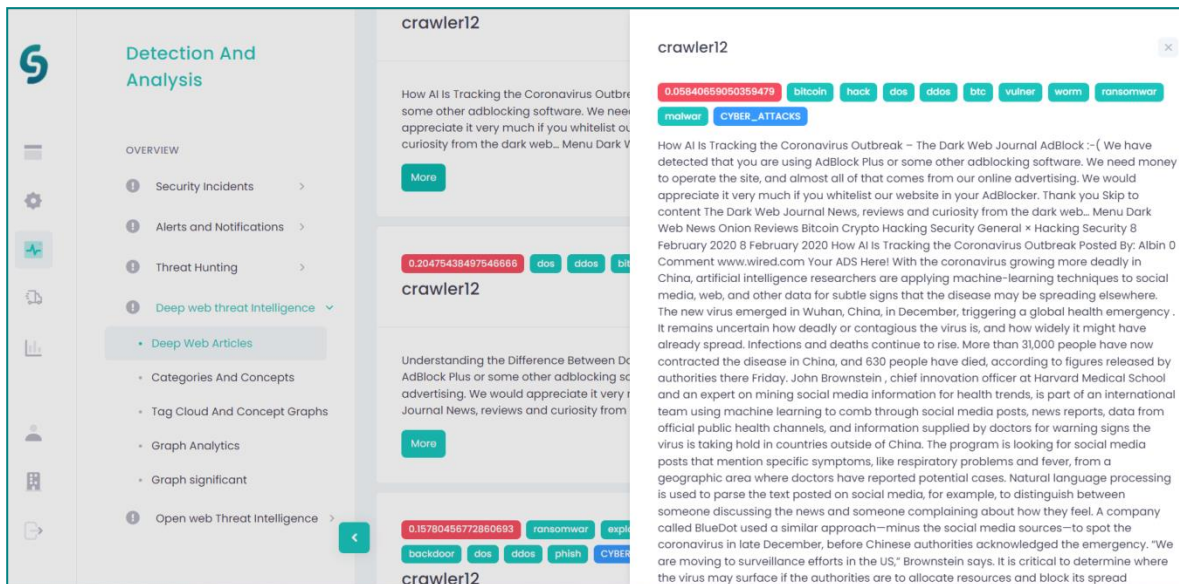


Figure 84: The entire article of a specific document can be accessed and explored.

In addition, the different sources where these articles are published can be viewed at the bottom of the crawler tab (Figure 85).

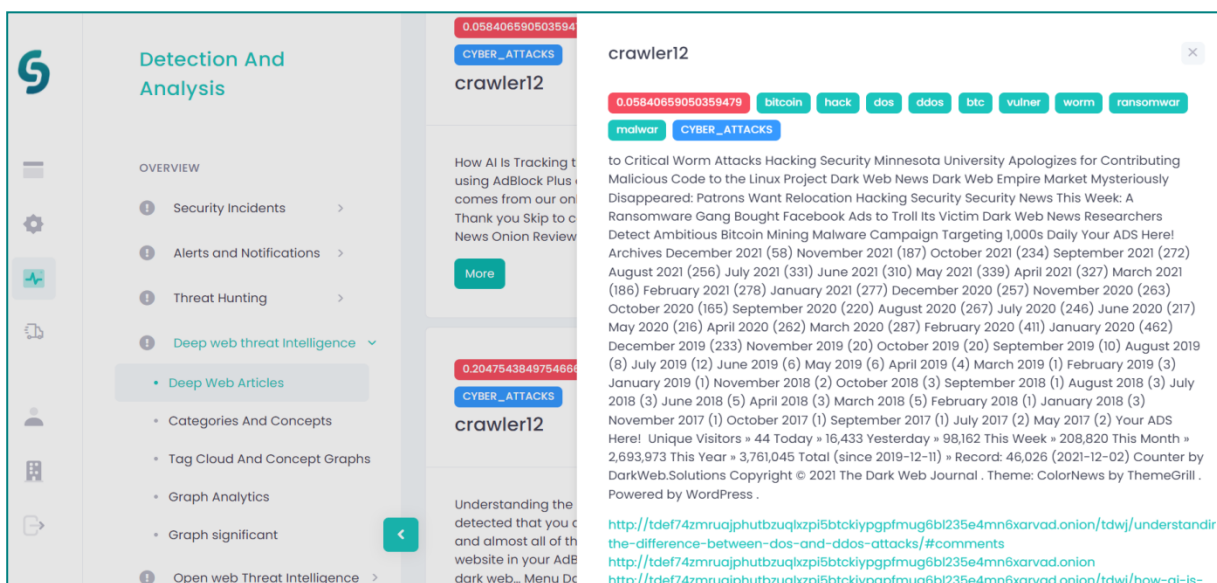


Figure 85: The crawler tab illustrates the different sources where the articles are published in the Deep and Dark Web.

New keywords can be added for customizing further the Security Professional's search by pressing the button "+add keyword" from the "Deep Web Articles" page and filling the corresponding fields, as shown in Figure 86.

## D9.2 – Training Materials and Report on Training Processes

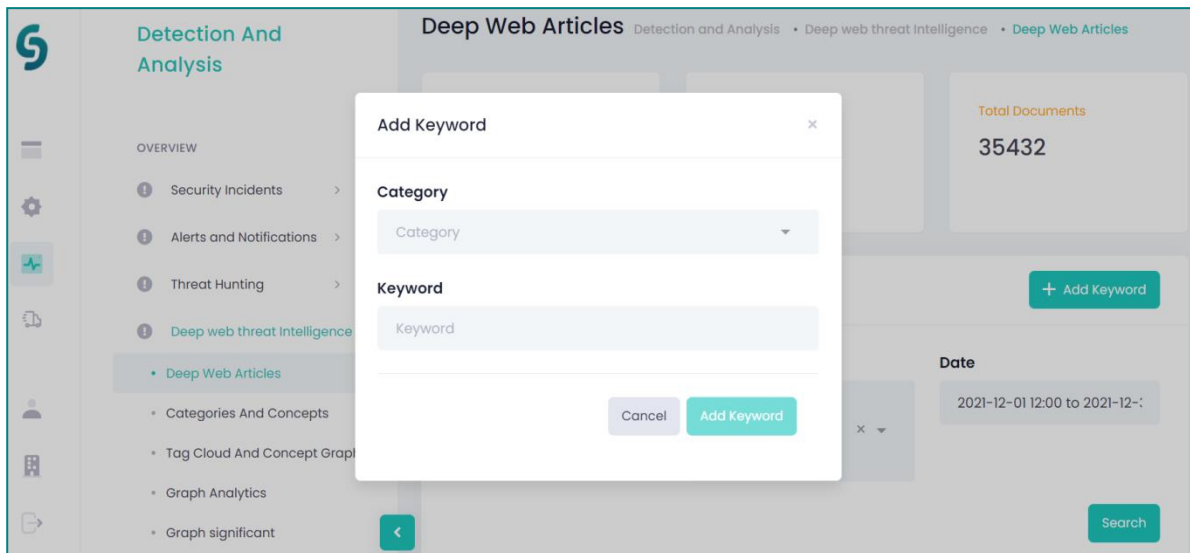


Figure 86: New keywords can be added by the Security Professional to further facilitate searching amid the Deep Web Articles.

### 5.4.2 Categories and Concepts

The “Categories and Concepts” option can be explored from the “Deep Web Threat Intelligence” functionality of the “Detection and Analysis” phase of the dashboard menu.

Herein, several graphs are implemented to perform a further analysis of the identified articles from the Deep and Dark Web upon specific search (Figure 87).

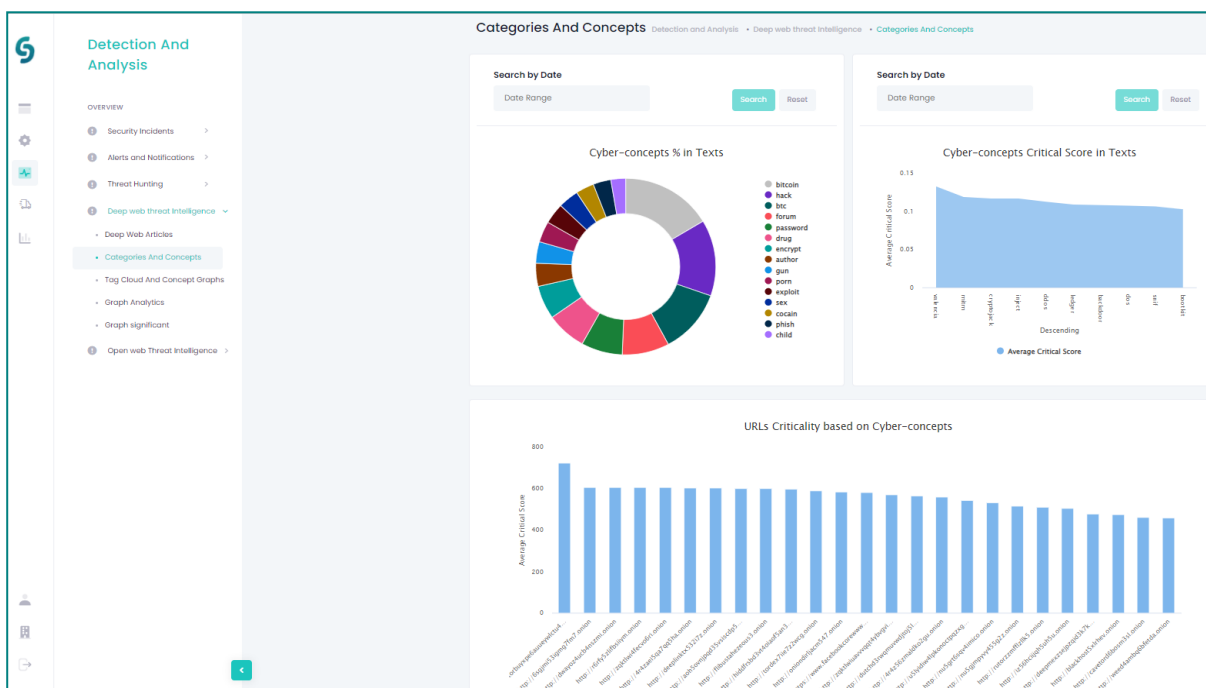


Figure 87: Graphs and statistics on the articles retrieved from the Deep and Dark Web are provided from the Categories and Concepts option of the “Deep Web Threat Intelligence” functionality.

## D9.2 – Training Materials and Report on Training Processes

Moreover, the “Categories and Concepts” option provides the articles’ hot cyber concepts discussed in the Deep and Dark Web related to the specific search provided by the Security Professional in text format based on the crawling and searching mechanisms of the CyberSANE system. For instance, from the doughnut chart can be viewed the frequency of the cyber concepts discussed, e.g. exploit, bitcoin, jack, drug, encrypt, etc. (Figure 88).

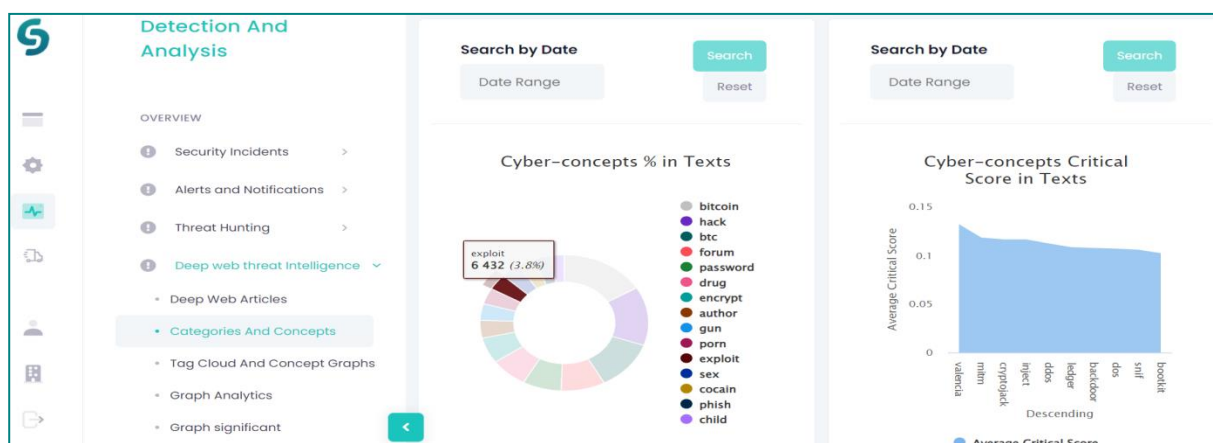


Figure 88: Popular cyber concepts and statistics can be viewed from related graphs. The current doughnut chart (graph on the left) illustrates the number of “exploits” cyber concept found for a specific period.

In addition, cyber concepts’ critical scoring can be viewed from the area chart (Figure 89).

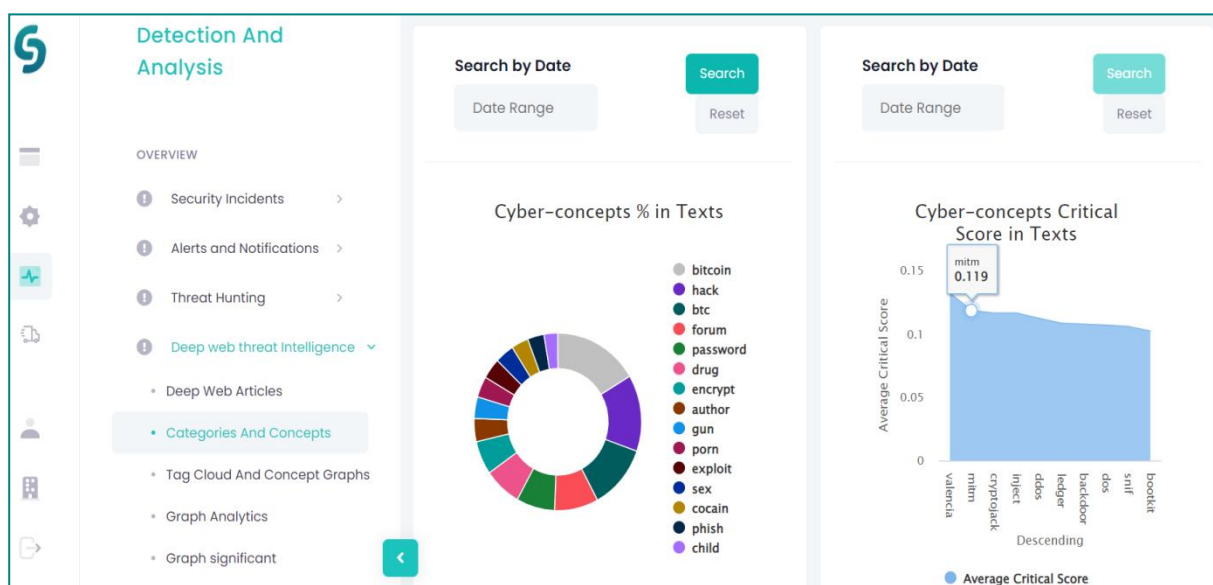


Figure 89: Critical scores for popular cyber concepts can be viewed from related graphs. The current area chart (graph on the right) illustrates the critical score for the “Man-In-The-Middle” attack concept for a specific period.

## D9.2 – Training Materials and Report on Training Processes

As shown in the previous screens (Figure 88; Figure 89), each of the generated graphs can be provided daily upon searching a specific date.

In addition, a graph illustrating the different sources of URLs where the identified articles are published can be explored from the “Categories and Concepts” option of the “Deep Web Threat Intelligence” functionality (Figure 90).

