

D6.8

Rules & Tools for Operators' Coordination and Reporting to CERTs in Case of Incidents V2

| | | | |
|----------------------------|------------|-----------------------------|------------------|
| DOCUMENT | D6.8 | WORKPACKAGE | WP6 |
| DELIVERABLE STATE | FINAL | PROGRAMME IDENTIFIER | H2020-SU-DS-2020 |
| REVISION | V1.0 | GRANT AGREEMENT ID | 101020560 |
| DELIVERY DATE | 31/03/2024 | PROJECT START DATE | 01/10/2021 |
| DISSEMINATION LEVEL | PU | DURATION | 3 YEARS |

© Copyright by the CyberSEAS Consortium

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101020560



DISCLAIMER

This document does not represent the opinion of the European Commission, and the European Commission is not responsible for any use that might be made of its content.

This document may contain material, which is the copyright of certain CyberSEAS consortium parties, and may not be reproduced or copied without permission. All CyberSEAS consortium parties have agreed to full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the CyberSEAS consortium as a whole, nor a certain party of the CyberSEAS consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and does not accept any liability for loss or damage suffered using this information.

ACKNOWLEDGEMENT

This document is a deliverable of CyberSEAS project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101020560.

The opinions expressed in this document reflect only the author's view and in no way reflect the European Commission's opinions. The European Commission is not responsible for any use that may be made of the information it contains.

| | |
|-------------------------------------|--|
| PROJECT ACRONYM | CyberSEAS |
| PROJECT TITLE | Cyber Securing Energy dAta Services |
| CALL ID | H2020-SU-DS-2020 |
| CALL NAME | Digital Security (H2020-SU-DS-2018-2019-2020) |
| TOPIC | SU-DS04-2018-2020 Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches |
| TYPE OF ACTION | Innovation Action |
| COORDINATOR | ENGINEERING – INGEGNERIA INFORMATICA SPA (ENG) |
| PRINCIPAL CONTRACTORS | CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (CINI), AIRBUS CYBERSECURITY GMBH (ACS), FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (FRAUNHOFER), GUARDTIME OU (GT), IKERLAN S. COOP (IKE), INFORMATIKA INFORMACIJSKE STORITVE IN INZENIRING DD (INF), INSTITUT ZA KORPORATIVNE VARNOSTNE STUDIJE LJUBLJANA (ICS), RHEINISCH-WESTFAELISCHE TECHNISCHE HOCHSCHULE AACHEN (RWTH), SOFTWARE IMAGINATION & VISION SRL (SIMAVI), SOFTWARE QUALITY SYSTEMS SA (SQS), STAM SRL (STAM), SYNELIXIS LYSEIS PLIROFORIKIS AUTOMATISMOU & TILEPIKOINONION ANONIMI ETAIRIA (SYN), WINGS ICT SOLUTIONS INFORMATION & COMMUNICATION TECHNOLOGIES IKE (WIN), ZIV APLICACIONES Y TECNOLOGIA SL (ZIV), COMUNE DI BERCHIDDA (BER), COMUNE DI BENETUTTI (BEN), ELES DOO SISTEMSKI OPERATER PRENOSNEGA ELEKTROENERGETSKEGA OMREZJA (ELES), PETROL SLOVENSKA ENERGETSKA DRUZBA DD LJUBLJANA (PET), AKADEMSKA RAZISKOVALNA MREZA SLOVENIJE (ARN), HRVATSKI OPERATOR PRIJENOSNOG SUSTAVA DOO (HOPS), ENERIM OY (ENERIM), ELEKTRILEVI OU (ELV), COMPANIA NATIONALA DE TRANSPORT ALENERGIEI ELECTRICE TRANSELECTRICA SA (TEL), CENTRUL ROMAN AL ENERIEI (CRE), TIMELEX (TLX). |
| WORKPACKAGE | WP6 |
| DELIVERABLE TYPE | OTHER |
| DISSEMINATION LEVEL | PU Public |
| DELIVERABLE STATE | FINAL |
| CONTRACTUAL DATE OF DELIVERY | 31/03/2024 |
| ACTUAL DATE OF DELIVERY | 25/07/2024 |
| DOCUMENT TITLE | Rules & Tools for Operators' Coordination and Reporting to CERTs in Case of Incidents V2 |
| AUTHOR(S) | ACS, CINI, CRE, EC, ELV, ENERIM, FRAUNHOFER, GT, HOPS, ICS, INF, OPR, PETROL, SI-CERT/ARN, SQS, STAM, SYN, TEL, WIN |

REVIEWER(S) BEN, PET, GT (SAB)

ABSTRACT SEE EXECUTIVE SUMMARY

HISTORY SEE DOCUMENT HISTORY

KEYWORDS Cybersecurity, Incident Response, Incident Response Frameworks, Incident Assessment and Reporting, Process Modelling and Management, Multiple Criteria Decision-Making, Collaborative Work, SOCs, CERTs, EPES Protection Solutions, Software Development

Document History

| Version | Date | Contributor(s) | Description |
|----------------|-------------|--|---|
| V0.1 | 15/03/2024 | INF | First draft |
| V0.2 | 07/05/2024 | ACS, EC/ELV, ENERIM, FRAUNHOFER, INF, SI- CERT/ARN | Content provided by all contributors |
| V0.3 | 16/07/2024 | INF | Complete draft – all document sections finalized, contributed content merged and edited, missing content provided, references added and edited, figures and tables edited, document formatted |
| V1.0 | 25/07/2024 | GT, ICS, INF, PET, STAM | The final document – corrections based on reviewers' comments |

Table of Changes in Version 2

| Section | Contributor | Change description and motivation |
|----------------|--|--|
| 1 | INF | The introduction has been updated |
| 5 | FRAUNHOFER, EC/ELV, ENERIM, INF, SI-CERT/ARN | A new section has been added to propose unified procedures, tools, and rules for the coordination and reporting to CERTs in the common EU space aligned with the national specifics described in Section 4 |
| 6 | INF | Former Section 5 has been renumbered to Section 6 |
| 7 | ACS, FRAUNHOFER, INF, SI-CERT/ARN | A new section has been added to describe the implementation and validation of the toolset and the introduced standardized coordination and reporting procedures |
| 8 | INF | The concluding section has been updated and renumbered to Section 8 |

Table of Contents

- Document History5
- Table of Changes in Version 2.....6
- Table of Contents7
- List of Figures.....9
- List of Tables..... 13
- List of Acronyms and Abbreviations 15
- Executive summary (updated).....21
- 1 Introduction (updated)22
 - 1.1 Intended audience24
 - 1.2 Relations to other activities.....24
 - 1.3 Document overview.....25
- 2 Underlying methods, standards, and frameworks.....26
 - 2.1 Overview of common incident response frameworks26
 - 2.2 Overview of CTI exchange standards34
 - 2.3 Reporting mechanisms37
 - 2.4 MCDM assessment methods.....43
 - 2.5 Group collaboration and coordination procedures.....46
 - 2.6 Incident response modeling.....49
- 3 Methodology53
 - 3.1 Overview of the applied methodology53
 - 3.2 Incident response policy.....59
 - 3.3 Incident response plan60
 - 3.4 MCDM model for impact assessment.....61
 - 3.5 Common CACAO vocabulary for BPMN modeling.....65
- 4 Incident response procedures and rules66
 - 4.1 Italian pilot scenarios.....66
 - 4.2 Slovenian and Croatian pilot scenarios.....71
 - 4.3 Romanian pilot scenarios97
 - 4.4 Finnish pilot scenarios101
 - 4.5 Estonian pilot scenarios.....110
- 5 Common procedures and rules (new)117



- 5.1 Comparative overview of rules and tools..... 117
- 5.2 Unification patterns and rules for the common EU space..... 123
- 5.3 Recommendations for standardized reporting and coordination with CERTs 127
- 5.4 Standardized response and playbook management for the common EU space .129
- 6 Toolset design and implementation..... 137
 - 6.1 Specification of functional and non-functional requirements..... 137
 - 6.2 Components, modules, and tools..... 145
 - 6.3 Data structures 149
 - 6.4 Architecture..... 150
 - 6.5 Playbook management integration 160
 - 6.6 Decision support tool..... 164
- 7 Implementation and verification of rules and tools (new)..... 169
 - 7.1 Infrastructure setup..... 169
 - 7.2 MISP reporting and CTI sharing scenarios 174
 - 7.3 Playbook sharing and reporting scenarios..... 187
 - 7.4 Summary of implemented rules and tools 193
- 8 Conclusions (updated)..... 195
- 9 References 197