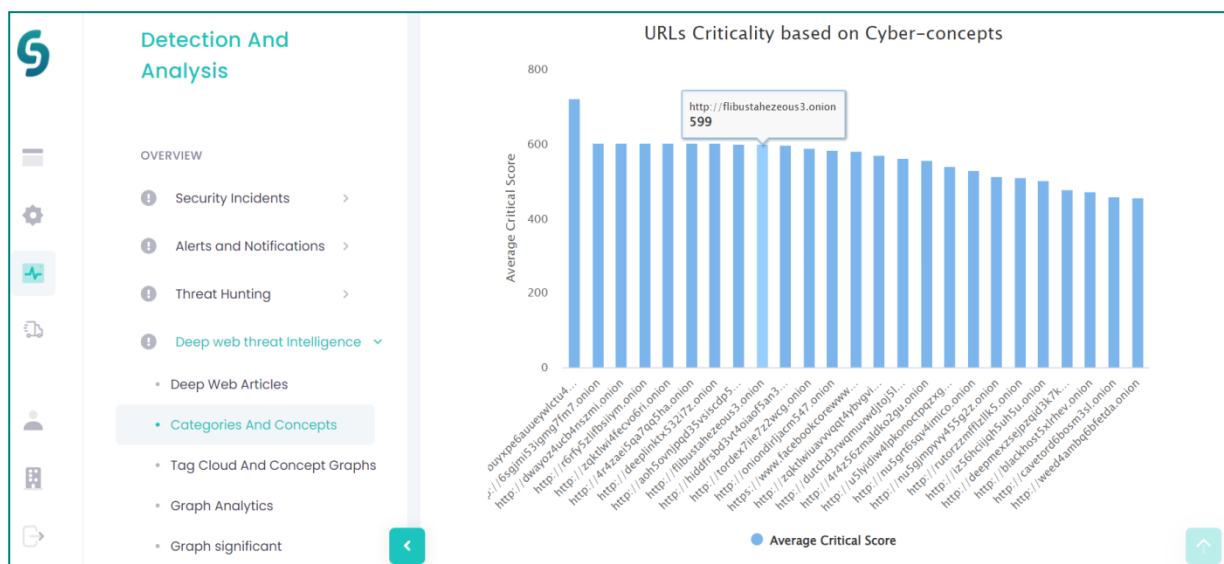


Figure 90: A visualization of the “URLs Criticality based on Cyber Concepts” graph.

A column chart illustrates the number of crawled URLs per day (Figure 91).

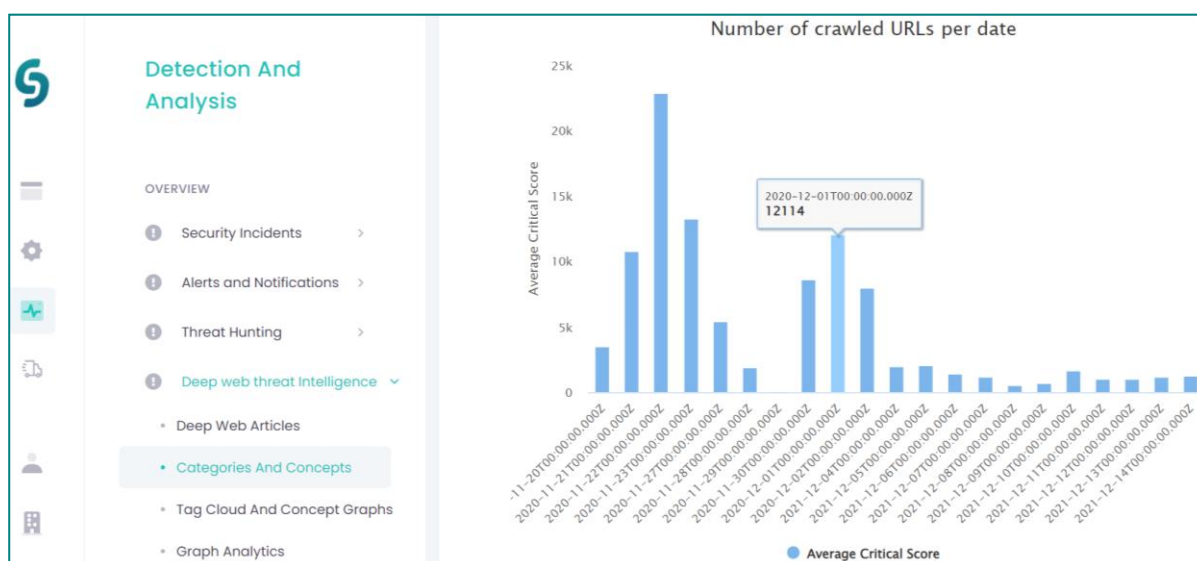


Figure 91: A graph from the “Categories and Concepts” option of the “Deep Web Threat Intelligence” functionality illustrating the number of crawled URLs per day within the selected period.

Furthermore, the Security Professional can review an extended heatmap of URLs scores and cyber concepts and a score for each one of them (Figure 92).



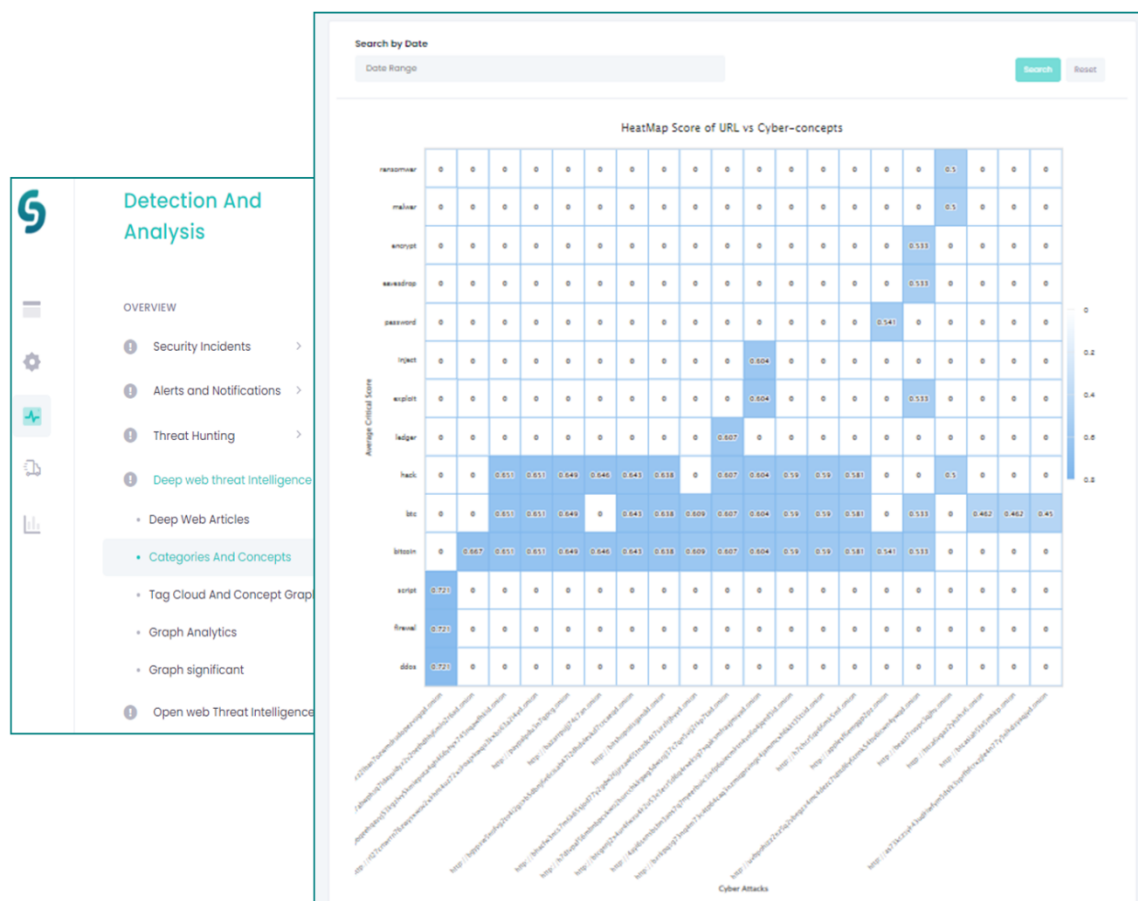


Figure 92: A heatmap of URLs scores and cyber concepts is provided from the “Categories and Concepts” option of the “Deep Web Threat Intelligence” functionality.

### 5.4.3 Tag Cloud and Concept Graphs

Detection and Analysis -> Deep Web Threat Intelligence -> Tag Cloud and Concept Graphs

The “Tag Cloud and Concept Graphs” can be viewed from the “Deep Web Threat Intelligence” functionality of the “Detection and Analysis” phase of the dashboard menu. Tag Cloud and Concept Graphs” are generated based on the crawling and searching mechanisms performed in the Deep and Dark Web and they can be searched upon specific date range (Figure 93).

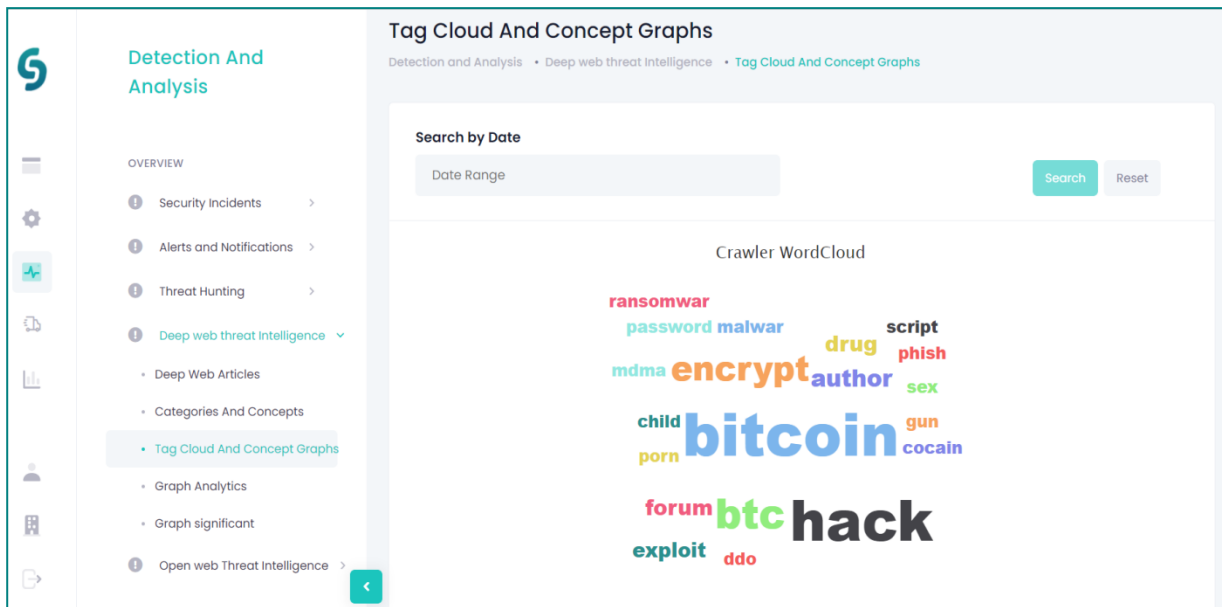


Figure 93: A screen from the “Tag Cloud and Concept Graphs” of the “Deep Web Threat Intelligence” functionality.

#### 5.4.4 Graph Analytics

Detection and Analysis -> Deep Web Threat Intelligence -> Graph Analytics

“Graph Analytics” can be viewed from the “Deep Web Threat Intelligence” functionality of the “Detection and Analysis” phase of the dashboard menu (Figure 94) to explore relations between URLs and concepts.

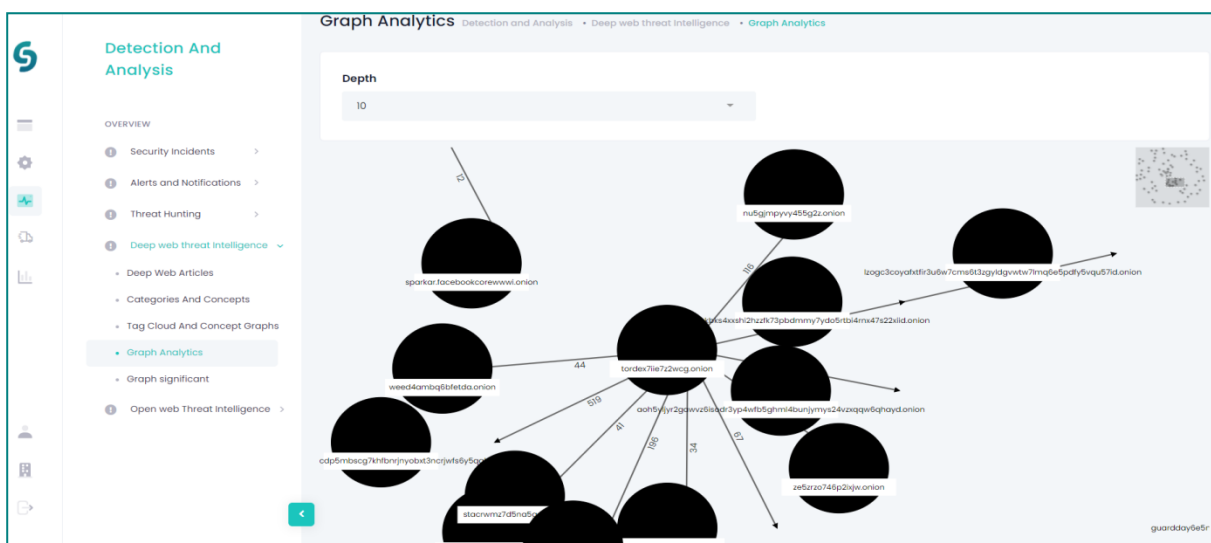


Figure 94: A screen from the “Graph Analytics” of the “Deep Web Threat Intelligence” functionality.

### 5.4.5 Graph Significant

Detection and Analysis -> Deep Web Threat Intelligence -> Graph Significant

The “Graph Significant” option can be reached from the “Deep Web Threat Intelligence” functionality of the “Detection and Analysis” phase of the dashboard menu (Figure 95). The Security Professional can explore further graph analytics on concepts or URLs by selecting “concepts” or “html” or preferred keywords and choosing the number of samples to appear.

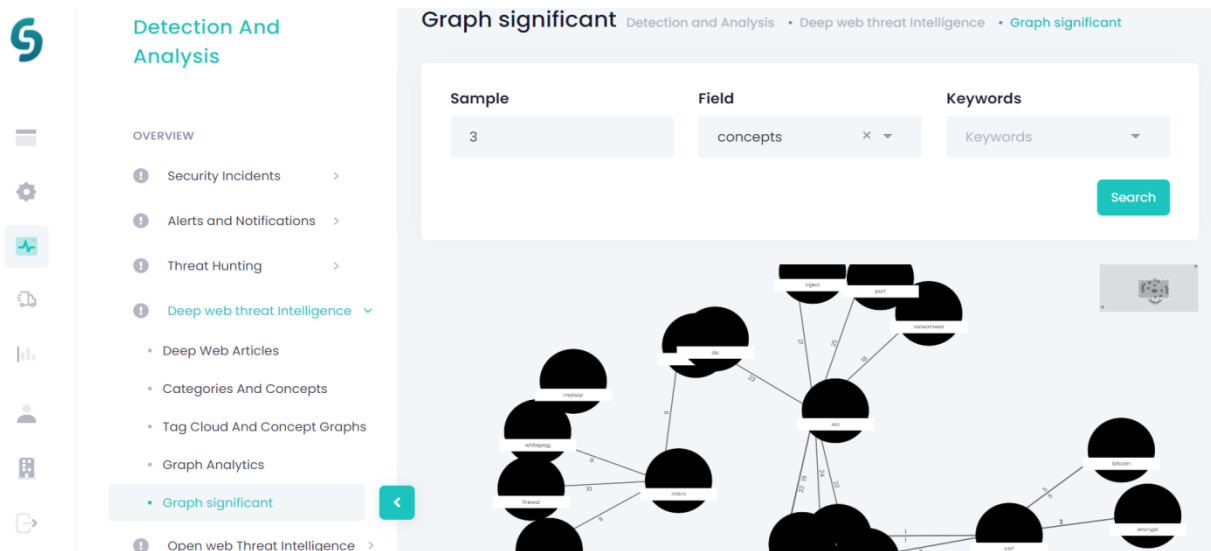


Figure 95: A screen from the “Graph Significant” of the “Deep Web Threat Intelligence” functionality.