List of Figures

| | |
|--|----|
| Figure 1 – D6.7 and D6.8 outcomes according to the T6.4 project plan. | 23 |
| Figure 2 – Dependencies to other WPs and tasks..... | 24 |
| Figure 3 – NIST IR lifecycle..... | 27 |
| Figure 4 – NIST OT DFIR phases..... | 29 |
| Figure 5 – SANS IR cycle..... | 30 |
| Figure 6 – ISO 27035 IR phases. | 32 |
| Figure 7 – TAXII – the logical structure of an API Root..... | 35 |
| Figure 8 – Sample dashboard showing the incoming and outgoing network traffic to hosts. | 38 |
| Figure 9 – Sample dashboard showing network flows with the visualized amount of network traffic. | 38 |
| Figure 10 – Sample dashboard showing connections of a specific network..... | 38 |
| Figure 11 – Sample dashboard showing the network traffic..... | 39 |
| Figure 12 – Sample KPI dashboard showing the MTD metric. | 40 |
| Figure 13 – Sample email notification as a response to a SIEM alert..... | 41 |
| Figure 14 – Sample PDF report as a response to a SIEM alert..... | 41 |
| Figure 15 – Additive value aggregation in the CVSS impact assessment model. | 45 |
| Figure 16 – An example of a DEXi decision model..... | 45 |
| Figure 17 – Generic group consensus-seeking procedure incorporating the aggregation-disaggregation analysis..... | 47 |
| Figure 18 – Generic Delphi procedure..... | 48 |
| Figure 19 – CACAO playbook structure..... | 51 |
| Figure 20 – Incident response lifecycle..... | 54 |
| Figure 21 – Steps of the methodology to define incident response procedures and rules.... | 55 |
| Figure 22 – Mapping of security events and vulnerabilities to incident response procedures. | 56 |
| Figure 23 – Example of a standardized malware incident response procedure in the BPMN notation..... | 59 |
| Figure 24 – Incident impact assessment phase of the decision-making process..... | 62 |
| Figure 25 – Cyber security cooperation governance use case. | 73 |
| Figure 26 – Cross-border cooperation and cyber security cooperation governance use case. | 75 |
| Figure 27 – SI-CERT Incident-handling flowchart..... | 77 |

| | |
|--|-----|
| Figure 28 – General incident response procedure for Informatika SOC. | 89 |
| Figure 29 – Ransomware incident response procedure. | 93 |
| Figure 30 – Phishing incident response procedure. | 94 |
| Figure 31 – ROM incident reporting form. | 101 |
| Figure 32 – FIN incident reporting form – basic information. | 109 |
| Figure 33 – FIN incident reporting form – information on the incident. | 109 |
| Figure 34 – JSON definition of the MISP NOKI object. | 127 |
| Figure 35 – Selection of the MISP NOKI object. | 128 |
| Figure 36 – MISP NOKI object. | 128 |
| Figure 37 – Conceptual framework for the incident handling flow. | 132 |
| Figure 38 – Common playbook repository in the SAPPAN playbook management tool. | 134 |
| Figure 39 – Metering service data breach playbook. | 135 |
| Figure 40 – Substation defense playbook. | 135 |
| Figure 41 – General use case. | 137 |
| Figure 42 – Components and modules of the toolset. | 145 |
| Figure 43 – T4.4 and T6.4 toolset integration. | 146 |
| Figure 44 – Architectural view of the playbook management system. | 149 |
| Figure 45 – Flowchart of the system. | 151 |
| Figure 46 – Definition of event correlations. | 151 |
| Figure 47 – Artifacts, data types, and IoCs in TheHive. | 152 |
| Figure 48 – List of artifacts and their corresponding datatypes. | 154 |
| Figure 49 – MITRE ATT&CK taxonomy provided to an alarm or a case (based on an IoC or a SIEM event). | 154 |
| Figure 50 – Integration with MISP from TheHive. | 156 |
| Figure 51 – Propagation of sharing a specific artifact or IoC. | 157 |
| Figure 52 – Sharing of a MISP case or event with connected companies or communities. | 157 |
| Figure 53 – MISP authentication. | 158 |
| Figure 54 – Connection of two MISP instances. | 158 |
| Figure 55 – Connection to SIEM. | 158 |
| Figure 56 – Cortex job. | 159 |
| Figure 57 – Cortex Responder. | 159 |
| Figure 58 – Cortex Analyzer report. | 159 |
| Figure 59 – Use of TheHive/Cortex data types. | 160 |
| Figure 60 – Creating a playbook step in the SAPPAN capturing tool. | 161 |

| | |
|--|-----|
| Figure 61 – Information/editing view of a created playbook step in the SAPPAN capturing tool..... | 161 |
| Figure 62 – Selecting and defining the confidentiality level of a playbook for exporting into JSON in the SAPPAN capturing tool..... | 162 |
| Figure 63 – High-level JSON export of a CACAO playbook in the SAPPAN capturing tool.. | 162 |
| Figure 64 – Details of JSON export of a CACAO playbook steps in the SAPPAN capturing tool. | 163 |
| Figure 65 – BPMN representation of a sample CACAO playbook in the SAPPAN capturing tool..... | 163 |
| Figure 66 – Asset identification form. | 165 |
| Figure 67 – Incident identification form..... | 166 |
| Figure 68 – Partially filled in incident impact assessment matrix. | 167 |
| Figure 69 – Completed incident impact assessment matrix. | 167 |
| Figure 70 – INF virtual pilot infrastructure for the CTI exchange scenario..... | 169 |
| Figure 71 – SI-CERT MISP infrastructure for the CTI exchange scenario..... | 170 |
| Figure 72 – Importing playbooks from a connected Kafka instance..... | 171 |
| Figure 73 – Playbook sharing as an event via MISP (top), and more relevant metadata attached (bottom)..... | 172 |
| Figure 74 – The overview page for an active playbook execution with the command prompt. | 173 |
| Figure 75 – The visual overview page to display the current stage of an active playbook execution..... | 173 |
| Figure 76 – CyberRange incident response environment. | 174 |
| Figure 77 – Malware blocking on the firewall based on CTI exchange in the community. . | 176 |
| Figure 78 – Generation of the authentication key for API calls to the MISP server. | 177 |
| Figure 79 – Definition of the MISP block table in the pfSense firewall. | 179 |
| Figure 80 – Creation of the pfSense firewall blocking rule..... | 180 |
| Figure 81 – Definition of the pfSense firewall blocking rule..... | 180 |
| Figure 82 – Published and shared network activity events in MISP..... | 181 |
| Figure 83 – Table of blocked IPs on the firewall..... | 181 |
| Figure 84 – System logs of firewall traffic blocking..... | 182 |
| Figure 85 – Resolving an IP address in MISP. | 182 |
| Figure 86 – Unblocking of an IP address on the firewall..... | 182 |
| Figure 87 – Unblocked IP address on the firewall..... | 183 |
| Figure 88 – Compilation of the malware dropper program..... | 184 |

| | |
|---|-----|
| Figure 89 – Security analysis of the malware dropper executable with VirusTotal..... | 184 |
| Figure 90 – Basic properties and hashes of the malware dropper executable. | 185 |
| Figure 91 – Creation of a malicious file..... | 185 |
| Figure 92 – The blocked malicious file generated by the malware dropper executable. ... | 185 |
| Figure 93 – A new MISP event published by the INF SOC..... | 186 |
| Figure 94 – IoC (SHA-256 hash) in the published MISP event..... | 186 |
| Figure 95 – Definition of a new MISP event addressing the malware dropper..... | 186 |
| Figure 96 – NOKI object for the standardized reporting of the malware dropper event. | 187 |
| Figure 97 – A command that invokes the NOKI Cortex Responder..... | 188 |
| Figure 98 – Conceptual approach for cyber security playbook management and sharing. | 189 |
| Figure 99 – Sharing the initial internal INF SOC playbook with the national CERT..... | 189 |
| Figure 100 – Modification and generalization of the playbook by the national CERT..... | 189 |
| Figure 101 – Resharing the generalized and sanitized playbook with the EPES community. | 190 |
| Figure 102 – Generalized playbook in the MISP repository..... | 190 |
| Figure 103 – UUID of a phishing IoC referencing a playbook for the standardized phishing IR. | 191 |
| Figure 104 – Adding of the NOKI object..... | 191 |
| Figure 105 – Added NOKI object (INF SOC)..... | 192 |
| Figure 106 – Received NOKI object (SI-CERT)..... | 192 |
| Figure 107 – Playbook execution scenario. | 193 |

List of Tables

| | |
|--|-----|
| Table 1 – Assessment of the functional impact for the coordination with CERTs..... | 56 |
| Table 2 – Assessment of the informational impact for the coordination with CERTs. | 57 |
| Table 3 – Types of incident response actions. | 58 |
| Table 4 – Incident impact assessment criteria..... | 63 |
| Table 5 – Incident impact scoring system..... | 64 |
| Table 6 – Exemplary mapping of assessed impact ratings to Slovenian national impact levels. | 65 |
| Table 7 – Mapping between assets and security events for the ITA pilot. | 68 |
| Table 8 – Mapping of incident response procedures for the SLO-CRO use case 3..... | 74 |
| Table 9 – Incident response procedure for the security incident from detected data anomaly. | 78 |
| Table 10 – Impact mapping table. | 90 |
| Table 11 – RACI matrix for security levels and roles..... | 90 |
| Table 12 – Malware incident response procedure..... | 91 |
| Table 13 – Disgruntled employee incident response procedure..... | 95 |
| Table 14 – Mapping of FIN assets and vulnerabilities. | 104 |
| Table 15 – FIN mitigation measures..... | 105 |
| Table 16 – Mapping of EST assets to applicable mitigation measures. | 112 |
| Table 17 – Comparison of pilot countries according to underlying national regulations..... | 117 |
| Table 18 – Comparison of pilot countries according to the required coordination with CERTs. | 118 |
| Table 19 – Comparison of pilot countries according to incident response procedures and rules..... | 119 |
| Table 20 – Comparison of pilot countries according to data structures, formats, and tools for reports. | 120 |
| Table 21 – Comparison of pilot countries according to the communication strategy and information-sharing mechanisms. | 122 |
| Table 22 – Common rules and tools for operators' coordination and reporting. | 125 |
| Table 23 – Alignment with legislative frameworks..... | 125 |
| Table 24 – Conceptual requirements on playbook utilization and playbook-assisted incident handling in cybersecurity. | 130 |
| Table 25 – List of shared standardized incident response playbooks. | 136 |
| Table 26 – Functional requirements on Playbook management (SAPPAN). | 138 |
| Table 27 – Functional requirements on Playbook selection (from the SAPPAN repository).. | 139 |

| | |
|---|-----|
| Table 28 – Functional requirements on Playbook execution. | 139 |
| Table 29 – Functional requirements on SIEM integration and analysis..... | 139 |
| Table 30 – Functional requirements on MISP integration and CTI exchange..... | 140 |
| Table 31 – Functional requirements on Reporting facilities. | 140 |
| Table 32 – Functional requirements on Incident impact assessment. | 141 |
| Table 33 – Functional requirements on Collaboration and work coordination facilities (for decision-making)..... | 142 |
| Table 34 – Functional requirements on Collaboration and work coordination facilities (for incident handling)..... | 144 |
| Table 35 – Non-functional requirements. | 145 |
| Table 36 – Summary of proposed and implemented procedures, rules, and tools..... | 193 |