## 5.5 Open Web Threat Intelligence

The “Open Web Threat Intelligence” functionality of the CyberSANE system allows the Security Professional to further investigate the real evidence gathered from the CII and get better prepared and make proper decisions at a later stage of the incident handling process for eradication and recovery actions towards the detected evidence. In particular, the Security Professional can search for articles from the open Web related to the identified evidence on the organisation’s CII. The “Open Web Threat Intelligence” functionality provides the below option for crawling and providing information from the open web (e.g. social networking, security newsfeeds, etc.), described in the following section (Figure 96):

- Articles



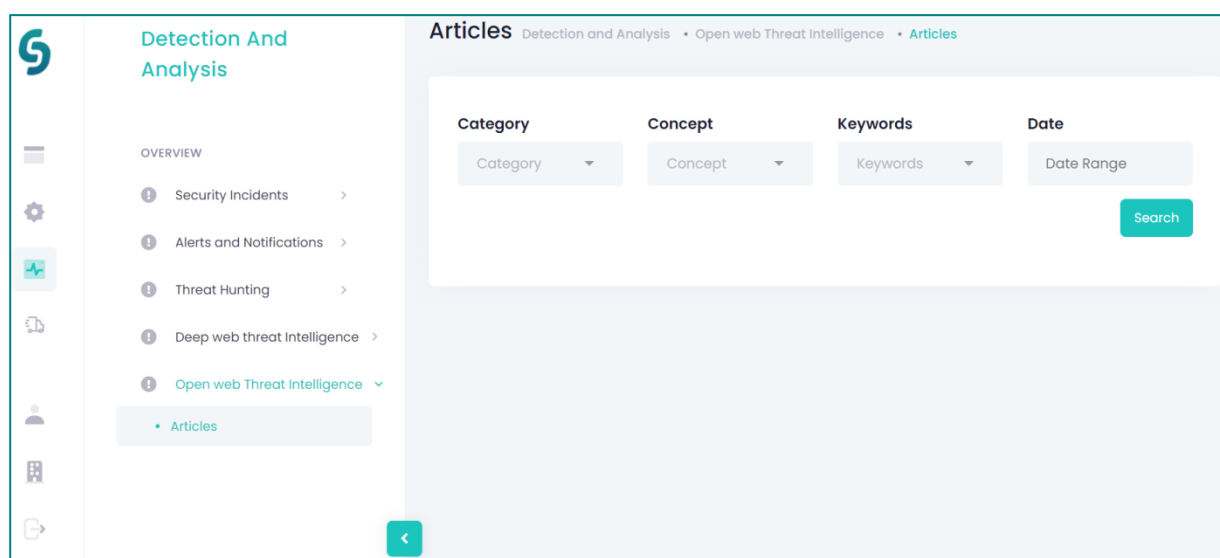


Figure 96: A screen from the “Open Web Threat Intelligence” functionality of the “Detection and Analysis” phase.

### 5.5.1 Articles

Detection and Analysis -> Open Web Threat Intelligence -> Articles

“Articles” from the open web can be searched and viewed from the “Open Web Threat Intelligence” functionality of the “Detection and Analysis” phase of the dashboard menu (Figure 96). The Security Professional can search for obtaining further information upon the identified evidence on the organisation’s CII, by filling the “Category”, “Concepts”, “Keyword” and “Date” fields in the “Open Web Threat Intelligence” environment (Figure 97) and pressing the “Search” button.



Figure 97: Security articles can be searched from the open web from the “Open Web Threat Intelligence” functionality.

Upon specific search (e.g. Figure 97) a list of related articles from the open web can be viewed (Figure 98).

## D9.2 – Training Materials and Report on Training Processes

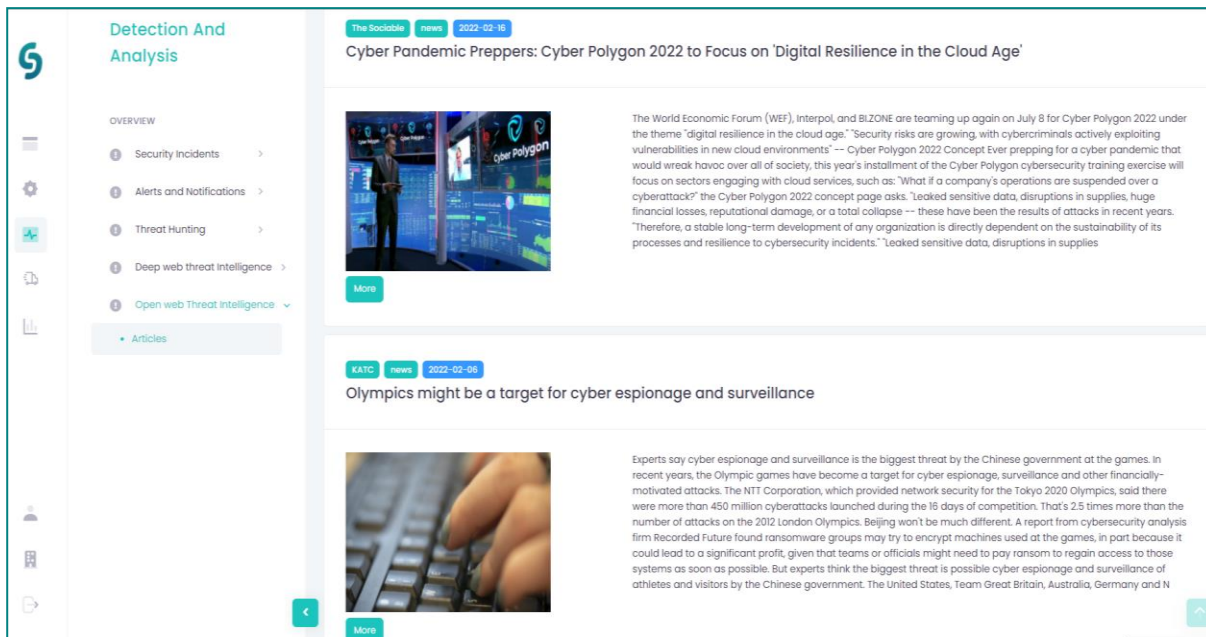


Figure 98: Articles from the open web can be explored upon search from the “Open Web Threat Intelligence” functionality.

By tapping on the “More” button under an article, the Security Professional can delve into the entire content of the article and see the respective sources where the article has been published and the publication date (Figure 99).

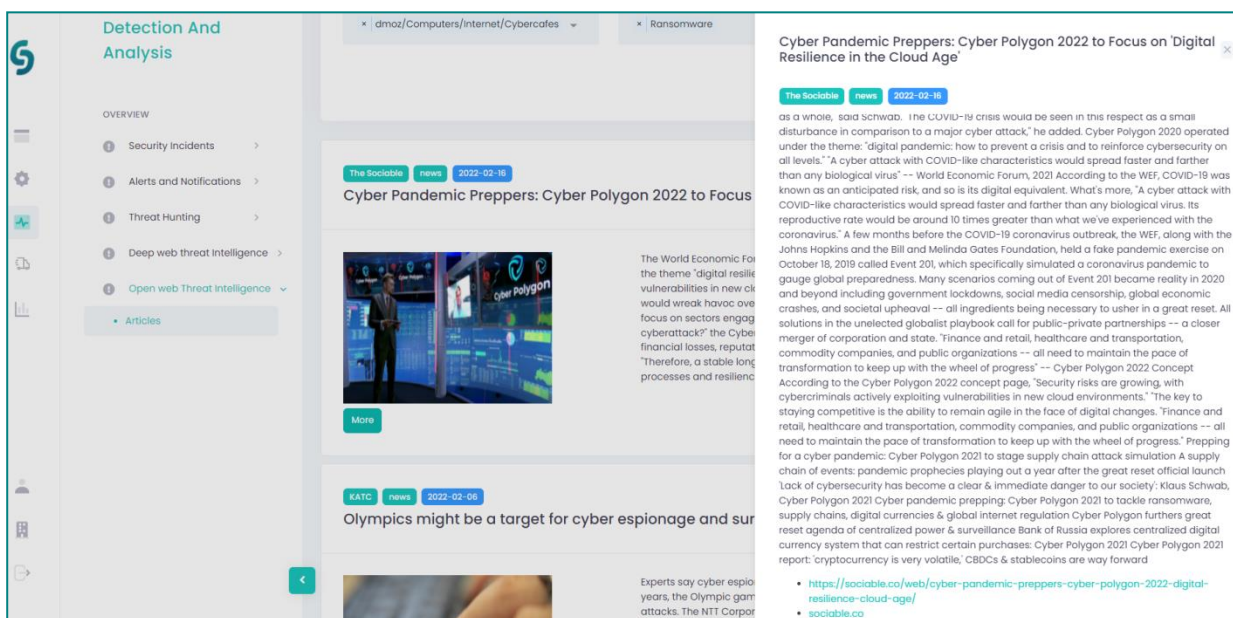


Figure 99: The entire content of an article and the sources where it is published on the open web can be viewed from the “Open Web Threat Intelligence” functionality.

## 6. Containment, Eradication and Recovery Phase

The Containment, Eradication and Recovery Phase in the CyberSANE system supports only the Containment activities of the incident handling process. Once the Security Professional has gathered the risk assessment results from the Preparation incident handling phase and all the evidence and relevant information retrieved from the Web during the “Detection and Analysis” incident handling phase, he/she can use the “Containment, Eradication and Recovery” functionality of the CyberSANE system to create strategies for eradication and recovery. The current incident handling phase can be reached upon clicking on the respective icon from the dashboard menu. Moreover, it supports a Simulation Environment where the Security Professional can experiment on different attack paths and gather information for proper decision making for eradication and recovery.

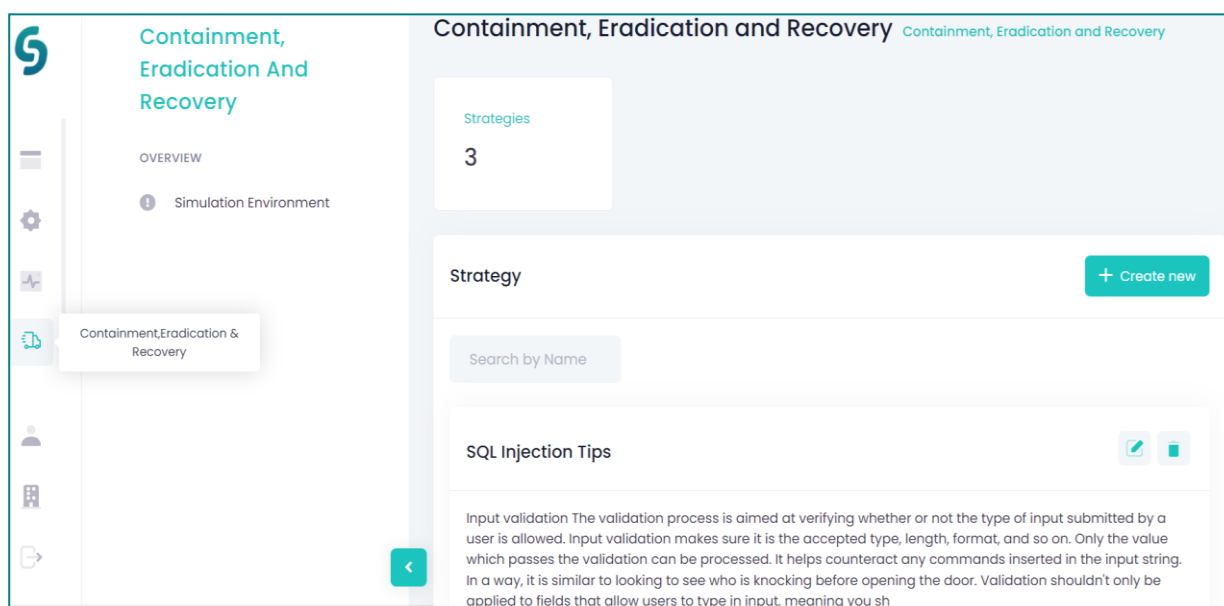


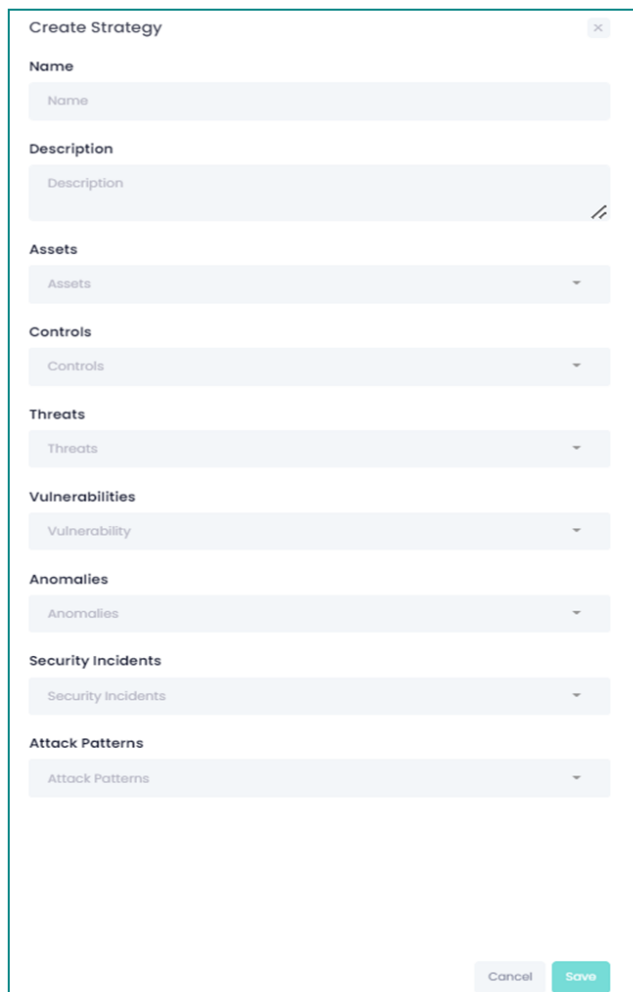
Figure 100: A screen from the “Containment, Eradication and Recovery” functionality of the CyberSANE system.

### 6.1 Create a Strategy

By selecting the “Containment, Eradication and Recovery” Phase icon from the dashboard menu and clicking on the “Create new” button from the Strategy table (Figure 100), the Security Professional can create a strategy for eradication and recovery. Then,

the “Create Strategy” tab appears, where the Security Professional can fill the corresponding fields:

- Name: specify the name of the strategy
- Description: provide a descriptive text of the strategy
- Assets: specify the organisation’s assets upon which the strategy will be implemented from a dropdown list (Optional)
- Controls: provide specific security controls from a dropdown list (Optional)
- Threats: provide specific threats from a dropdown list (Optional)
- Vulnerabilities: provide specific vulnerabilities from a dropdown list (Optional)
- Anomalies: provide specific detected anomalies from a dropdown list (Optional)
- Security Incidents: provide specific detected security incidents from a dropdown list (Optional)
- Attack Patterns: provide specific recognized attack patterns from a dropdown list (Optional)



The screenshot shows a web form titled "Create Strategy" with a close button (X) in the top right corner. The form contains several input fields, each with a label and a placeholder text:

- Name:** A text input field with the placeholder "Name".
- Description:** A text input field with the placeholder "Description" and a small icon of two overlapping lines in the bottom right corner.
- Assets:** A dropdown menu with the placeholder "Assets".
- Controls:** A dropdown menu with the placeholder "Controls".
- Threats:** A dropdown menu with the placeholder "Threats".
- Vulnerabilities:** A dropdown menu with the placeholder "Vulnerability".
- Anomalies:** A dropdown menu with the placeholder "Anomalies".
- Security Incidents:** A dropdown menu with the placeholder "Security Incidents".
- Attack Patterns:** A dropdown menu with the placeholder "Attack Patterns".

At the bottom right of the form, there are two buttons: "Cancel" and "Save".

Figure 101: The “Create Strategy” tab from the “Containment, Eradication and Recovery” phase functionality.

By documenting these strategies, the latter can be easily shared with the Security Team and all the organisation's users to undertake proper mitigation actions on the detected security events.

## 6.2 Manage a strategy

Strategies can be either edited or deleted. To edit a strategy, the Security Professional shall select the "Containment, Eradication and Recovery" Phase icon from the dashboard menu, and then hit the pen icon (Figure 102).

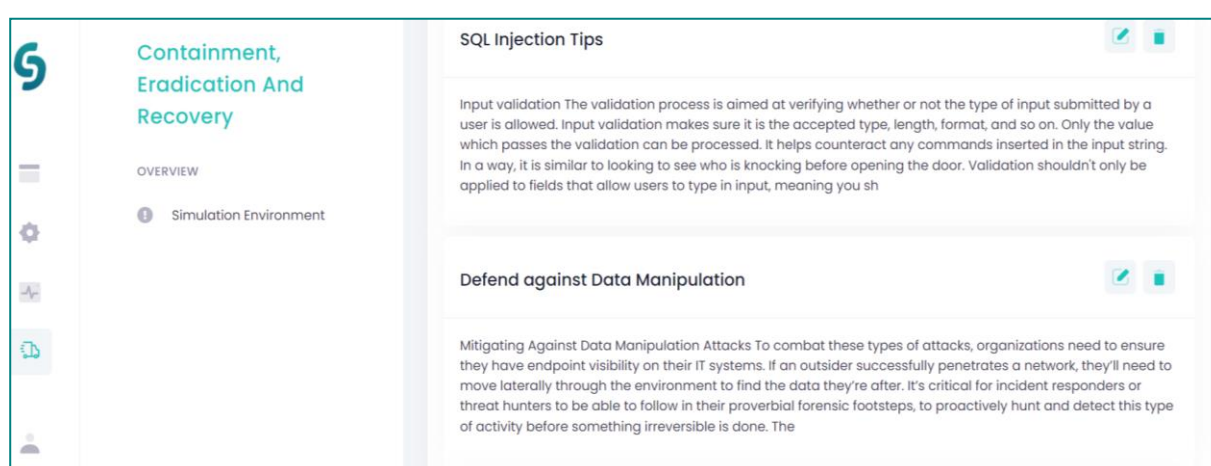


Figure 102: Managing an existing strategy from the "Containment, Eradication and Recovery" phase functionality.