List of Acronyms and Abbreviations

| | |
|--------|---|
| AD | Active Directory |
| AI | Artificial Intelligence |
| API | Application Programming Interface |
| APT | Advanced Persistent Threats |
| ATT&CK | Adversarial Tactics, Techniques, and Common Knowledge |
| ATP | Advanced Threat Protection |
| AV | Audio Visual |
| BI | Business Intelligence |
| BPM | Business Process Management |
| BPMN | Business Process Model and Notation |
| BSP | Balancing Service Provider |
| C2 | Command and Control |
| CA | Certificate Authority |
| CACAO | Collaborative Automated Course of Action Operations |
| CCDCOE | Cooperative Cyber Defence Centre of Excellence |
| CER | Critical Entities Resilience |
| CERT | Computer Emergency Response Team |
| CI/CD | Continuous Integration/Continuous Delivery |
| CIM | Common Information Model |
| CIO | Chief Information Officer |
| CIRCL | Computer Incident and Response Center Luxembourg |
| CIRT | Computer Incident Response Team |
| CISA | Cybersecurity & Infrastructure Security Agency |
| CISO | Chief Information Security Officer |
| CMC | Computer-Mediated Communication |
| CMMI | Capability Maturity Model Integration |
| COBIT | Control Objectives for Information and Related Technologies |

| | |
|-------|--|
| CPE | Common Platform Enumeration |
| CRM | Customer Relationship Management |
| CSF | Cybersecurity Framework |
| CSIRT | Computer Security Incident Response Team |
| CSRF | Cross-Site Request Forgery |
| CSV | Comma Separated Values |
| CTI | Cyber Threat Intelligence |
| CVD | Coordinated Vulnerability Disclosure |
| CVE | Common Vulnerabilities and Exposures |
| CVSS | Common Vulnerability Scoring System |
| DAG | Directed Acyclic Graph |
| DB | Database |
| DCU | Data Concentrator Unit |
| DDoS | Distributed Denial of Service |
| DEXi | DEcision eXpert |
| DFIR | Digital Forensics and Incident Response |
| DIS | Dipartimento delle Informazioni per la Sicurezza |
| DLP | Data Loss Prevention |
| DM | Decision-Maker |
| DNS | Domain Name System |
| DNSC | Directoratul National de Securitate Cibernetica |
| DoS | Denial of Service |
| DPO | Data Protection Officer |
| DSO | Distribution System Operator |
| DSP | Digital Service Provider |
| DSS | Decision Support System |
| EDR | Endpoint Detection and Response |
| ENISA | European Union Agency for Cybersecurity |

| | |
|---------|---|
| ENTSO-E | European Network of Transmission System Operators for Electricity |
| EPES | Electrical Power and Energy System |
| EPS | Events per Second |
| EU | European Union |
| FCR | Facility Control Room |
| FTP | File Transfer Protocol |
| GDPR | General Data Protection Regulation |
| GNU | GNU's not Unix! |
| GUI | Graphical User Interface |
| HTML | HyperText Markup Language |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| HVK | Huoltovarmuuskeskus (Finnish National Emergency Supply Agency) |
| IAM | Identity Access Management |
| IDS | Intrusion Detection System |
| IEC | International Electrotechnical Commission |
| IoA | Indicator of Attack |
| IoC | Indicator of Compromise |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| IR | Incident Response |
| ISA | Information Security Act |
| ISACA | Information Systems Audit and Control Association |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| JSON | JavaScript Object Notation |
| KPI | Key Performance Indicator |
| LDAP | Lightweight Directory Access Protocol |

| | |
|---------|--|
| LIRI | Level Impact Reduction Index |
| LUW | Linux, UNIX and Windows |
| LV | Low Voltage |
| MAUT | Multi-Attribute Utility Theory |
| MCDM | Multi-Criteria Decision Making |
| MISP | Malware Information Sharing Platform |
| MS | Microsoft |
| MTD | Mean Time to Detection |
| MV | Medium Voltage |
| NAS | Network Attached Storage |
| NCC | Network Code on Cybersecurity |
| NCSC-FI | National Cyber Security Centre Finland |
| NESCOR | National Electric Sector Cybersecurity Organization Resource |
| NGFW | Next Generation Firewall |
| NIS | Network and Information Security |
| NIST | National Institute of Standards and Technology |
| NOKI | National Cybersecurity Incident Response Plan (Načrt Odzivanja na Kibernetske Incidente) |
| NVD | National Vulnerability Database |
| OASIS | Organization for the Advancement of Structured Information Standards |
| OES | Operators of Essential Services |
| OpenIOC | Open Indicators of Compromise |
| OS | Operating System |
| OSINT | Open-source intelligence |
| OT | Operational Technology |
| OWA | Ordered Weighted Averaging |
| PAM | Privilege Access Management |
| PAP | Permissible Actions Protocol |
| PC | Personal Computer |

| | |
|--------|---|
| PDF | Portable Document Format |
| PGP | Pretty Good Privacy |
| PoC | Proof of Concept |
| RACI | Responsible, Accountable, Consulted, Informed |
| RDF | Resource Description Framework |
| REST | REpresentational State Transfer |
| RIA | Riigi Infosüsteemi Amet (Estonian Information System Authority) |
| SANS | SysAdmin, Audit, Network, Security (Escal Institute of Advanced Technologies) |
| SAPPAN | Sharing and Automation for Privacy Preserving Attack Neutralization |
| SCADA | Supervisory Control and Data Acquisition |
| SDOs | STIX Domain Objects |
| SFTP | SSH File Transfer Protocol |
| SIEM | Security Information and Event Management |
| SLA | Service Level Agreement |
| SMEs | Small and Medium-sized Enterprises |
| S/MIME | Secure/Multipurpose Internet Mail Extensions |
| SMW | Semantic MediaWiki |
| SOAR | Security Orchestration, Automation, and Response |
| SOC | Security Operations Center |
| SQL | Structured Query Language |
| SSO | Single Sign-On |
| STIX | Structured Threat Information eXpression |
| TAXII | Trusted Automated eXchange of Intelligence Information |
| TC | Technical Committee |
| TCP | Transmission Control Protocol |
| TLP | Traffic Light Protocol |
| TOR | The Onion Router |
| TSO | Transmission System Operator |

| | |
|-------|---|
| TST | Technical Support Team |
| TTA | Time to Acknowledge |
| TTC | Time to Contain |
| TTD | Time to Detect |
| TTQ | Time to Qualify |
| TTR | Time to Resolve |
| TTT | Time to Triage |
| TTPs | Techniques, Tactics and Procedures |
| UCF | Use Case Factory |
| URL | Uniform Resource Locator |
| UTF | Unicode Transformation Format |
| UUID | Universally Unique Identifier |
| VBA | Visual Basic for Applications |
| VCC | Virtual Cross-border Control Center |
| VPN | Virtual Private Network |
| WA | Weighted Averaging |
| WP | Work Package |
| XML | eXtensible Markup Language |
| ZInfV | Information Security Act (Zakon o Informacijski Varnosti) |
| ZVOP | Personal Data Protection Act (Zakon o Varstvu Osebnih Podatkov) |

Executive summary (updated)

This deliverable introduces a playbook for collaborative activities among SOCs and CERTs in the electricity sector. National incident response procedures are defined, which consist of containment, eradication, recovery, and reporting activities, and in which the current status is shared with CERTs in order to support a coordinated response to incidents and reduce the impact of incidents on the critical infrastructure. Specified rules determine the required levels of coordination with CERTs, i.e., when and how incidents are reported to CERTs according to their classification, severity, and functional and informational impact.

The methodology provided and utilized in the D6.8 deliverable results in the definition of the incident response strategy, incident response procedures, cooperation and communication strategy, information sharing mechanisms, formats of reports for national CERTs, and tools to exchange the reports. It presents the basis for implementing a toolset for reporting to CERTs, coordination and cooperation among different stakeholders, analysis of incidents, decision-making, and the selection of appropriate incident response procedures. A fully functional toolset integrates several components: a group collaboration system, a decision support system, a process execution engine, a knowledge repository, CTI exchange mechanisms, and the capabilities of data management systems and SIEM systems.

The compiled set of rules for efficient coordination of EPES operators and reporting to CERTs is based on compromised assets and classes of cybersecurity attacks. Assets and events are mapped to incident response procedures that include containment, eradication, recovery, reporting, and coordination activities and rules. The impacts and effects of cybersecurity events are assessed to select appropriate procedures. The assessment is performed with MCDM methods by determining the scope, severity, impact, and extent of the damage caused by the incident. The mapping considers compromised assets, cybersecurity events, vulnerabilities of assets, and national pilot scenarios with their attack trees.

Incident response procedures are modeled as process diagrams by using the SAPPAN tool. The standard BPMN notation and a common vocabulary are applied. At first, procedures are defined separately for national pilots to consider the specifics of regulations in different countries. On this basis, common rules for EPES are derived. They are aligned with European legislation, focusing particularly on the NIS 2 Directive, the CER Directive, and the Network Code on Cybersecurity.

In addition to incident response procedures and rules, D6.8 also provides the design and implementation of the supporting toolset. It is built on SAPPAN, MISP, TheHive, Cortex, and DSS. It supports all levels of SOC operations: L1, L2, and L3.

Finally, the proposed rules and tools are implemented. Key scenarios are verified dealing with the malware and phishing incident response procedures. These scenarios address reporting to CERTs through the standard NOKI object, CTI exchange with the MISP platform, playbook management and sharing by utilizing MISP and SAPPAN, playbook automation, and rules for efficient coordination of stakeholders within EPES communities.

1 Introduction (updated)

Incident response is one of the fundamental processes in cybersecurity. It prescribes how to systematically overcome the consequences of cyber incidents, attacks, and breaches [1]. Its goal is to limit the impact of cybersecurity incidents, shorten the recovery time, and reduce the required costs. Incident response can be vastly optimized in several ways. Firstly, it can be facilitated by CTI (Cyber Threat Intelligence) exchange mechanisms and standards and by the use of intelligent approaches [2]. This means that the incident response process is not only limited to preparing and executing the incident response plan but is also able to identify attackers, recognize the motives and techniques of attackers, analyze incidents and their impacts, and share and utilize information about known past attacks.

Secondly, it is even more important to incorporate the perspectives of different stakeholders into the incident response procedures. This is especially true in the critical EPES infrastructure, where many assets may be interconnected and several stakeholders may be involved to provide common essential services, connect or share assets, participate in common energy supply chains, support processes based on national or cross-border cooperation, etc. Such critical infrastructures also require that, in the case of incidents, national regulations and rules are followed. In particular, incidents must be reported to CERTs based on their severity and in a prescribed way. It is the role of CERTs to collaborate with EPES operators to help them recover efficiently from incidents.

Thirdly, regulatory compliance is a crucial aspect of incident reporting. The European Parliament boosted the protection of the EU's essential infrastructure on November 22nd, 2022, giving its final approval to legislation tightening the risk assessments and reporting requirements for critical organizations in eleven sectors, including digital infrastructure and the energy sector [3]. The NIS 2 directive [4] sets stricter cybersecurity obligations for EU countries related to supervision. In particular, it increases the level of harmonization regarding security and reporting requirements. It aims to improve cooperation between EU countries, especially on large-scale incidents, under the umbrella of the EU Agency for Cybersecurity (ENISA) [5].

To deal with these issues, this deliverable aims to create a playbook for collaborative activities among SOCs and CERTs in the electricity sector, consisting of incident response procedures and current status to be shared among CERTs to support a coordinated response to incidents and their impact on the critical EPES infrastructure. Rules determine when and how incidents are reported to CERTs according to their severity and classification. These rules must adhere to EU regulations and specific national regulations followed by five CyberSEAS pilots.

In addition, the D6.8 deliverable also aims to develop appropriate tools to enable reporting, decision-making, analysis of incidents, and cooperation among different stakeholders. The outcomes of D6.8 are hence:

- a set of rules for operators' coordination and reporting to CERTs in case a cyber incident occurs (presented in Sections 3, 4, and 5); and
- a set of tools for operators' coordination and reporting to CERTs in case a cyber incident occurs (presented in Sections 6 and 7).

The initial set of outcomes was already provided as a result of the preceding deliverable D6.7 in M18 of the CyberSEAS project. D6.7 focused primarily on the specification of national rules and incident response procedures, toolset design, and the implementation of the first basic prototype that focused on a single PoC incident response procedure. It was the intermediate result of the T6.4 task after 6 months of work (from M12 to M18). We defined the unified rules for the common EU space and covered more implementation activities in the next stage of T6.4. From M18 to M30, we primarily focused on implementation and validation to provide a fully functional toolset. The second toolset version deals with a full stack of incident response procedures. It supports some functionalities omitted by the first version, particularly work coordination and collaboration facilities, reporting capabilities, decision-making for incident impact assessment, and integrations with external systems, such as MISP and the decision support system, which was developed in T4.4. The development timeline of T6.4 is presented in the project plan in Figure 1.

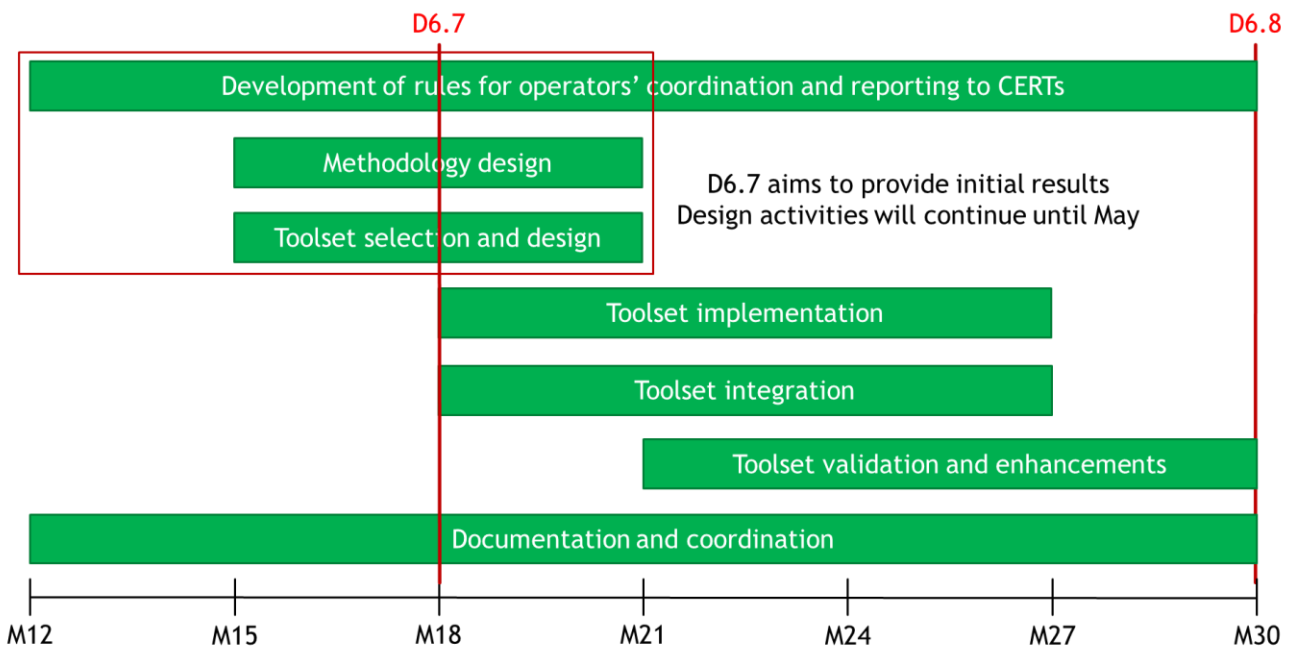


Figure 1 – D6.7 and D6.8 outcomes according to the T6.4 project plan.

The toolset facilitates L1, L2, and L3 SOC. It is built upon several tools and technologies, which include SAPPAN for playbook modeling and management, TheHive and Cortex for playbook execution, and MISP for CTI exchange and collaboration with CERTs. It also incorporates DSS for incident impact assessment and appropriate reporting mechanisms based on the NOKI object and capabilities of the MISP platform.

An important aspect of D6.8 is to set the methodological foundations for the implementation of the toolset. The theory underlying incident response procedures and collaboration rules should be introduced as well to provide the legislative framework and define the general approach to be followed to coherently specify national procedures and rules. D6.8 hence includes a brief presentation of widely accepted incident response frameworks, standards for CTI exchange, reporting technologies, business process modeling tools and notations, multi-criteria decision-making (MCDM) methods, and group collaboration technologies and techniques.

Incident response, coordination, and reporting activities that have to be carried out depend on the type and severity of the addressed incident. There are many different types of cyber incidents and attacks that are possible. To reduce the number and complexity of possible incident response procedures and rules, a properly focused approach must be introduced and followed. Such an approach is proposed and used within the scope of D6.8. As a starting point, it considers the attack scenarios of CyberSEAS pilots as well as the national rules and regulations that pertain to these pilots.

1.1 Intended audience

This document has a limited audience. It is primarily intended for H2020 CyberSEAS project partners, leaders, and coordinators working on CyberSEAS WPs and tasks.

1.2 Relations to other activities

D6.8 and T6.4 are related to many CyberSEAS WPs and tasks. All dependencies are depicted in Figure 2.