Then, the "Edit Strategy" tab appears, where the Security Professional can review and edit the provided information (Figure 103). To keep the changes on the strategy, the "Save" button shall be clicked.

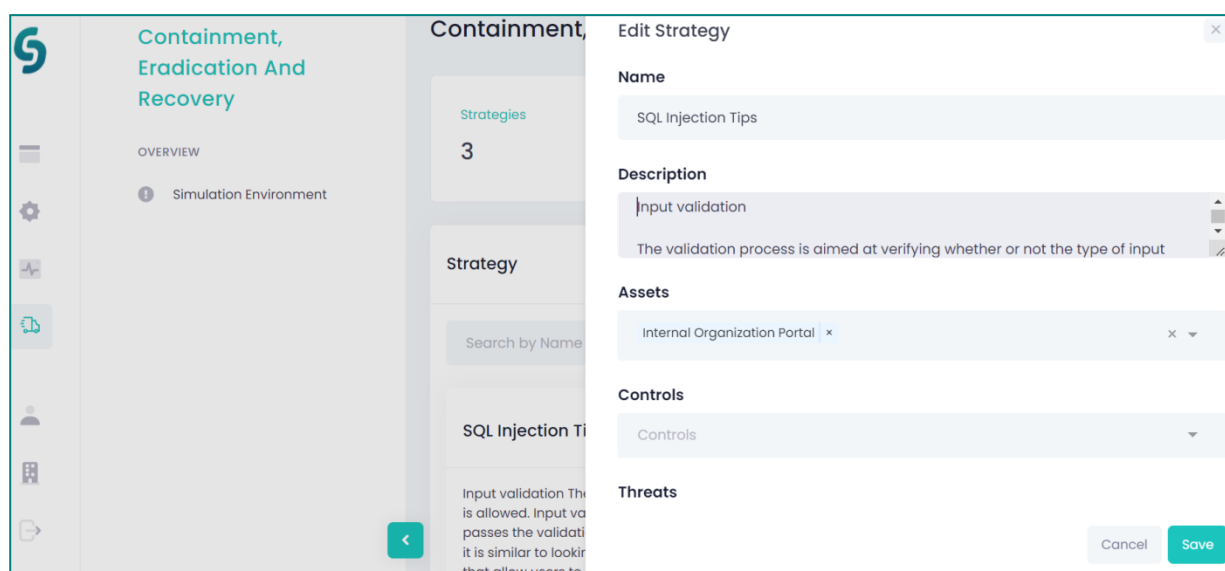


Figure 103: The Security Professional can edit information on an existing strategy from the “Edit Strategy” tab.

## 6.3 Simulation Environment

Containment, Eradication and Recovery -> Attack Path

The simulation environment capabilities can be accessed by selecting the “Simulation Environment” option from the “Containment, Eradication and Recovery” phase of the dashboard menu (Figure 104). Though this virtual environment, the Security Professional can develop threat cases of attack paths and review the reported results.

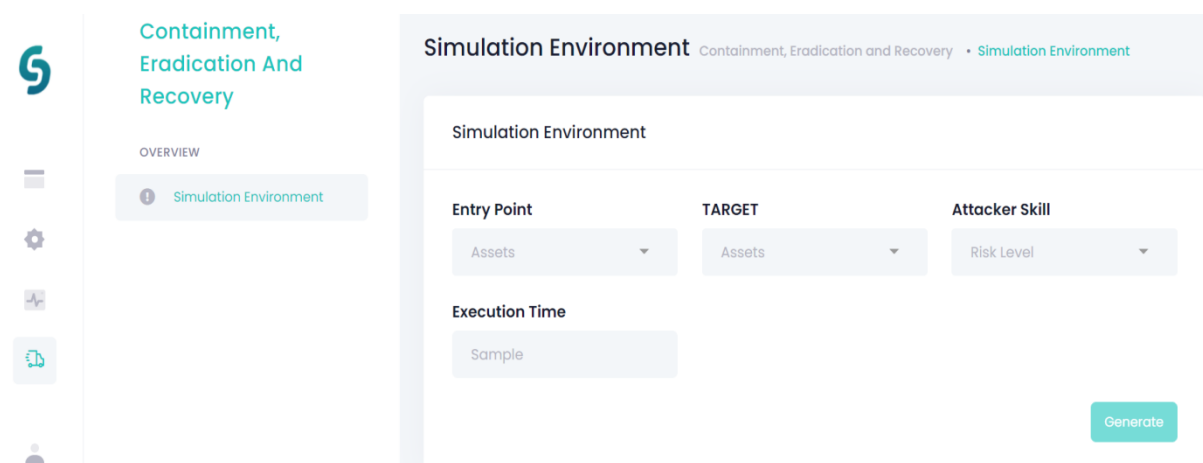


Figure 104: The “Simulation Environment” of the “Containment, Eradication and Recovery” phase.

Furthermore, to build a threat case, the Security Professional shall specify:

- the asset “Entry Point” upon which the attack is initiated

## D9.2 – Training Materials and Report on Training Processes

- the asset “Target Point” which is the attacker’s targeted asset
- the Attacker’s skill (High/Medium/Low)
- the execution time required to provide this attack path

**Example:** Supposing, the Security Professional select the “Node.js” asset as an entry point, the “Ubuntu” asset as a target point, specifies that the attacker has “High” level of expertise and sets the value “5” for the execution time to conduct the attack path (Figure 105).

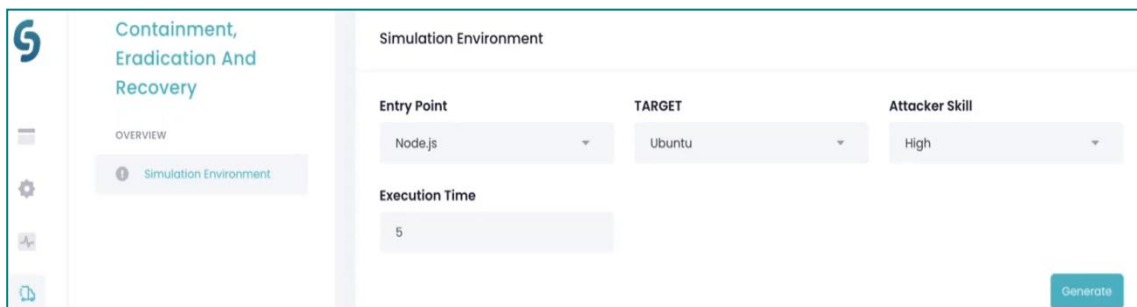


Figure 105: Setting an attack path example.

Once he/she presses the “Generate” button all potential attack paths are provided (Figure 106). The green colour in the attack paths indicates which of them are successful, namely the produced vulnerability chains are set of vulnerability combinations that can potentially produce attack paths upon their exploitation (Chain 1 and Chain 2 in the current example are possible attack paths). Attack paths coloured in red are not successful, where the exploitation of their vulnerability combinations cannot produce attack paths, namely the attacker would not be able to compromise an asset point and use it as a stepping stone to reach and compromise another interconnected asset (Chain 3 in the current example delivers impossible attack paths).

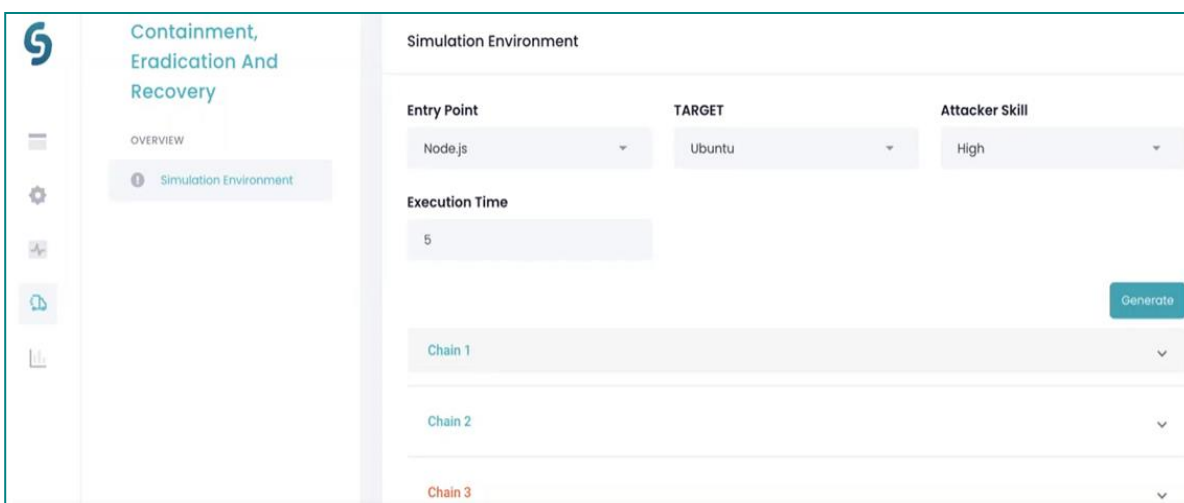


Figure 106: Attack Path results are provided upon a given attack path query. The green coloured chains are successful attack paths that might have been occurred in the organisation’s assets according to the detected evidence.

By selecting a specific chain, an attack graph appears illustrating the attack path on asset nodes (Figure 107).



## D9.2 – Training Materials and Report on Training Processes

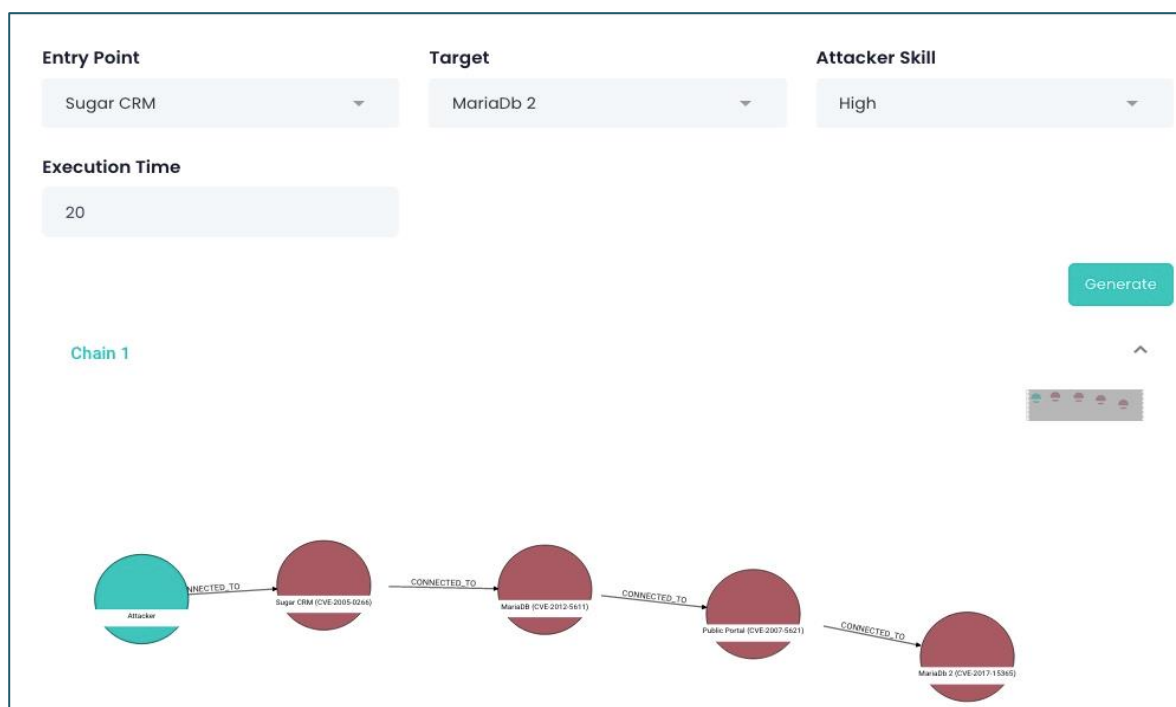


Figure 107: Attack graphs illustrate the potential attack paths between asset nodes upon specific query.

Upon clicking on a specific asset node, a “Node Details” tab appears where security information can be viewed for the specific asset. For instance, in case of selecting the green “chain 1” (successful attack path) in the current example and clicking on the “Node.js” asset entry point (Figure 108) further details appear for the current asset (Figure 109). Figure 109 depicts vulnerability details and information on the estimated business value for the asset “Node.js”.

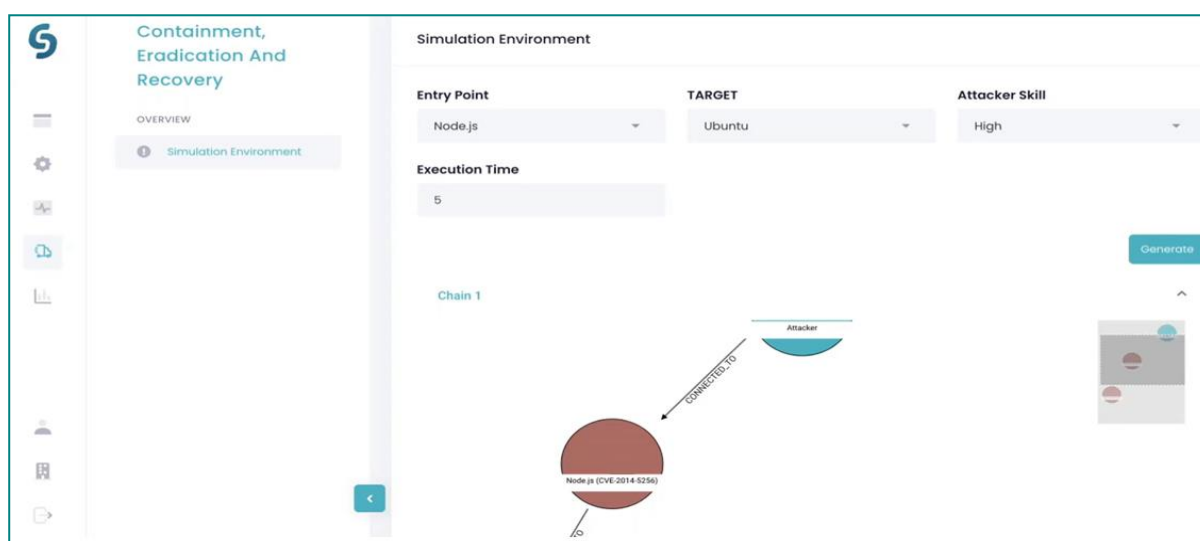


Figure 108: Further security information can be viewed by clicking on a specific asset node.



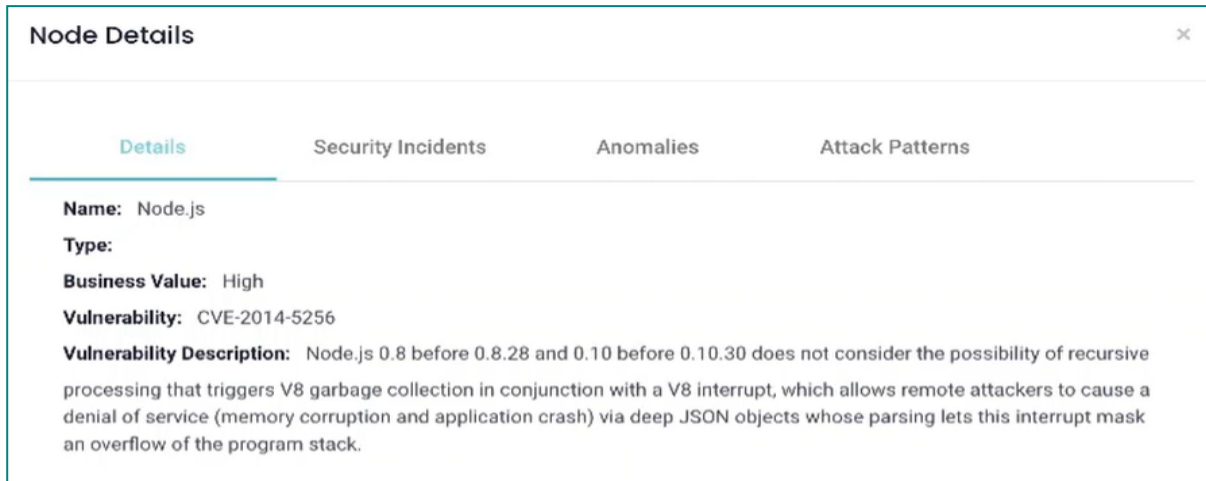


Figure 109: The “Node Details” tab illustrates further security information of an asset node.