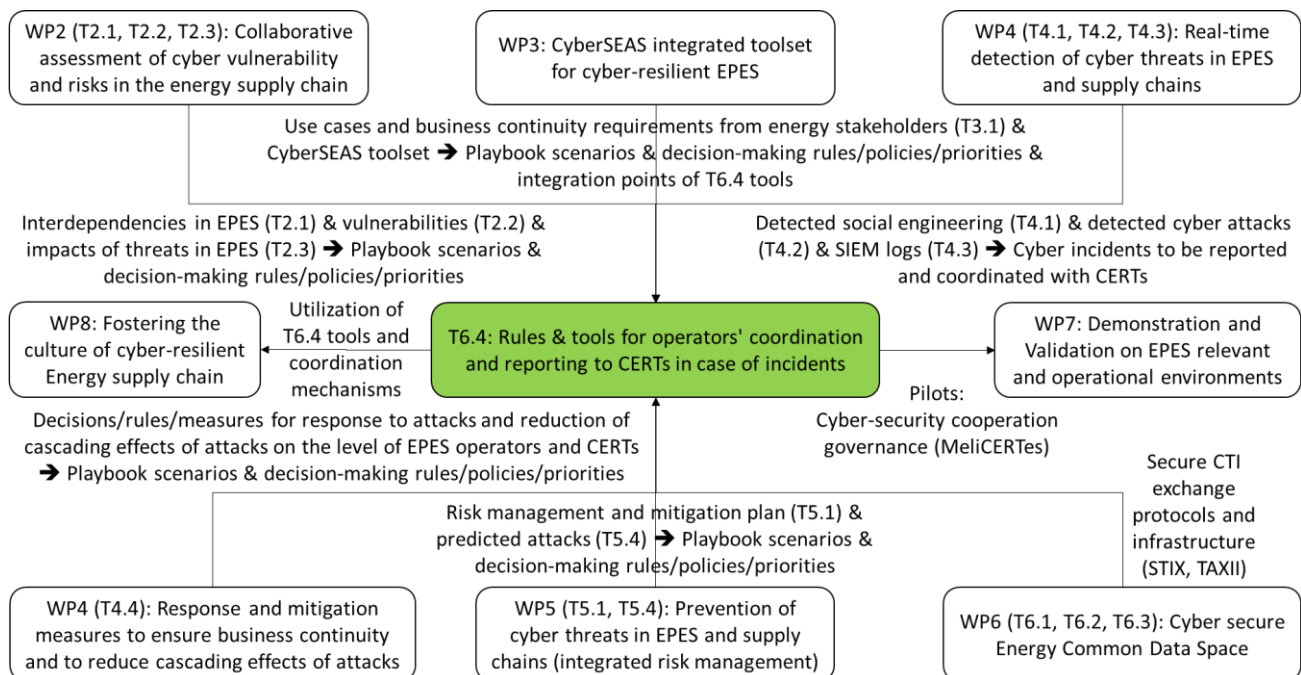


Figure 2 – Dependencies to other WPs and tasks.

The key dependencies are to:

- WP2: to base incident response procedures and rules for reporting and coordination with CERTs on common CyberSEAS vulnerabilities, risks, and dependencies related to the energy supply chain;
- WP3: to base incident response procedures and rules for reporting and coordination with CERTs on pilot attack scenarios and attack techniques that are exploited in these scenarios;

- T4.3: to obtain SIEM logs about detected cybersecurity incidents as input information for decision-making and selection of appropriate incident response procedures;
- T4.4: to share a common MCDM model for incident impact assessment as the basis to determine appropriate incident response rules/playbooks for reporting to CERTs and coordinating with them;
- T6.1: to align specific incident response procedures and rules with the defined general governance strategies, models, and plans for EPES operators and other stakeholders;
- T6.3: to define and share common CTI exchange protocols;
- WP7: to use incident response procedures and rules in the validation of specific pilot attack scenarios;
- WP8: to utilize T6.4 tools and coordination mechanisms.

1.3 Document overview

The rest of the document consists of seven sections. Section 2 is the theoretical part of D6.8, which sets the background for the design and development process by presenting the most relevant common incident response frameworks, CTI exchange standards, process modeling notations and tools, reporting mechanisms and technologies, MCDM methods, and group collaboration approaches that are underlying the definition of incident response procedures and rules, and are applied by the developed toolset to support the execution of incident response procedures. Section 3 introduces the methodology upon which we can base the definition of national incident response procedures and the toolset implementation. Section 4 presents procedures and rules defined by the pilot partners based on their attack scenarios and national legislation. These procedures and rules are facilitated by the toolset. Section 5 infers and proposes universal procedures, rules, and tools for the common EPES ecosystem in the EU by analyzing and unifying national rules and practices collected and presented in Section 4. Common rules for operators' coordination and reporting to CERTs are aligned with European legislation. Section 6 reports on the toolset design and describes the prototype. It specifies functional and non-functional requirements, defines the high-level architecture, and outlines key modules of the toolset based on TheHive, Cortex, and SAPPAN technologies. In Section 7, we report on the implementation and verification of the proposed procedures, rules, and tools. We cover key scenarios for coordination, CTI exchange in the communities, and reporting. Finally, Section 8 concludes the document. It recaps the outcomes and gives directions for future work.

2 Underlying methods, standards, and frameworks

This chapter provides the theoretical background for the work done for D6.8. It describes the fundamental frameworks and standards on which incident response procedures, rules, and practices for the coordination between SOCs and CERTs are based. It also gives an overview of the methodologies and technologies underlying the toolset design and implementation.

2.1 Overview of common incident response frameworks

In this section, an overview of some of the well-known frameworks and methodologies to manage incident response is introduced. The National Institute of Standards and Technology (NIST) has produced two special publications referring to incident response, thus creating a framework. SANS Institute is the second framework to be introduced. Thereafter, the ISO 27035 will be shown, followed by other well-established methodologies which are relevant to the scope of CyberSEAS.

2.1.1 NIST incident response framework

In the year 2012, NIST published a special publication (NIST SP 800-61r2 [6]) to cover the “Computer Security Incident Handling Guide” establishing the way to define an Incident Response organization, a method to handle incidents, and an approach to coordinate and share information. This is what we know as the NIST Incident Response Framework.

Moreover, NIST has also published an Internal Report in 2022 (NISTIR-8428 [7]) covering “Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)” covering the identification, handling, analysis, response, and finalization of incidents in the scope of OT environments. This publication establishes the NIST OT DFIR Framework.

2.1.1.1 NIST SP 800-61r2

2.1.1.1.1 Organization

These sets of guidelines indicate the most important administrative measures to be implemented to manage the IR capabilities of an organization. The following are the most important measures:

- a. **Policies** for incident response ought to have a purpose, scope, terms definition, roles, responsibilities, severity ratings, performance measures, reporting forms, and above all commitment of management.
- b. **Plan**, formally established and including the approach to respond to incidents (mission, communication guidelines, organizational approach, metrics).
- c. **Procedure elements**, involving “standard operating procedures (SOPs)” which include “technical processes, techniques, checklists, and forms”.

- d. **Information sharing**, how to, what to, who to and when to inform. Some parties that may be involved in the communication process include other departments of the organization, vendors, media, outside IR teams, service providers, law enforcement, and customers.

2.1.1.1.2 Incident handling

NIST proposes an incident response lifecycle (shown in Figure 3 [6]), focused on four big steps detailed in the following lines:

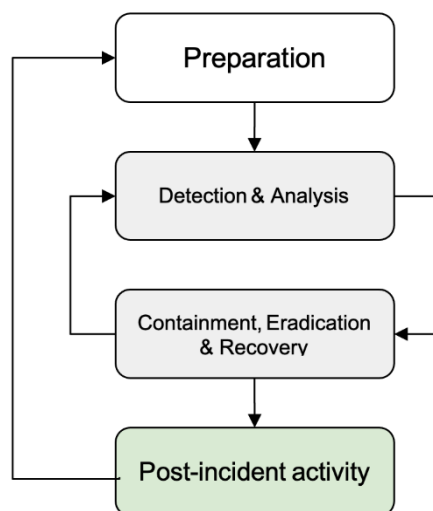


Figure 3 – NIST IR lifecycle.

- a. **Preparation:** This step takes care of preparing actions as well as preventive measurements. On the preparation side, the IR team ought to have information on contact, mechanisms for IR defined, an issue tracking system in place, smartphones, war room, encryption software, secure storage facility, forensic workstations, laptops, spare parts, blank removable media, portable printers, packet sniffers and port analyzers, and evidence gathering accessories. Moreover, incident analysis resources such as port lists, documentation, network diagrams, baselines, and cryptographic keys shall be at hand. Finally, access to images with clean OS (Operating Systems) and applications must be provided. As for the preventive actions, the organization ought to perform risk assessments, implement measures for host and network security, include malware prevention solutions and invest in awareness and training programs.
- b. **Detection and Analysis:** in order to start the **response** actions, the IR team needs to be ready to handle both unknown and well-known attack vectors. For the former, it is imperative to have access to documentation about Techniques, Tactics, and Procedures (TTPs). Signs of an incident might be difficult to find, the IR team will use its expertise to look into data available at Intrusion Detection Systems, antivirus, log analyzers, user's issue reports, file integrity tools, and authentication mechanisms, among others. Signs come in the form of precursors and indicators, both need to be part of the IR analysis activity. The framework includes recommendations in order to make the **Incident Analysis** as effective as possible: Profile networks and systems, understand normal behaviors, create a log retention policy, perform event correlation, keep all hosts clock synchronized, maintain and use a knowledge base of

information, run packet sniffers, perform internet research, filter data, seek assistance from third parties. Incident **documentation** must be standardized, and for that the NIST IR framework offers a list of topics to be covered. As for Incident **prioritization**, the NIST IR framework covers three factors that can be used to perform it, namely: functional impact, information impact and recoverability. These three factors have 4 categories each, which will allow the IR team to make a decision on how to react. This step finalizes with incident **notification**, for which, the NIST IR Framework provides a list of exact reporting requirements all organizations must fulfill.

- c. **Containment, Eradication & Recovery: Containment** starts with choosing the right strategy. As the framework states, “organizations should create separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision-making”. Afterward, **evidence gathering and handling** must be done. All procedures performed in this step must be thoroughly documented, especially when legal proceedings will be required. The information must be well-identified. The time and place where the evidence was found, and the name of the person in the team in charge are a must-have. Thereafter, identification of the attack host is performed by identifying IP addresses, internet research, incidents databases, and other communication channels. Finally, **eradication and recovery** take care of eliminating any source of malware, communication channels to command and control, disable faulty user accounts, setting up a clean version of the production environment, test and validate that all mitigation patches are applied and working properly.
- d. **Post-Incident activity**: when the incident has been closed, an analysis of all actions taken, tools used, procedures, and methods put in place, are documented on a **lessons learned** knowledge base, for future reference and improvements. Moreover, the data of the incident is also analyzed in order to extract key performance indexes, such as time of response, effectiveness of assessments, among others.

2.1.1.1.3 Coordination and information sharing

When more than one IR team acts in order to eradicate a threat, a coordination and communication strategy needs to be in place. The NIST IR Framework details guidelines for coordination activities, handling relationships, sharing agreements and reporting requirements, and techniques used to share incident data.

2.1.1.2 NIST IR 8428

The OT DFIR Framework (Digital Forensics and Incident Response Framework for Operational Technology) from NIST is based on the NIST IR Framework shown in the previous section and has six phases (shown in Figure 4 [7]):

- a. **Routine**: this constitutes the preparation phase of the framework. The focus is on Asset Identification and Data Collection. The aim is to integrate SOC activities and Facility Control Room (FCR) monitoring with the IR team analysis.
- b. **Identification**: the SOC and the FCR check alerts on the system and check whether it corresponds to “normal” operational malfunction. If so this phase is used to repair the malfunction and go back to routine. If not, a technical report is declared.
- c. **Handling**: This phase occurs when an event has been identified and reported. An in-depth analysis is performed by the Technical Support Team (TST) to either solve it or

escalate it while saving all evidence in the chain of custody. At this point, an incident has been identified and is properly reported.

- d. **Analysis and response:** Management agrees to launch incident handling activities. This phase constitutes the actions performed to declare and respond to such incidents. IR Team collects data from all sources relevant to the incident, including data coming from the Routine phase. Digital Forensics and Response activities start, in parallel with continuous situational analysis. In order to apply countermeasures and perform contaminants, eradication, and recovery, the IR Team will need a green light from management and all stakeholders from the FCR.
- e. **End of incident:** In this phase Management announces that either the incident has been solved or that the issues remaining no longer affect the “normal” operation of the system and therefore the incident can be closed. IR Team performs lessons learned analysis and publishes a final report.
- f. **Post-incident:** During this phase, the SOC and FCR perform monitoring activities with focus on the part of the system that was affected by the incident. The behavior of the system is analyzed for a previously agreed-on.

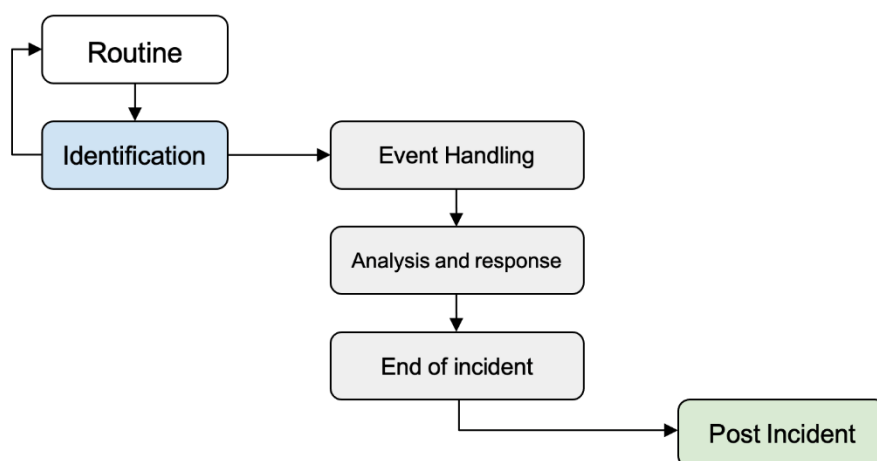


Figure 4 – NIST OT DFIR phases.

2.1.2 SANS incident response framework

The institute SANS provides a handbook [8] describing the “six phases of the incident handling process” as a framework to create “incident response policies, standards, and teams” for any organization.

The cycle entails six phases, as shown in Figure 5.

- I. **Preparation:** The Response teams prepare to handle the incident regardless of the cause. In order to do that, this phase of the cycle shall be used to implement a policy, response plan or strategy, a communication plan, incident documentation (notes, commands, systems affected), a list of team members, access controls (for the IR team), tool set (preferably already in a “jump bag”, ready to be used), and training (the IR team should not only be ready to act but know how to).
- II. **Identification:** The operations team evaluates information available (e.g. log files, error messages, network monitoring, behavior analysis, Intrusion detection, or protection

systems) in order to check if the event can be cataloged as an incident. When an incident has been identified, then it is reported to the Incident Response team to be handled. The Incident Response team shall gather evidence while handling the incident. Documentation is also key in this phase as all tasks performed, information gathered, people communicated, tools used, and blocking points found should be available transparently during the following phases.

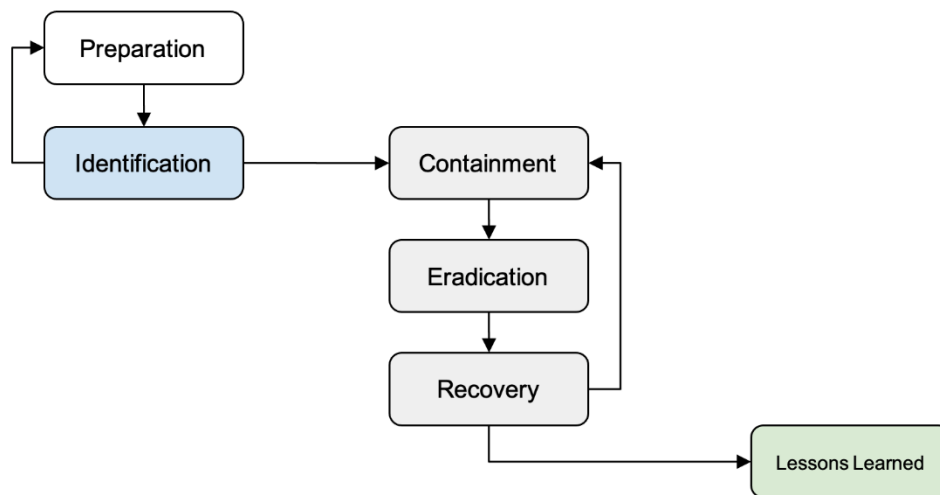


Figure 5 – SANS IR cycle.

- III. **Containment:** This phase is about closing doors so that the incident does not spread, mitigating it and taking the actions required to protect the evidence from destruction or loss. Three sub-tasks are part of this phase, short-term containment <<limit the damage>>, system back-up <<wipe, reimaging and forensic analysis>>, and long-term containment <<fix temporarily and give the systems back to production>>.
- IV. **Eradication:** This phase takes care of the removal of malicious content (cleaning, patching, reconfiguring, deleting unused services/ports) in the systems of scope, as well as on the neighboring systems, and documenting everything that has been performed. After all this is done, a validation needs to take place in order to check that the incident does not happen again.
- V. **Recovery:** Return to normal operation is the objective of this phase. In order to get them back into production, a plan shall be in place with the proper maintenance window defined to reinstall, test, monitor, and validate all previous systems (including neighboring systems). Test and validation must have a proper protocol and a timeframe should be appointed for monitoring.
- VI. **Lessons Learned:** A post-incident analysis needs to be performed. In order to do that, the documentation from all previous phases needs to be complete, clear, and put into report mode. It shall contain all information regarding the detection of the incident, the scope of work, and all containment, eradication, and recovery actions (including persons responsible, methods, and tools). Blocking points and improvement actions shall be included as well, so that incident handling practices are enhanced.

2.1.3 ISO/IEC 27035 incident management

ISO/IEC 27035 [9] guidance provides concepts and steps of information security incident management and combines these concepts with principles in a structured approach to incident detection, reporting, assessment, and response, and applying lessons learned. ISO/IEC 27035 is not a complete guide, but a reference for some basic principles aimed at ensuring that tools, techniques, and methods can be appropriately selected and, where necessary, demonstrated fit for purpose.

Organizations such as Energy Companies can adjust the guidance given in this part of ISO/IEC 27035 according to their type, size, and nature of business in relation to the information security risk situation.

From an organization's perspective, the primary goal is to prevent or contain the impact of information security incidents to minimize the direct and indirect damage to operations caused by the incidents. As a key element of an organization's overall information security strategy, the organization should establish controls and procedures to enable a structured, well-planned approach to information security incident management.

A structured well-planned approach to incident management should include the following:

- a. Information security events are detected and dealt with efficiently, in particular deciding when they should be classified as information security incidents.
- b. Identified information security incidents are assessed and responded to in the most appropriate and efficient manner.
- c. The adverse effects of information security incidents on the organization and its operations are minimized by appropriate controls as part of incident response.
- d. A link with relevant elements from crisis management and business continuity management through an escalation process is established.
- e. Information security vulnerabilities are assessed and dealt with appropriately to prevent or reduce incidents. This assessment can be done either by the IRT or other teams within the organization, depending on duty distribution.
- f. Lessons are learned quickly from information security incidents, vulnerabilities, and their management. This feedback mechanism is intended to increase the chances of preventing future information security incidents from occurring, improve the implementation and use of information security controls, and improve the overall information security incident management plan.

To achieve the objectives outlined above, information security incident management consists of five distinct phases shown in Figure 6:

- a. **Plan and Prepare:** Effective information security incident management requires appropriate planning and preparation. For an efficient and effective information security incident management plan to be put into operation, an organization should complete a number of preparatory activities, such as formulation and production of an information security incident management policy and define and document a detailed information security incident management plan.
- b. **Detection and Reporting:** This phase involves detecting the gathering and reporting occurrences of information security events. For the detection and reporting phase, an organization should undertake the following key activities such as monitoring and recording system and networking activity of the constituency or parent organizations

as appropriate. Reporting security events in line with your organization's reporting policies allows for later analysis if needed.

- c. **Assessment and Decision:** This phase involves the assessment of information associated with occurrences of information security events and the decision on whether to classify events as information security incidents.