In addition, from the “Security Incident”, Anomalies and “Attack Patterns” categories of the “Node Details” tab, the Security Professional can view information either for detected security incidents or anomalies or recognized attack patterns on the asset whether they exist.

The Security Professional by reviewing the attack path results and considering the detected evidence may decide whether an attack path is feasible to occur within the organisation’s CII.

## 7. Post Incident Activity Phase

The Post Incident Activity Phase can create lesson learned from the previous incident handling phases and share it with the security team and all organisation's users. The "Post Incident Activity" Phase can be reached upon clicking on the respective icon of the dashboard menu (Figure 110). The "Post Incident Activity" phase contains the "Data Sharing Agreements" functionality for sharing lessons learned from the previous incident handling phases with other organisations.

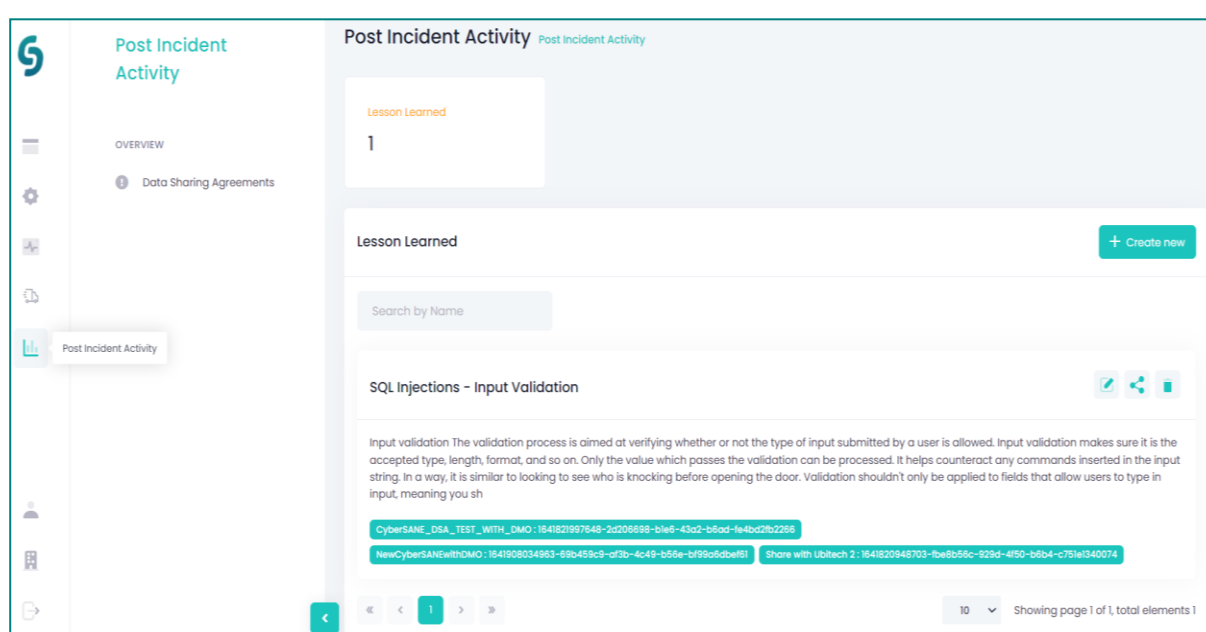


Figure 110: A screen from the "Post Incident Activity" phase of the CyberSANE system.

### 7.1 Create a Lesson Learned

To create a lesson learned from the previous incident handling phases, the Security Professional shall select the "Post Incident Activity" phase from the dashboard menu and then click on the "Create new" button in the "Post Incident Activity" page (Figure 110). Afterwards, the "Create Lesson" tab appears where the Security Professional can fill information for the lesson learned and press the "Save" button (Figure 111). Upon successful process, a new lesson learned has been created.

After creating a lesson learned, the Security Professional can select the proper Data Sharing Agreement for this lesson learned and share it (cf. section 7.2).

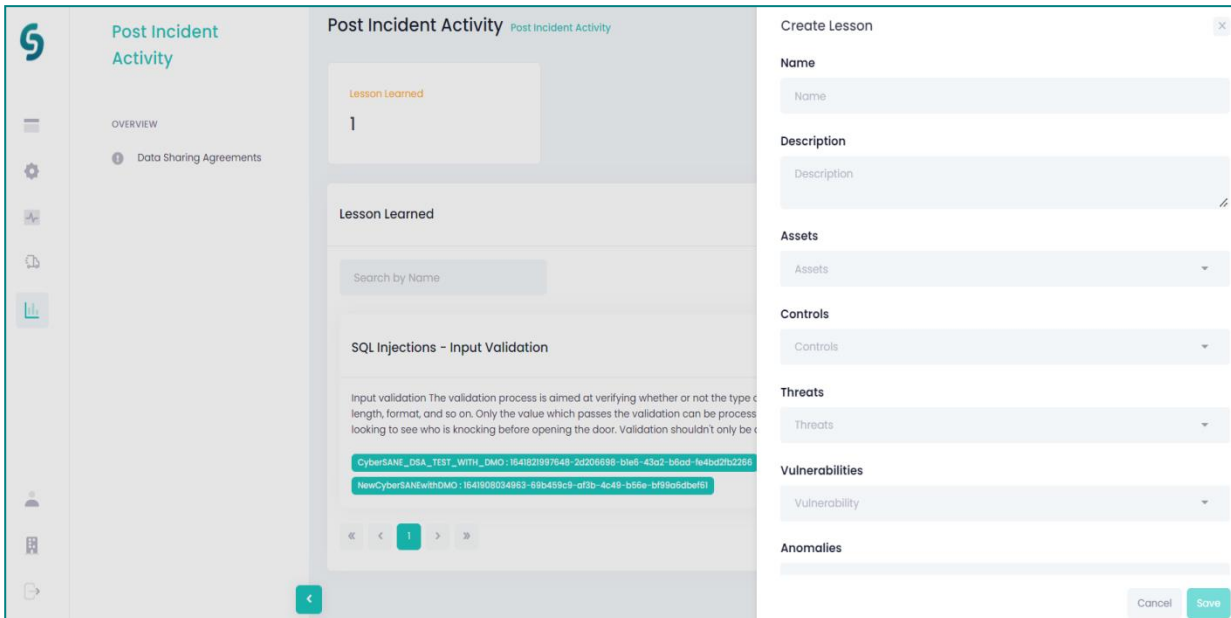


Figure 111: The “Create Lesson” tab shall be filled and saved to create a lesson learned.

## 7.2 Sharing

The CyberSANE system allows the Security professional through the ShareNet services (cf. section 8.4) to share the Lessons Learned with parties in a secure manner. ShareNet provides two methods for information sharing. Thus, with the first method security professionals can share information exploiting the Malware Information Sharing Platform (MISP) API to automatically convert Lessons Learned to the MISP Event format and publish it on a predefined MISP instance. With the second method the ShareNet system will generate and send a notification message with the relevant links to access the corresponding Lessons Learned stored in ShareNet.

Depending on the notification method selected in the Data Sharing Agreement (DSA) (cf. section 7.3), the message will be sent either by email or as an SMS. The system will permit access if a user is authorized to access the Lessons Learned under certain conditions. For this purpose, security professionals can upload Lessons Learned to the local ShareNet database also specifying the corresponding DSA by using the relevant button on the Lessons Learned webpage. Hence, the ShareNet system will validate the DSA, and if the “export to MISP” operation requested by a user is allowed, the system will post that Lessons Learned as a MISP Event or notify the user with the message. Also, depending on the corresponding DSA, the ShareNet system may request PrivacyNet to execute one or multiple Data-Manipulation Operations (DMOs) to preserve privacy (cf. section 7.3).

## 7.3 Data Sharing Agreements

### Post Incident Activity-> Data Sharing Agreements

The Data Sharing Agreement (DSA) Editor is part of the ShareNet component of the CyberSANE system and can be reached by selecting the “Post Incident Activity” phase from the dashboard menu. The next sections describe the DSA creation process starting from the review of existing DSAs and finishing with the application of the DSA.

The ShareNet component of the CyberSANE platform offers two principal functionalities – secure information sharing with third parties and the ability to manage security policies. The sharing functionalities of ShareNet are directly integrated into a CyberSANE allowing security professional to share their data according to security policies defined in DSAs. To manage those DSAs, the ShareNet component provides a build-in tool called DSA Editor.

The DSA Editor provided by the ShareNet systems was designed to allow security professionals to create, review and apply security policies defined through DSAs. The main purpose of the DSA is to protect data from unauthorized access and provide a specification of rules under which access to data is permitted since it is denied by default.

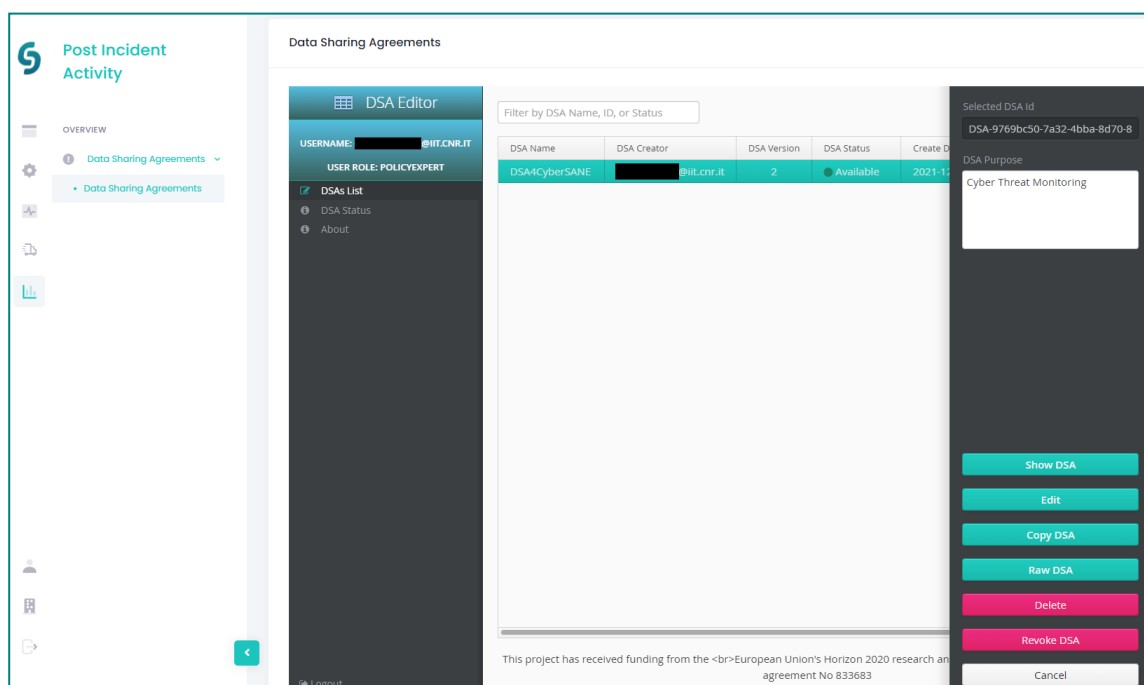


Figure 112: DSA Editor - list of available operations on DSAs

### 7.3.1 Operations on DSA

The DSA Editor provides multiple operations on DSA defined by security professionals. This section provides a list of operations with a corresponding description. Figure 112 depicts the DSA Editor page with the list of available DSAs and allowed operations. Following part provides a list of allowed operations on DSAs and briefly describes each operation.

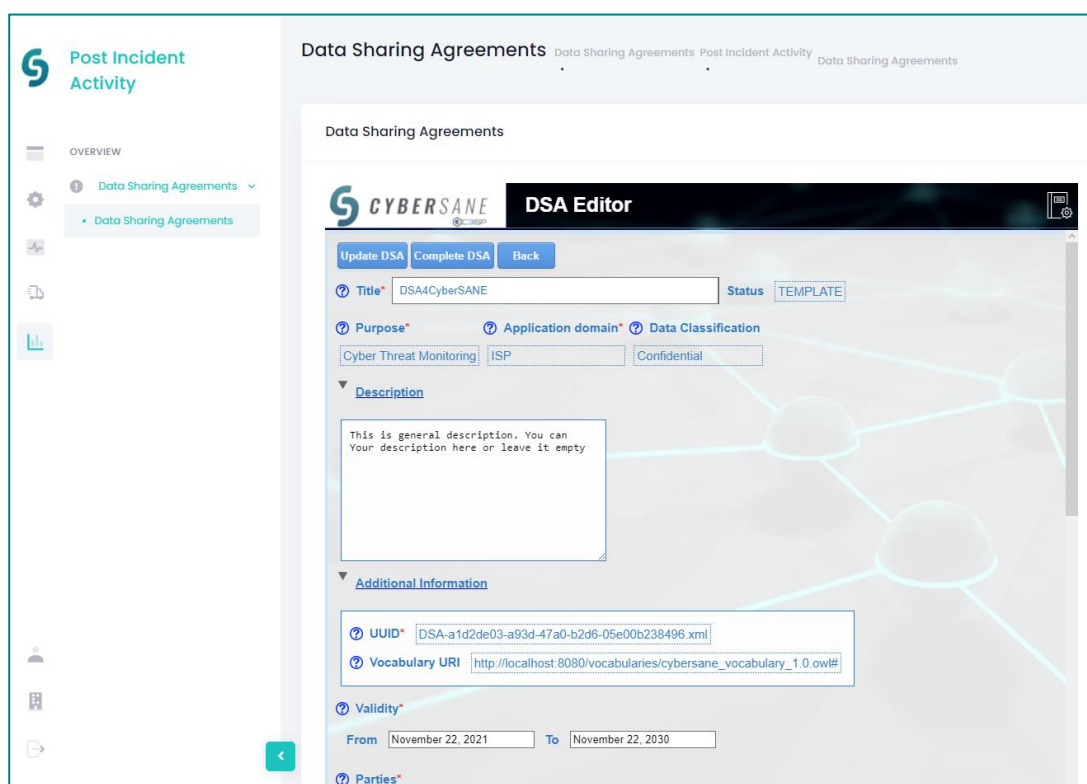
## D9.2 – Training Materials and Report on Training Processes

- **Create DSA** – by using this operation, security professionals can specify their security constraints as a DSA.
- **Show DSA** – allows security professionals to review previously created DSA.
- **Map DSA** – is an operation that makes the DSA available for further usage.
- **Edit DSA** – with this operations security professionals can modify previously defined DSA.
- **Copy DSA** – allows security professionals to create a copy of the DSA.
- **Raw DSA** – by using this operation, security professionals can review the DSA in the .xml format.
- **Delete** – with this operation, security professionals can remove the DSA.
- **Revoke DSA** – allows security professionals to revoke the DSA making it not available for further usage.

It worth noting that after using the **Delete**, **Edit DSA** or **Revoke DSA** operation, corresponding data uploaded to the system will not be longer accessible.

### 7.3.2 Data Sharing Agreement structure

As shown in Figure 113, each DSA has its metadata that includes DSA Title, Purpose, Description and Universally Unique Identifier (UUID).



The screenshot displays the 'DSA Editor' interface within the 'Data Sharing Agreements' section. The interface includes a sidebar with navigation options like 'Post Incident Activity' and 'Data Sharing Agreements'. The main content area shows the 'DSA Editor' form with the following fields:

- Title\***: DSA4CyberSANE
- Status**: TEMPLATE
- Purpose\***: Cyber Threat Monitoring
- Application domain\***: ISP
- Data Classification**: Confidential
- Description**: This is general description. You can Your description here or leave it empty
- Additional Information**:
  - UUID\***: DSA-a1d2de03-a93d-47a0-b2d6-05e00b238496.xml
  - Vocabulary URI**: http://localhost:8080/vocabularies/cybersane\_vocabulary\_1.0.owl#
- Validity\***:
  - From**: November 22, 2021
  - To**: November 22, 2030
- Parties\***

Figure 113: DSA Editor - DSA metadata

- **Title** – specifies title of the DSA that can be used to select particular DSA from the list of available DSAs.

## D9.2 – Training Materials and Report on Training Processes

- **Purpose** – defines the purpose of the DSA, which is a “Cyber Threat Monitoring” in the CyberSANE context.
- **Description** – a textual description of the DSA, which may also describe its purpose and another organisation-specific information.
- **Additional Information** – provides UUID of the DSA and the Vocabulary Uniform Resource Identifier (URI) used to create the DSA.
- **Validity** – specifies the DSA time interval defined between two dates.
- **Parties** – a list of organisations that can use the DSA to map it with their data.

It is worth mentioning that once the DSA validity expires, corresponding data is no longer accessible since the system denies access by default. Hence, to upload new data to the system, security professionals must define new DSA.