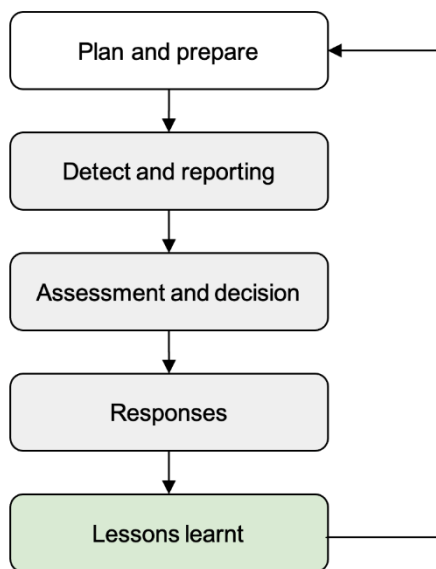


Figure 6 – ISO 27035 IR phases.

Once an information security event has been detected and reported, some of the subsequent activities should be performed such as distributing the responsibility for information security incident management activities through an appropriate hierarchy of personnel with assessment. The IRT can conduct a quality review to ensure that the incident handler correctly declared an incident. All information collected pertaining to an information security event, incident, or vulnerability should be stored in the information security database managed by the IRT. The information reported during each activity should be as complete as possible at the time. This will support assessments, decisions, and actions to be taken.

- d. **Responses:** In the fourth phase, the IR team implements the response actions determined in the Assessment and Decision phase. Responsibility for actions is distributed, along with well-documented procedures and guidelines. This Framework states that the following activities need to be performed while responding to incidents: an investigation based on the classification scale rating of the incident, review and perform response or crisis management actions, assign resources, escalate as needed, document all actions, gather and store digital evidence securely, communicate to stakeholders according to the communication plan. After recovery from an incident, perform an investigation of the information surrounding the incident, create a report, and close the incident after storing all data relative to the incident in the knowledge base.
- e. **Lessons Learned:** The fifth phase starts when incidents are resolved. All actions regarding incident handling, vulnerability management, and information security control implementation, are analyzed. Moreover, the effectiveness of processes, procedures, reporting formats, and organizational structure are checked and

enhancement actions are triggered. Documentation improvement, IRT performance analysis, and information sharing (if required) happen also in this phase.

It must be kept in mind that some activities can occur in multiple phases or throughout the incident handling process such as the documentation of event and incident evidence, coordination and communication between the involved parties, notification of significant incidents to management and other stakeholders, and so on.

2.1.4 MITRE ATT&CK

The MITRE ATT&CK framework [10], short for Adversarial Tactics, Techniques, and Common Knowledge, is a knowledge base of adversarial tactics and approaches. These approaches are indexed and break down in detail how hackers operate. This allows teams to understand the actions that can be used against a particular platform. Furthermore, MITRE also includes cyber threat intelligence, which documents the behavioral profiles of attackers to record which attacker groups use which procedures.

The ATT&CK matrix structure resembles a periodic table with column headers describing the phases in the attack chain (from initial access to full attack), while rows describe specific procedures. This framework helps the user to learn more about the platforms attacked, and the tactics and procedures an attacker might use. It provides examples of known attacks and/or reference material like white papers for each technique. This information will support the security expert with knowledge about the risks, possible detection, and measures.

The MITRE ATT&CK framework is widely recognized as a reference work, explaining the behaviors and approaches that attackers are currently using against businesses. It removes the ambiguity and provides industry professionals with a consistent vocabulary to share and collaborate on combating these hostile methods.

2.1.4.1 TTP-Based Detection

Rather than characterizing and searching for tools and artifacts, a more robust approach is to characterize and search for the techniques adversaries must use to achieve their goals. These techniques do not change frequently and are common across adversaries due to the constraints of the target technology. The MITRE ATT&CK framework is an effective way to characterize those techniques. ATT&CK categorizes reported adversary TTPs from public and open cyber threat intelligence and aligns them by tactic category within the phases of the Cyber Attack Lifecycle [11].

2.1.5 Other frameworks

Given that Incident Response is an important aspect of wider cyber operations, it is important to ensure that IR capabilities are applied systematically and consistently. Several authoritative governmental and industry bodies (e.g., ISACA, CREST) have proposed IR models that organizations can use to establish and mature their own IR capabilities.

In 2013, CREST published a guide for cybersecurity IR that outlines a model with three high-level phases [12]. The guide focuses on providing practical advice, but the model includes a number of detailed steps associated with each phase of the life cycle.

CREST advises that it is important to determine current maturity levels so companies can ensure they have adequate IR capability to match that of their industry peers. A unique aspect of the CREST model is the recognition that for some organizations outsourcing all or part of the IR capabilities is the most appropriate course of action. In fact, CREST has published a Cybersecurity IR Supplier Selection Guide to help organizations identify which processes and activities to outsource, set supplier selection criteria, and then appoint an IR supplier [13].

NIST and CREST have proposed similar IR lifecycle models, highlighting the consensus that an IR lifecycle should include phases focused on identification, response, and lessons learned. These models also emphasize the importance of ensuring that IR capability is fully prepared for an incident, and both recommend that post-incident organizations hold regular lessons-learned sessions to identify opportunities for continuous improvement.

Management Objective DSS02 of the COBIT 2019 IT governance framework [14], published by ISACA (Information Systems Audit and Control Association), addresses managed service requests and incidents. From the incident's perspective, the guidance states that the ultimate purpose of IR is to support the delivery of information and technology services. The COBIT model does not include a lifecycle, but it does describe the management processes that should be in place for IR and the mechanisms needed to assess the maturity of those processes.

COBIT can be used by organizations to understand the maturity associated with IR processes. Not all organizations require full IR capability but using CMMI (Capability Maturity Model Integration) maturity levels allows them to identify their current maturity level and perform a gap analysis against the ideal target state.

2.2 Overview of CTI exchange standards

CTI (Cyber Threat Intelligence) allows for a more proactive and intelligent incident response. CTI exchange may increase the efficiency of coordination between SOCs and CERTs. It can hence be implemented as an integral part of the T6.4 toolset for operators' coordination and reporting to CERTs in case of incidents. For this purpose, this section provides an overview of the key CTI exchange standards and frameworks.

2.2.1 STIX and TAXII, Version 2.1

STIX (Structured Threat Information eXpression) is a standardized XML programming language and serialization format for exchanging data regarding cybersecurity threats. It is a common language that can be easily understood by humans and security technologies.

STIX enables organizations to share Cyber Threat Information (CTI) with each other in a consistent and machine-readable way. It allows security communities to better understand computer-based attacks and to be better prepared to respond to such attacks faster and more effectively.

STIX is an open-source standard that was initially defined in 2012 by the OASIS Cyber Threat Intelligence TC (Technical Committee). The current version of STIX is 2.1 and was released in March 2020 [15].

STIX (in version 2.1) defines a total of 18 STIX Domain Objects (SDOs), which are higher level intelligence objects that represent behaviours and constructs that are typical to work with while understanding the threat landscape. Each of these objects corresponds to a concept commonly used in CTI.

TAXII (Trusted Automated Exchange of Intelligence Information) [16] is an application layer protocol used to exchange Cyber Threat Intelligence (CTI) information in a simple and scalable manner. It is an OASIS standard, developed and managed by the Cyber Threat Intelligence Technical Committee. A TAXII client can request desired CTI information from a TAXII server by specifying a set of metadata filters, included in the request. A manifest of available CTI content can also be requested, in addition to information about how a CTI collection is structured and may be navigated.

TAXII defines two primary services, Collections and Channels, to support a variety of commonly-used sharing models. Collections allow a producer to host a set of CTI data that can be requested by consumers. Channels allow producers to push data to many consumers and allow consumers to receive data from many producers.

The current version (v2.1) of the TAXII specification reserves the keywords required for Channels, but does not specify Channel services. Channels and their services will be defined in a subsequent version of the TAXII specification.

TAXII was designed to transport Structured Threat Information Expression (STIX) and some of its features are intended to align with STIX. However, TAXII is pay-load agnostic and does not assume any specific CTI format. TAXII and STIX are independent standards. TAXII can be used to transport non-STIX CTI information and STIX does not rely on any specific transport mechanism.

TAXII relies on existing protocols wherever possible. It uses HTTP for content negotiation and authentication. TAXII servers can be discovered within a network via DNS service records. TAXII uses UTF-8 encoded JSON as the serialization format for all TAXII exchanges. In addition, HTTPS provides the transport for all TAXII communications.

TAXII defines an API Root that organizes and provides access to CTI data. A TAXII Server can host multiple API Roots to provide for division of content and access control. Figure 7 below depicts the logical structure of an API Root.

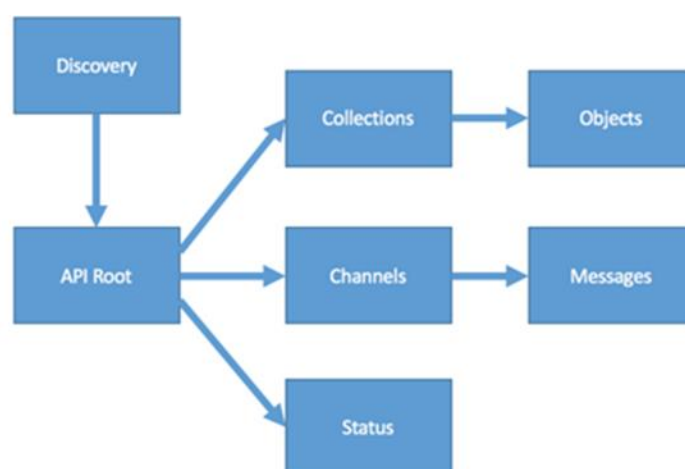


Figure 7 – TAXII – the logical structure of an API Root.

Discovery information can be used to learn about the API Roots hosted by a TAXII Server. Collections in an API Root allow TAXII Clients and Servers to exchange CTI using a request-response paradigm. Interactions with Collections include getting a manifest of CTI contained in the Collection, adding new CTI content, and retrieving CTI content. Individual items of CTI content in a Collection are referred to as Objects.