### 7.3.3 Parties Policies

Party's policies as a part of the DSA, define security constraints that regulate access to data. Authorisations, Obligations and Prohibitions specify those constraints.

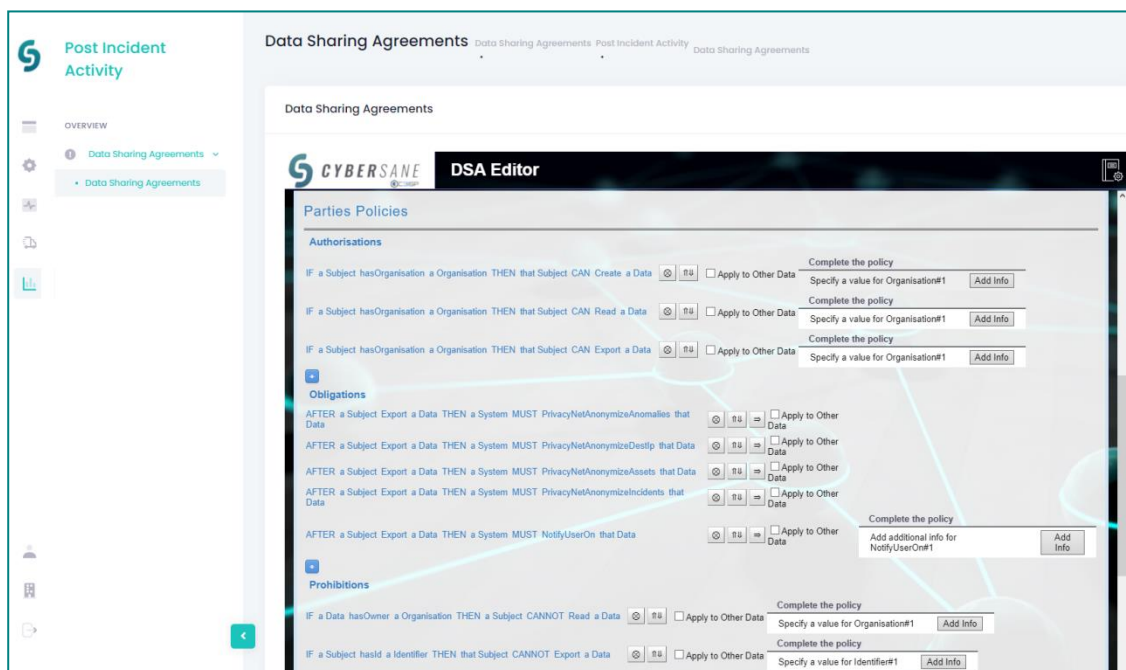


Figure 114: DSA Editor - Parties Policies

### 7.3.4 Authorizations

Authorisations define a set of authorisations functions that specify who can access data and under which conditions it is allowed. Those conditions may be related to user- or data-specific characteristics defined through attributes. In the DSA editor, any user is considered a subject that requests the execution of a specific operation (create, read, export, delete) on data.

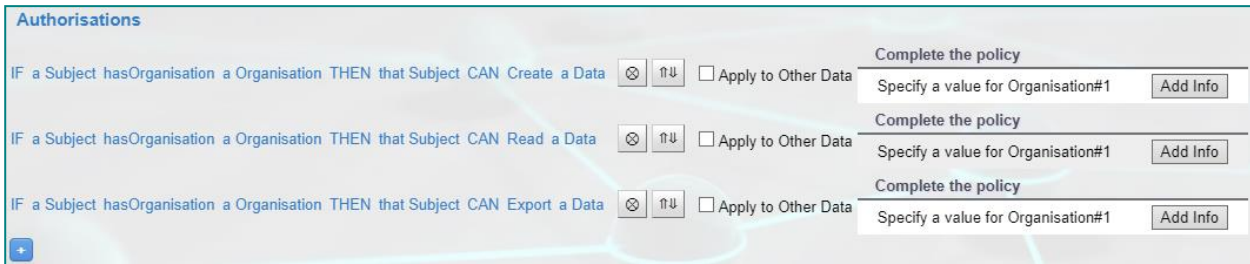


Figure 115: DSA Editor - Authorisations

With the DSA Editor, security specialists can define four different operations, which may be requested by subjects. Those operations are the following:

- **Create** - allows data owners to upload their data to the ShareNet system.
- **Read** - permits users to download corresponding data from the ShareNet system.
- **Export** - allows users/data owners to publish Lesson Learned to the predefined MISP instance.

**Delete** - allows users to remove data from ShareNet.

Depending on data criticality, defined by security professionals, authorisation functions may permit access to data to all users. However, it is also possible to define authorisations with conditions. As mentioned, those conditions may be related to user- or data-specific attributes.

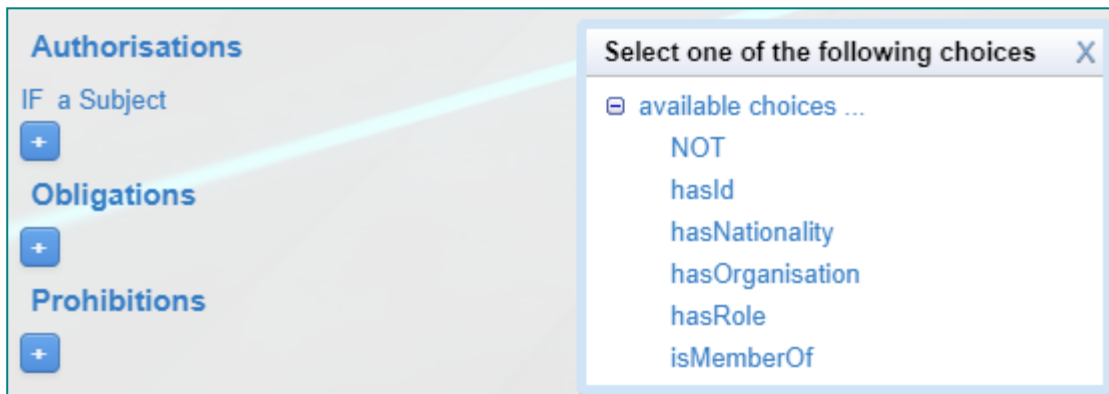


Figure 116: DSA Editor - Subject attributes for authorisations

With the DSA Editor security professionals can allow access to their data only for user with affiliation and/or role. Some attributes are the following:

- **hasId** – permits access to data for a subject with particular ID.
- **hasNationality** – allows subjects from specific countries to access data.
- **hasOrganisation** – specifies that subjects with affiliation to a particular organisation(s) can access data.
- **hasRole** – permits access to data for a subject with specific role (e.g., admin, analyst).
- **isMemberOf** – allows subjects from particular group access data.



It worth noting that for attributes, which describe subject's ID (hasId), Nationality (hasNationality), affiliation to particular organisation (hasOrganisation) and membership of a group (isMemberOf), it is required to specific attribute value in the corresponding field available with the “Add info” button.

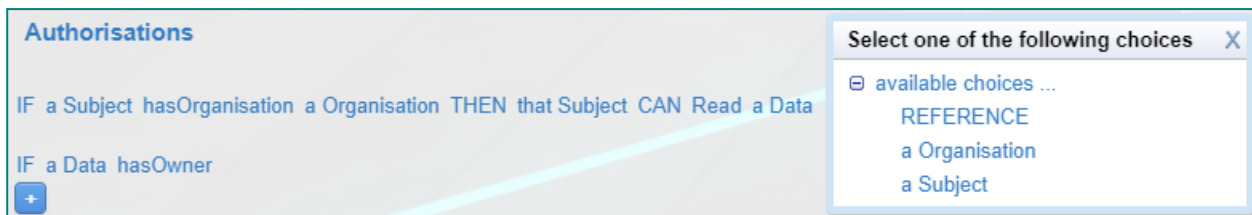


Figure 117: DSA Editor - data attributes for authorisations

It is also possible to use the “NOT” policy constructor for each statement described above to express negation. In addition, depending on data attribute that defines the data owner, it is also possible to specify conditions. Organisation or a particular subject can act as a data owner.

### 7.3.5 Obligations

Obligations define a set of obligation rules that define required operations that must be performed either by a system or a subject. In the CyberSANE context, obligations are used to specify Data Manipulation Operations (DMOs) executed by the subsystem of the CyberSANE platform on data either at the moment when a data owner uploads data or before providing data to other users.

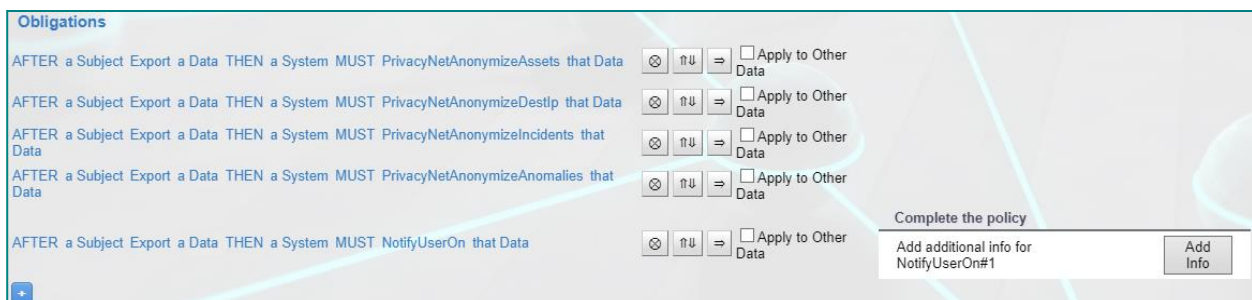


Figure 118: DSA Editor - Obligations

The DSA Editor allows specifying four predefined DMOs that aim at anonymising sensitive data specified in Lessons Learned. Those operations are:

- **AnonymiseAssets** – allows security professionals to anonymise assets information specified in the Lesson Learned.
- **AnonymiseDestIp** – anonymises all IP addresses of the targeted equipment.
- **AnonymiseIncidents** – security professionals can anonymise security incidents specified in Lessons Learned.
- **AnonymiseAnomalies** – allows security professionals to anonymise anomalies information of the Lessons Learned.



In addition to anonymisation functions, security professionals can notify user or data owner about any operation performed on data by using the **NotifyUserOn** operation. For example, once a security professional uploads a Lesson Learned to ShareNet, the system will generate a message and notify a user about uploaded information. For this, security professionals can select one of the available options, which are e-mail or SMS message. This operation requires security professionals to specify corresponding contact. The message includes the URL to the Lesson Learned stored in the ShareNet component.


### 7.3.6 Prohibitions

Similarly to authorisation rules, prohibitions define a set of operations, which are **“NOT”** allowed on data under certain conditions. For example, authorisations may allow access to data for users with specific affiliations, while prohibitions may restrict access to that data for users with a particular role from all organisations.



Figure 119: DSA Editor – Prohibitions

Once a security professional specified authorisations, obligations and prohibitions, it is possible to complete the DSA creation process by using the **Complete DSA** button. In case of modification of the DSA, security professionals should use **Update DSA** button. After that the DSA Editor will return a user to the page of available DSAs and it is necessary to map DSA to make it available for further usage.

Hence, to share Lessons Learned with organisations, security professionals have to use share button depicted as  and then select a DSA from the list of available DSAs.

## D9.2 – Training Materials and Report on Training Processes

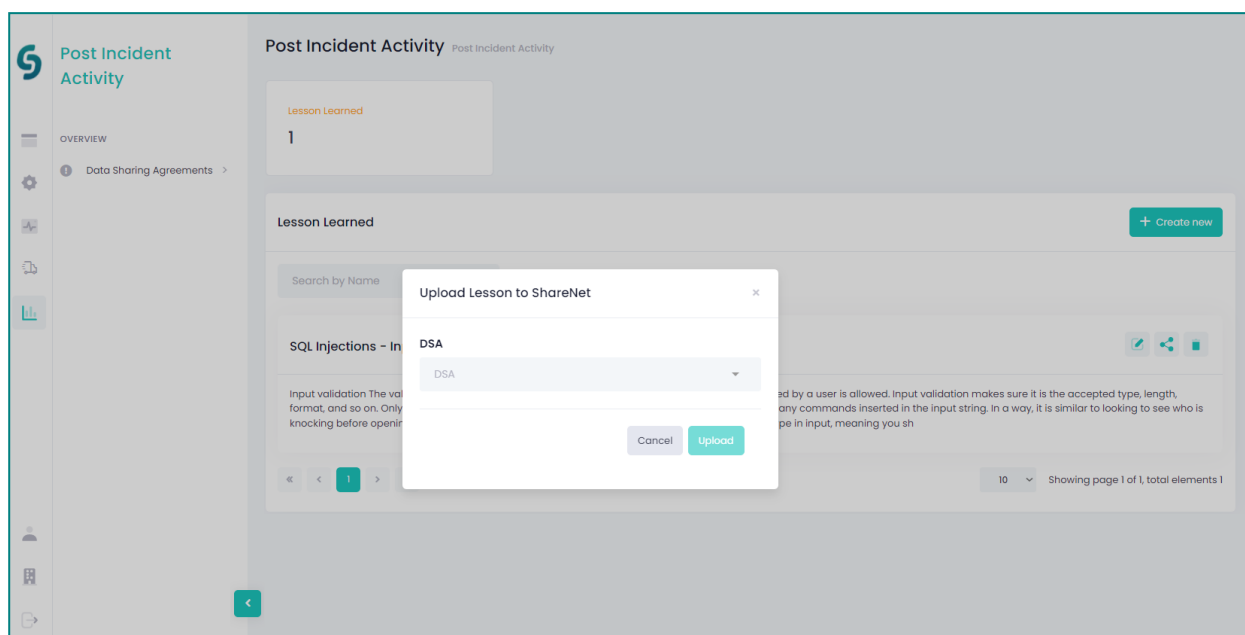


Figure 120: CyberSANE Post Incident Activity - select DSA

After that, ShareNet will evaluate a request against the selected DSA and if evaluation results in “permit”, then the system will store selected Lesson Learned and perform other operations if they were specified in the DSA previously.

## 8. The CyberSANE services

The CyberSANE functionalities of the incident handling phases are driven from services and operations driven by the following CyberSANE components which are further described and visualized in the following:

- LiveNet
- DarkNet
- HybridNet
- ShareNet
- PrivacyNet

### 8.1 LiveNet

CyberSANE LiveNet component operates as the interface between the underlying Critical Information Infrastructure and the CyberSANE platform, combining security information and event management functions, into one security management system.

It undertakes the responsibility of preventing and detecting threats, providing security professionals and experts both insight into and a track record of the activities within their Information Technology environment.

It provides the following operations:

- Attack Patterns Registration and Update
- Live Monitoring
- Security Event Classification and Notification
- Known Threat Detection
- Security Incident Detection
- Signature Generation

LiveNet operations are provided by the following supporting tools in the CyberSANE system:

- GLORIA
- SiVi
- XL-SIEM

The LiveNet service can be viewed in Figure 121 and described in the following sections.

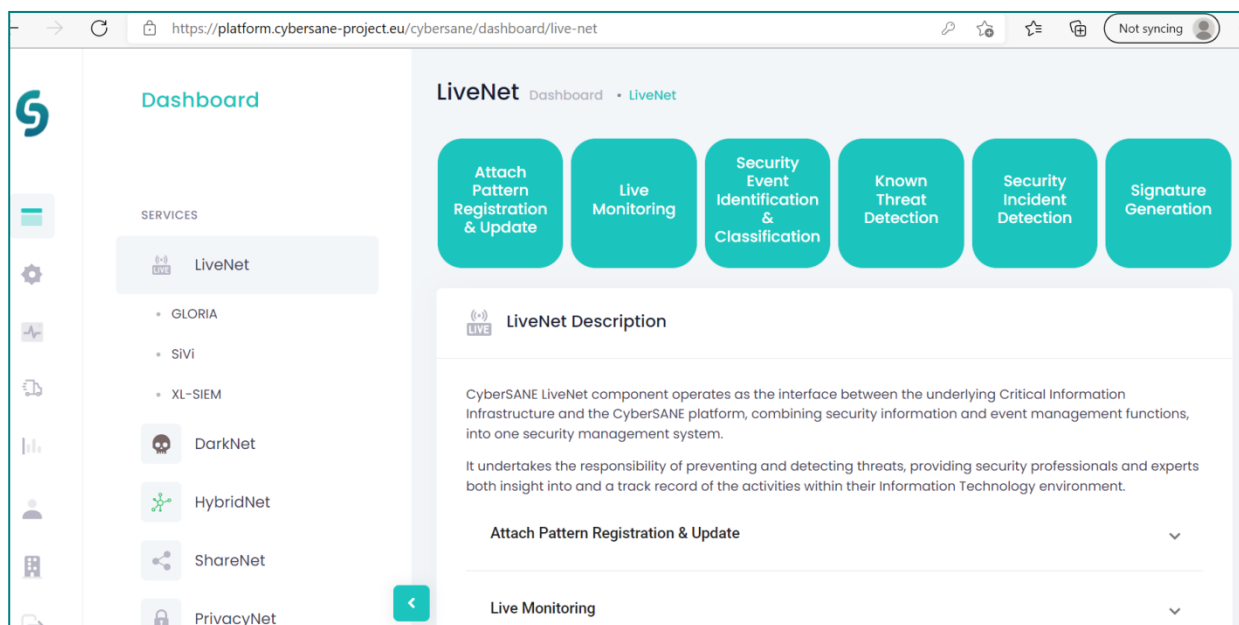


Figure 121: The CyberSANE LiveNet service.

## 8.1.1 LiveNet Operations

### 8.1.1.1 Attack Patterns Registration and Update

New attack patterns are registered and applied for real-time security incident detection, as part of the knowledge base, in order to be prepared for detection of new attack vectors and patterns.

### 8.1.1.2 Live Monitoring

It implements a set of monitoring features, for gathering information from critical assets and devices. All security-related information is monitored in real-time, to be further processed and classified.

### 8.1.1.3 Security Event Classification and Notification

Security logs are processed to extract relevant attributes and information. Once the extraction is performed, depending on the values of each attribute, the information is tagged and classified.

### 8.1.1.4 Known Threat Detection

Security events are properly evaluated against event correlation rules, representing the conditions described in the attack patterns. Whenever the patterns are matched, LiveNet provides an incident alert with contextualized information in order to be analysed by security analysts, as part of the incident management process.

#### **8.1.1.5 Security Incident Detection**

Once attack patterns are detected based on correlation rules, the incident management lifecycle starts providing all the contextualized information to be presented to security analysts, via alerts and messages. The latter investigates the incident, by analysing all security events attributes, such as payloads, attack vectors, and the criticality of the incident, based on the possible harm against the organisation assets.

#### **8.1.1.6 Signature generation**

The incident is documented, by complementing additional findings of possible variations to detect the same type of attack from a general perspective, derived from the generation of attack signatures that are included in the incident knowledge base.

### **8.1.2 LiveNet Tools**

#### **8.1.2.1 GLORIA**

GLORIA (TRL=9) is a SIEM toolchain aimed at SOC operation in order to monitor an infrastructure, covering both IT and OT components.

It provides functionality beyond the SIEM. While the classic SIEM solution addresses the security operation by detecting the known threats based on event correlation rules derived from already known signatures and patterns, GLORIA provides advanced intelligence correlation techniques to face targeted and advanced threats that have not been detected yet, and thus, are not matched by any signature, as well as automation and orchestration mechanisms in order to improve the efficiency and effectiveness of the incident response teams:

- Security Incident Handling and Response
- Encrypted Network Analysis
- Attack scenarios representation
- Log data transformation and normalization
- Activity classification and modelling

#### **How does it contribute to the overall effectiveness of CyberSANE System?**

GLORIA allows the normalization of logs, activity classification and modelling and attack scenarios representation, perform the appropriate transformation, normalization and representation tasks to convert the incident-related information and data gathered by the cybersecurity sensors from multiple, different and diverse sources into one unified and convenient format to be presented to cybersecurity analysts, making the investigation tasks more efficient. Based on these functionalities, the collected data is normalized, cleansed to remove redundant and duplicate information.

#### **8.1.2.2 SiVi**

SiVi Tool (TRL=8) is a human-interactive visual-based anomaly detection system 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. SiVi is a human-interactive visual-based anomaly

detection system that is capable of monitoring and promptly detecting several devastating forms of security attacks.

The tool's novelty lies on the development of intuitively visualization graphs capable to offer a quick, reliable, and intuitively overview in the network. In comparison with other tools that offer a simple presentation of the traffic inside the network, SiVi uses pre-trained neural networks that can identify different cyber-attacks.

#### **How does it contribute to the overall effectiveness of CyberSANE System?**

SiVi tool is used in CyberSANE to recognize familiar threats as well as identify threats that have not been experienced before. SiVi Tool's capabilities is integrated into LiveNet for:

- near real-time identification of anomalies;
- proactive reaction to threats and attacks;
- dynamic decision making.

#### **8.1.2.3 XL-SIEM**

XL-SIEM is a Security Information and Event Management (SIEM) solution with added high-performance correlation engine to deal with large volumes of security information. Monitoring and alerts of cyberattacks (broad).

#### **How does it contribute to the overall effectiveness of CyberSANE System?**

As CyberSANE targets CII's the XL-SIEM allows for having an overall status of the system and rise alerts when an attack is detected.

## 8.2 DarkNet

CyberSANE DarkNet component (Figure 122) allows the exploitation and analysis of security, risks and threats related information, embedded in the User Generated Content (UGC), via the analysis of both the textual and meta-data content available from various electronic streams.

It gets advantage of one of the most valuable applications of dark web research, which is the identification of compromised assets or information.

Its main goal is for the threat-actors' communications in Dark Web communities to be properly monitored and analysed. This enables security professionals and experts to identify attacks before they even happen, providing them with the opportunity to manage and close vulnerabilities in their organisational infrastructure, or even strengthen technical controls pre-emptively.

It provides the following operations:

- Incidents Identification
- Attach Techniques Identification
- Tools for Advanced Cyberattacks Identification
- Cyber Actors Activity Reconstruction
- Textual & Meta-data Content Registration
- Risk & Threat Exploitation Analysis

DarkNet operations are provided by the following supporting tools in the CyberSANE system:

- EventRegistry
- MEDUSA

Figure 122 depicts the DarkNet CyberSANE component which is analysed in the next sections.

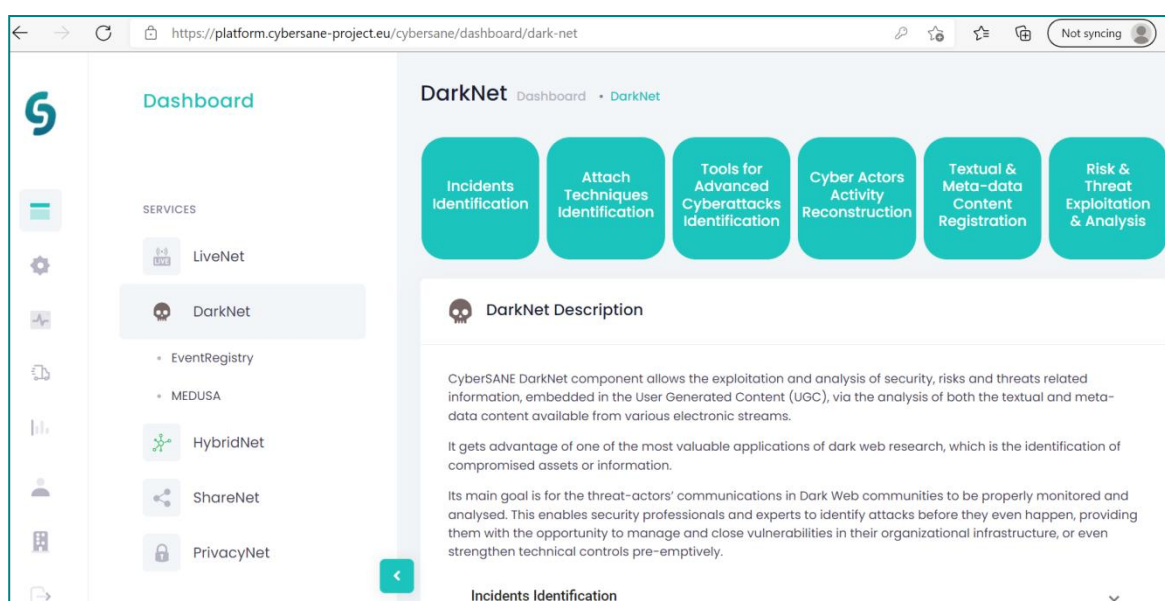


Figure 122: CyberSANE DarkNet service.

## **8.2.1 DarkNet Operations**

### **8.2.1.1 Incidents Identification**

To grasp and properly analyse the big picture of global malware and cybersecurity activities, DarkNet component is used for searching the Dark Web and its sources of information, discussions and rumours about concrete cyber-attacks.

### **8.2.1.2 Attach Techniques Identification**

Based on the results of the search for incidents, it also searches and identifies the attack techniques that are related to the identified cyber-attacks, or even new cyber-attack techniques.

### **8.2.1.3 Tools for Advanced Cyberattacks Identification**

It is used for the proper identification of tools, or traces of tools, concerning the previously identified cyber-attacks.

### **8.2.1.4 Cyber Actors Activity Reconstruction**

It is utilized for reconstructing the social graphs and user activities for specific forums, enabling security professionals and experts to perform investigation more efficiently on the various cyber incidents of their critical infrastructure and organisation.

### **8.2.1.5 Textual & Meta-data Content Registration**

DarkNet can store various data and metadata for further analysis, that could be related to classification, search for related cases, etc.

### **8.2.1.6 Risk & Threat Exploitation Analysis**

As an individual component, it can further analyse the harvested data (i.e., data aggregation, visualization, classification, etc.) to get the big picture of global malware cybersecurity activities.

## **8.2.2 DarkNet Tools**

### **8.2.2.1 EventRegistry**

The EventRegistry system (TRL=9) can monitor and aggregate knowledge that is currently spread across mainstream and social media, and to enable cross-lingual services for publishers, media monitoring and business intelligence.

It allows you to discover news content minutes after it is published and use our advanced filtering options to get only the content related to your topic of interest. It helps you keep track of the content of your interest, and monitor your company mentions in 40+ languages. It also performs analysis of media articles and blog posts.

## **How does it contribute to the overall effectiveness of CyberSANE System?**



The tool helps users to get the big picture of global cybercrime/cybersecurity activities and to carry out the investigation of the identified incidents.

#### **8.2.2.1 MEDUSA**

The MEDUSA Cyber Intelligence suite (TRL=6) constitutes a sophisticated, modular, highly -configurable and -scalable Web mining and intelligence platform that benefits from Artificial Intelligence 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:

- Dark web crawling
- Data collection, curation and harmonisation
- Business intelligence and data analytics from texts

#### **How does it contribute to the overall effectiveness of CyberSANE System?**

It contributes in the DarkWeb Layer as a core component for crawling and curating texts from the dark web also feeding the ShareNet Layer to raise awareness about cyber incidents to end-users.

## 8.3 HybridNet

CyberSANE HybridNet component provides the intelligence needed to perform effective and efficient analysis of security events, on the information produced internally within the component, and on information and data derived and acquired by other CyberSANE components, and especially the LiveNet and DarkNet components.

Towards this, HybridNet analyses a large amount of data to further evaluate and correlate attack-related patterns associated with specific malicious or anomalous activities in the underlined CII.

It provides the following operations:

- Anomalies & Incidents Registration
- Anomalies Detection
- Attack & Behaviour Simulation
- Decision Making Support
- Alert & Notification Generation

HybridNet operations are supported by the following tools in the CyberSANE system:

- OLISTIC
- L-ADS
- CARMEN

Figure 123 shows the HybridNet component of CyberSANE, described in the following sections.

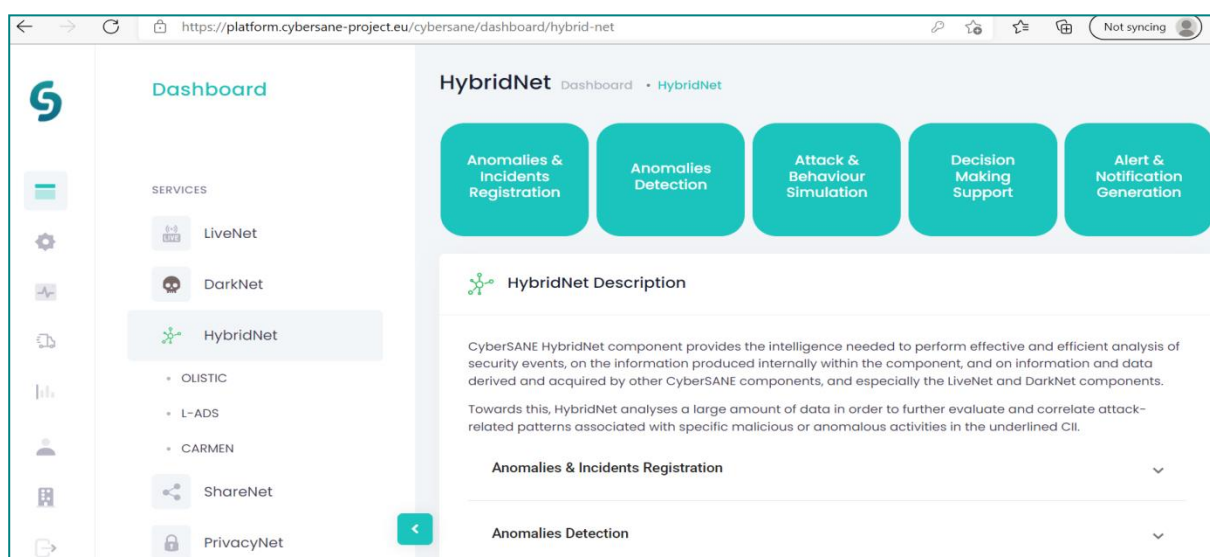


Figure 123: The CyberSANE HybridNet service.

### **8.3.1 HybridNet Operations**

#### **8.3.1.1 Anomalies & Incidents Registration**

HybridNet enables the creation and maintenance of the knowledge base of known anomalies and security incidents.

#### **8.3.1.2 Anomalies Detection**

HybridNet allows the identification of unusual activities that match the structural patterns of possible intrusions. This is succeeded utilizing machine learning techniques and technologies.

#### **8.3.1.3 Attack & Behaviour Simulation**

It provides an attack and behaviour simulation tool enabling the testing of the impact of an attack on their system by a) modelling the cyber-attacks and threats paths and patterns, and b) allowing the reconstruction of reliable and valid chains of evidence associated with real security events and incidents already identified and registered on the platform.

#### **8.3.1.4 Decision Making Support**

All data generated (either from the HybridNet individually and the other CyberSANE components) is used to enable security professionals and experts: a) to understand the impact of an attack in their systems, and b) to reach the proper decisions in regards with the security aspects of their CIIIs.

#### **8.3.1.5 Alert & Notification Generation**

HybridNet enables the generation and provision of near real-time notifications regarding real and/or potential vulnerabilities related to the assets of the CIIIs.

### **8.3.2 HybridNet Tools**

#### **8.3.2.1 OLISTIC**

OLISTIC (TRL=9) is a web-based software solution designed to enable organisations to achieve all the benefits possible from an enterprise risk management process. It has a friendly and intuitive user interface and supports multiple risk management domains. Its rich risk scenario library, available out of the box, enables it to be easily configured by business process owners. This offers significant time savings and reduces total cost of ownership over bespoke and toolkit-based solutions.

- Risk Assessment
- Individual Asset Risk
- Propagating Risk and Cumulative Risk

#### **How does it contribute to the overall effectiveness of CyberSANE System?**

It is used to perform the risk assessment in the CyberSANE Platform also assisting in the simulation of several cyber-attack scenarios.

### 8.3.2.2 L-ADS

The L-ADS (TRL=5) 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. Detection and notification of anomalies in communications based cyberthreats

#### How does it contribute to the overall effectiveness of CyberSANE System?

It can detect attacks that can access or modify information in the CIs.

### 8.3.2.3 CARMEN

CARMEN, Centre of Log Analysis and Mining of Events (TRL=9), is a tool developed by the National Cryptologic Centre and the company S2Grupo to identify compromises by advanced persistent threats (APTs), and is the first tool based on Spanish technology and know-how. The product focuses on anomaly detection in network traffic. Different modules oversee detecting indications of lateral movement or data exfiltration:

- Misuse detection
- Statistical anomaly detection
- Time series anomaly detection
- Host anomalies
- Lateral movement

#### How does it contribute to the overall effectiveness of CyberSANE System?

It is potentially one of the multiple anomaly detection tools to be used within the HybridNet.

## 8.4 ShareNet

CyberSANE ShareNet component provides the necessary threat intelligence and information sharing capabilities with other involved parties (i.e., industry cooperation groups, Computer Security Incident Response Teams, etc.), allowing them to determine the trustworthiness of each information source, and identify them, as soon as the data is received.

This information is properly shared with 3rd party systems and entities outside the platform, respecting the data sharing agreements required to be properly enforced.