Channels will allow TAXII Clients to exchange information using a publish-subscribe paradigm by the means of Messages. Channels will be specified in a future version of TAXII.

Status information pertaining to requests sent to the TAXII Server are also supported by the API Root. For example, if a TAXII Client submitted new CTI to a Collection, a Status request allows the Client to check on whether the new CTI was accepted and added to the Collection.

2.2.2 MISP

The Malware Information Sharing Platform (MISP) is an open-source threat intelligence platform. It is licensed under the GNU Affero General Public License version 3. It offers a flexible data model that can express complex objects and link them, including events, objects, object references, tags, and sightings, as well as MISP Galaxy [17]. It can be used to share both technical and non-technical information about malware samples, incidents, attacks, and general cyber threat intelligence.

The primary purpose of MISP is to enable organizations to share valuable threat intelligence in real-time to help each other prevent cyber-attacks. It allows users to share indicators of compromise (IoC), threat intelligence, and other security-related data in a structured and standardized format, such as shareable cybersecurity playbooks. This helps to ensure that all security teams are on the same page and can act quickly to mitigate potential security risks.

One of the key advantages of MISP is its flexibility, as it allows for the storage and sharing of information without mandating users to contribute data. Organizations can customize the tool to fit their specific cybersecurity requirements and share threat intelligence quickly and efficiently. Additionally, MISP's structured format for storing data helps automation in utilizing databases, and its user interface supports export to various data formats, including Snort, STIX, OpenIOC, text, and CSV.

Furthermore, MISP offers various import and integration capabilities, including feed import and integration of threat intelligence or OSINT feeds. It allows for the automated synchronization of events and attributes with other MISP instances. It can be used to delegate sharing functionalities as well.

Two key components are developed to support the data representation in the MISP platform: the MISP Taxonomy [18] and MISP Galaxy. The MISP Taxonomy is a structured format for storing data. It is described in JSON that uses Machine Tags ("Triple Tags") and provides a flexible and adjustable taxonomy for classifying and tagging events. MISP also provides a PyMISP API. Events can be classified and tagged via a large collection of existing taxonomies, and custom classification schemes can also be created. Taxonomies can be local or shared among MISP instances. Sighting support is also available to share observations concerning

shared indicators and attributes. Moreover, MISP integrates encryption and signing for notifications via PGP and S/MIME, and provides a real-time publish-subscribe channel for threat intelligence sharing.

The MISP Galaxy, on the other hand, allows for a standardized approach to data classification and consistent data representation across different organizations. The MISP Galaxy consists of a set of pre-defined categories, including threat actors, malware families, attack patterns, and tools. Each category is a separate JSON file that includes a set of pre-defined tags. These tags can be utilized to categorize events and attributes within the MISP platform.

2.3 Reporting mechanisms

In this section, an overview of common reporting techniques, tools and mechanisms is given. Suitable reporting capabilities are an essential part of the implemented toolset to facilitate coordination with CERTs.

2.3.1 Dashboards

Dashboards give a meaningful overview of what is currently happening in the monitored systems. They provide security analysts with insights into the infrastructure and any occurring alarms or, in the worst case, ongoing attacks. The general dashboard should show some statistical as well as real-time values like the EPS (Events per Second). These values can be used to build statistics on an overall level or break down to some critical components, which are monitored. A deviation of the current EPS value could indicate an ongoing attack phase (with a higher amount of occurring events) or some outages (with a lower amount of events).

The infrastructure dashboards give an overview of the current status of the critical components, like the workload or utilization of servers or network components. The security dashboards should give an overview of triggered alarms and might be enriched with CTI information (e.g., ongoing attacks in other industries or verticals).

Statistical values can be built upon the different domains of detection use cases, which are grouped into tactics, techniques, and procedures (TTPs) based on a standardized security framework like the MITRE ATT&CK. An increase in events or alarms related to a specific domain could be the first indicator of a compromise.

As the Level-1 Analyst is the first line of protection, he/she should monitor the dashboards all the time. The figures below show several sample dashboards. Figure 8 gives an example of the average network traffic divided into known and unknown connections. Figure 9 shows the network flows with the visualized amount of network traffic. A sample dashboard in Figure 10 shows connections of a specific network. The red-marked connections are not whitelisted and are thereby potentially malicious. Finally, Figure 11 presents the network traffic, used ports, and protocols of a specific network/host. The used protocols are divided into known IT/OT protocols.



Figure 8 – Sample dashboard showing the incoming and outgoing network traffic to hosts.

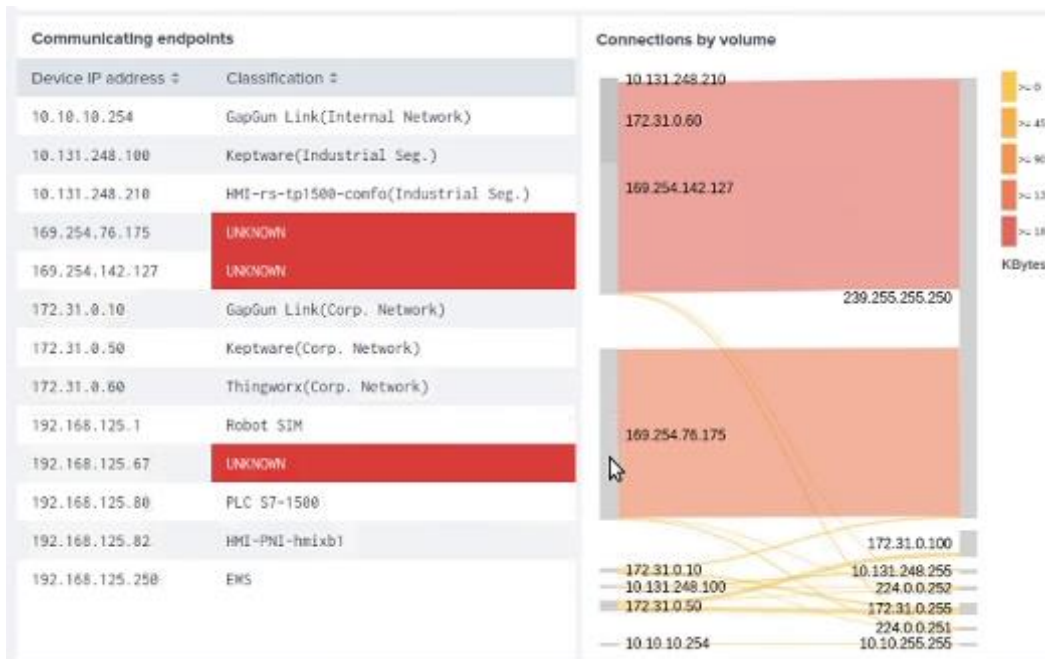


Figure 9 – Sample dashboard showing network flows with the visualized amount of network traffic.

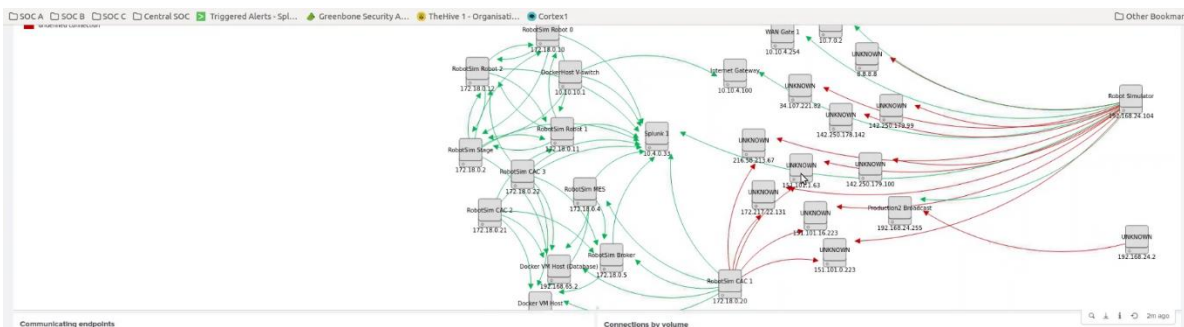


Figure 10 – Sample dashboard showing connections of a specific network.



Figure 11 – Sample dashboard showing the network traffic.

2.3.2 KPI-based reporting in the SOC

Various KPIs (Key Performance Indicators) are needed to keep track of the efficiency of the detection rules. When they're grouped into TTPs, based on the MITRE ATT&ACK framework, they also highlight the detection capability of each domain. Furthermore, the KPIs are needed for the agile approach of the Use Case Factory as feedback and for the tuning process of Use Cases. Some KPIs are also needed for the reporting to the customer (e.g., the SLA – Service Level Agreement) to verify that the SOC complies with contractual regulations. Some of the more relevant KPIs are the following:

- Alarms triggered by the CTI input
- Intrusion attempts
- EPS, statistics
- Metric of correlated IOCs
- False positive rate
- Statistics of solved cases (L1/L2/L3)
- Reportings to CERTs
- Tasks performed by security analysts
- Response tasks performed
- Duration (time) per case
- SLAs (Service Level Agreements)
- Successful/unsuccessful responses/detections per playbook
- TTPs (Based on MITRE) per alarm
- Time to detect (TTD)

- Time to triage (TTT)
- Time to qualify (TTQ)
- Time to acknowledge (TTA)
- Time to response (TTR)
- Time to contain (TTC)

Some of the listed indicators are native to TheHive [19]. A sample KPI dashboard in Figure 12 depicts the Mean Time to Detection (MTD) metric. Using this metric in dashboards can help us to understand our efficiency and identify areas that may require more attention or effort.