It provides the following operations:

- Attack Pattern Collection
- Protected Data Storage
- Data Sharing Agreements
- Knowledge Sharing

ShareNet operations are provided by the following supporting tools in the CyberSANE system:

- C3ISP
- Sharing Platform

The below figure illustrates the ShareNet component of the CyberSANE system. It is further described in the following sections.

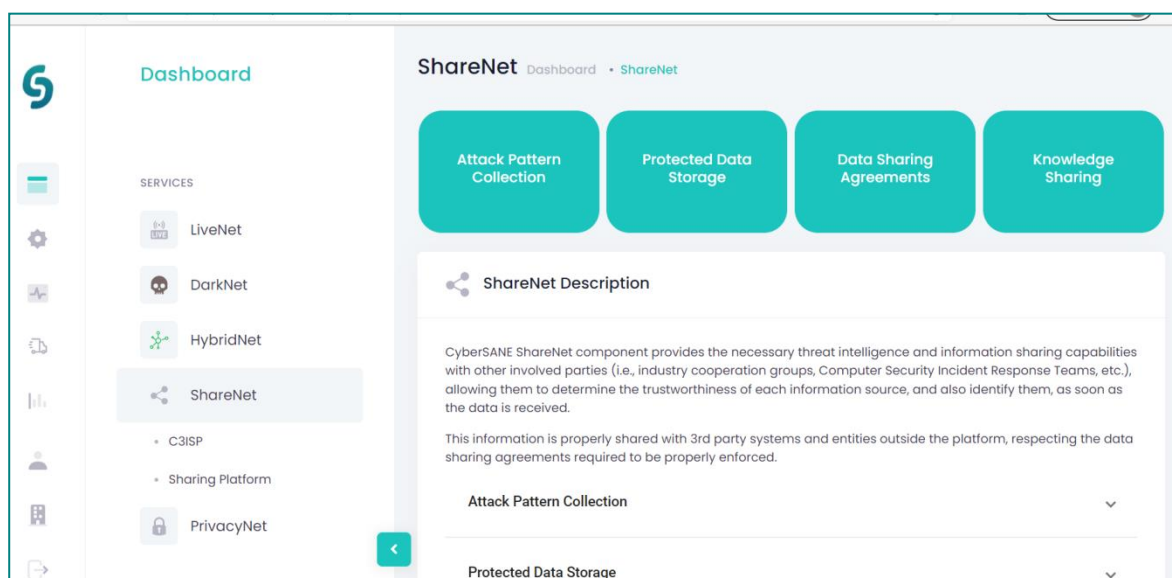


Figure 124: The CyberSANE ShareNet service.

### **8.4.1 ShareNet Operations**

#### **8.4.1.1 Attack Pattern Collection**

ShareNet is used as one of the main points for identifying new attack patterns from the public internet. These attack patterns can be properly registered in the CyberSANE platform through the LiveNet to be applied for real time security incident detection.

#### **8.4.1.2 Protected Data Storage**

It stores security incident data in a protected and secure way, ensuring its confidentiality and integrity at all implemented and supported CyberSANE scenarios.

#### **8.4.1.3 Data Sharing Agreements**

ShareNet allows the creation and maintenance of agreements between two or more internal and/or external to CyberSANE entities, concerning the sharing of data or information of any kind between these. This set of features and services enable the proper description, and enforcement of all the mandatory rules, terms and conditions set for and agreed upon by the involved parties.

#### **8.4.1.4 Knowledge Sharing**

ShareNet implements all required functionalities for sharing the data.

### **8.4.2 ShareNet Tools**

#### **8.4.2.1 C3ISP**

C3ISP defines a collaborative and confidential information sharing, analysis, and protection framework as a service for cyber security management. Its innovation is the possibility to share information in a flexible and controllable manner inside a collaborative multi-domain environment to improve detection of cyber threats and response capabilities, still preserving the confidentiality of the shared information.

The tool supports the whole CyberSANE platform with necessary threat intelligence and information sharing capabilities, enabling entities to collect attack patterns, store information securely, sharing information according to security policies defined through human-readable data-sharing agreements.

#### **How does it contribute to the overall effectiveness of CyberSANE System?**

The tool provides timely sharing of threat information, thus allowing the whole CyberSANE platform analyze information faster

#### **8.4.2.2 Sharing Platform**

Sharing Platform is based in the cooperation of Greek National CERT, Cyber Defence Directorate of Ministry of Defence, Greek Research and Technology Network and FORTH CERT. It provides cybersecurity related information exchange, integration with MeliCERTes CSP platform and proposes cybersecurity solutions that allow ICT enabled organisation and enterprises to focus on their real products and services that they offer to citizens.

FORTH's Sharing Platform is based in the cooperation of Greek National CERT, Cyber Defence Directorate of Ministry of Defence, Greek Research and Technology Network and FORTH CERT. It provides cybersecurity related information exchange and an indirect integration with MeliCERTes platform.

### **How does it contribute to the overall effectiveness of CyberSANE System?**

All the security information, threat intelligence, IoC, APT analysis and more could be propagated to a larger cooperative network to increase the overall preparedness of EU.

## 8.5 PrivacyNet

CyberSANE PrivacyNet component is responsible for managing and orchestrating the application, regarding the required privacy mechanisms, maximizing achievable levels of confidentiality and data protection. It sets up the security and data privacy policies, allowing security professionals and experts to specify all the protection rules and terms that must be performed, and the required conditions to execute them.

This component is in very close interoperation with ShareNet, covering a wide range of techniques and mechanisms, including homomorphic cryptography, attribute-based and searchable encryption, anonymization, location privacy, multi-party, and verifiable computation, to meet highly demanding regulatory compliance obligations.

It provides the following operations:

- PII Detection
- Privacy Policy Enforcement
- Homomorphic Cryptography
- Format Preserving Attribute Based Encryption
- Incident Data Redaction

PrivacyNet operations are supported by the following tool in the CyberSANE system:

- CHIMERA

The next figure depicts the PrivacyNet component in the CyberSANE system. Further information is provided in the next sections.

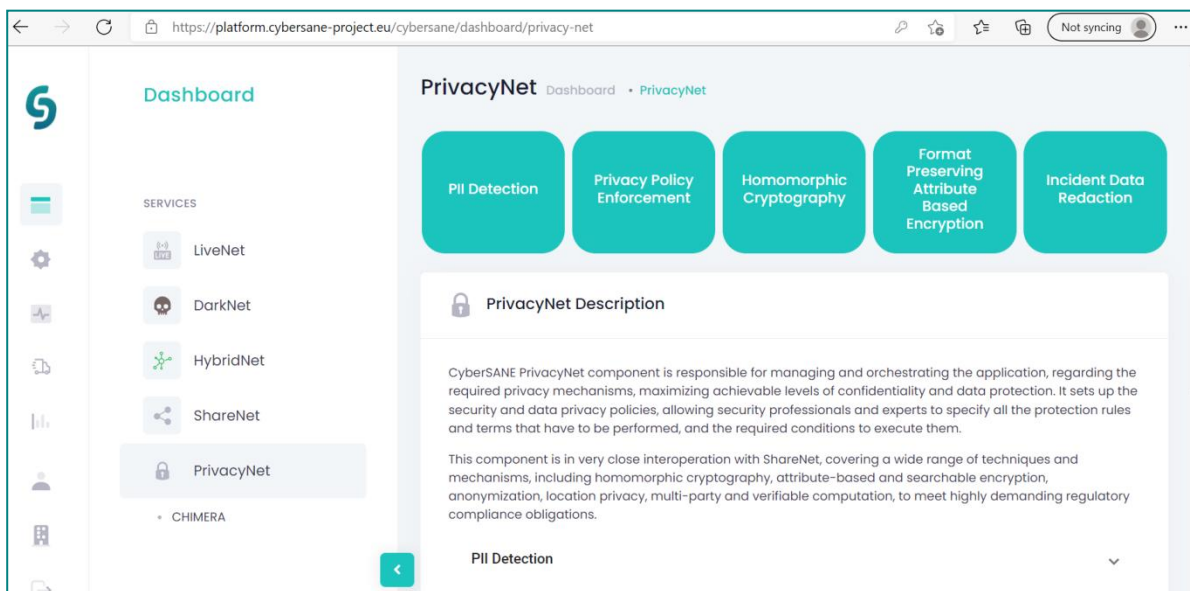


Figure 125: The CyberSANE PrivacyNet service.

### 8.5.1 PrivacyNet Operations

#### 8.5.1.1 PII Detection

PrivacyNet implements specific mechanisms for detecting personally identifiable data and information within the CyberSANE platform. This is achieved using a combination of



predefined rules for matching typical PII patterns with fuzzy detection attempts, through ML models.

#### **8.5.1.2 Privacy Policy Enforcement**

One of the most critical sets of features and services are related to the Privacy Policy enforcement process. Policies in CyberSANE are statements or documents that disclose some or all the methods, a party gathers, uses, discloses, and manages data. In this regard, CyberSANE provides the proper framework to support this declarative way required to define such usages and information owners, as well as semi-automatic conversion of said rules to a privacy engine, responsible for enforcing them.

#### **8.5.1.3 Homomorphic Cryptography**

PrivacyNet implements encryption schemes for allowing mathematical function to be executed directly on encrypted data, that yield the same results as if the function was executed on plain text.

#### **8.5.1.4 Format Preserving Attribute Based Encryption**

It allows for the output format of encryption to be the same as the input format, utilizing attribute-based encryption techniques and performing of encryption on partial data only.

#### **8.5.1.5 Incident Data Redaction**

Incident data redaction techniques allow the removal of personal identifiable data in security incident data while keeping the redacted data useful for security professionals and experts.

### **8.5.2 PrivacyNet Tool**

#### **8.5.2.1 CHIMERA**

CHIMERA (TRL=8) prevents unintended access to sensitive data and ensure compliance with evolving data protection regulations, while facilitating data sharing between organisations.

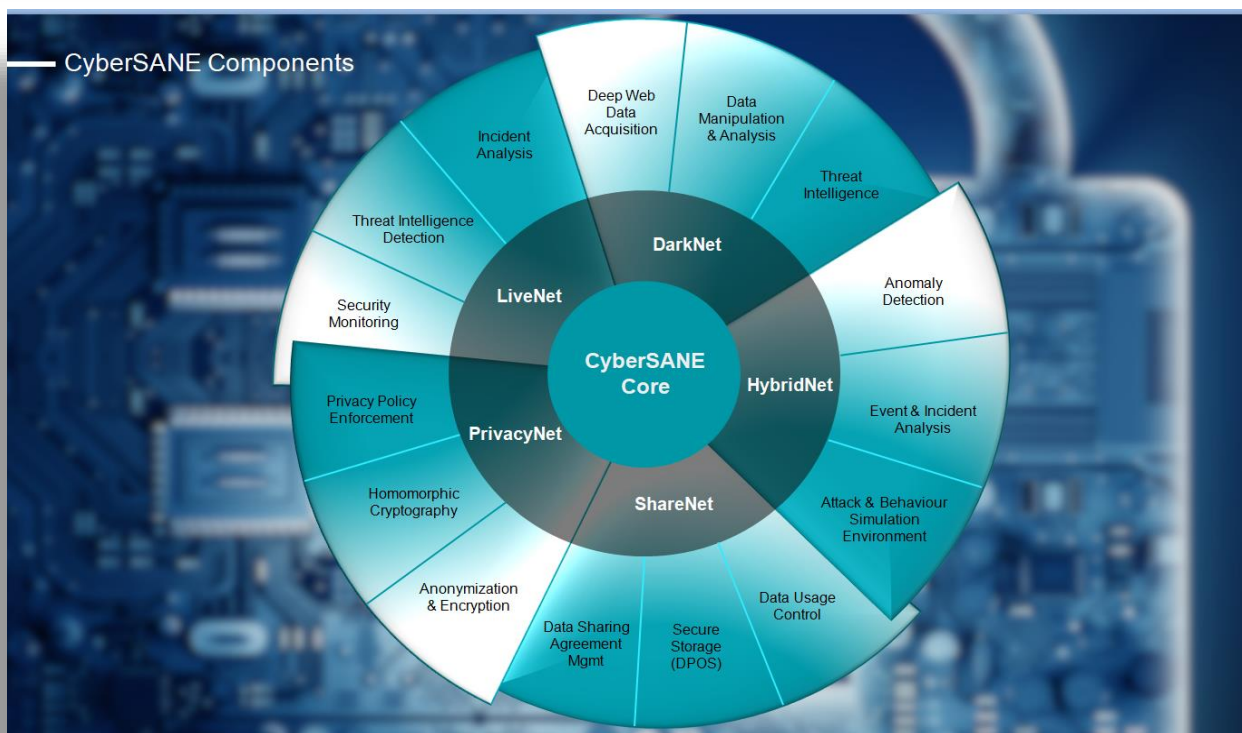
Chimera is a dataflow application, integrated in a Web User Interface that can communicate with the Orchestration-Frameworks APIs allowing a user to manipulate knowledge and data generated by other tools. It can safeguard access to data through anonymization. Using an algorithm which make it very difficult to decode in a timely manner (less than a few million years).

The data is collected, processed, transformed, and filtered in order to discard what is not relevant. It can support auto detection of personal data through scanning of existing files (e.g. documents, pdf, spreadsheets, txt, etc.) but in the case of the CyberSANE platform it will be instructed to do so according to a configuration in PrivacyNet service.

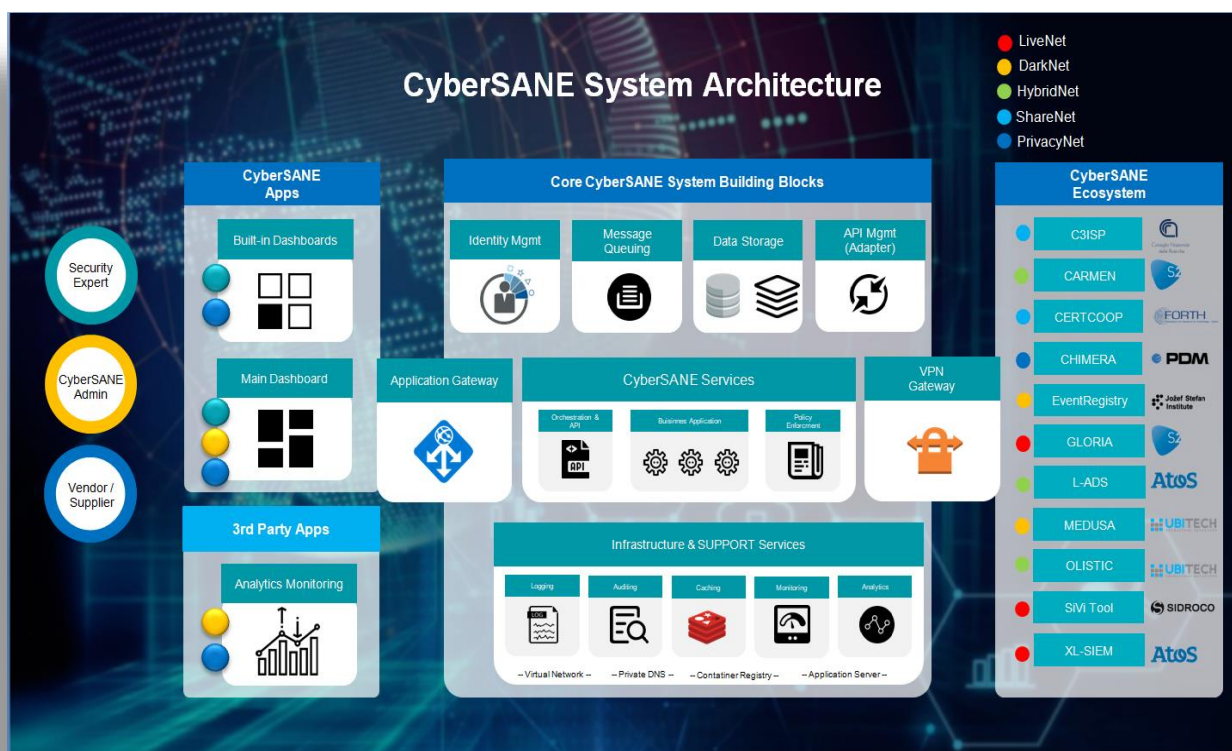
#### **How does it contribute to the overall effectiveness of CyberSANE System?**

Chimera is the main tool behind the PrivacyNet component, focusing on providing the anonymization services to scrub clean, network traffic, logs, incident data and user data.

## **Annex III. CyberSANE System Architecture**



## D9.2 – Training Materials and Report on Training Processes





\*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833663.\*



# CYBERSANE

## H2020 Project : WP2

Contacts:

Thanos Karantjias (Maggioli) – [thanos.Karantjias@maggioli.it](mailto:thanos.Karantjias@maggioli.it)

4

Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures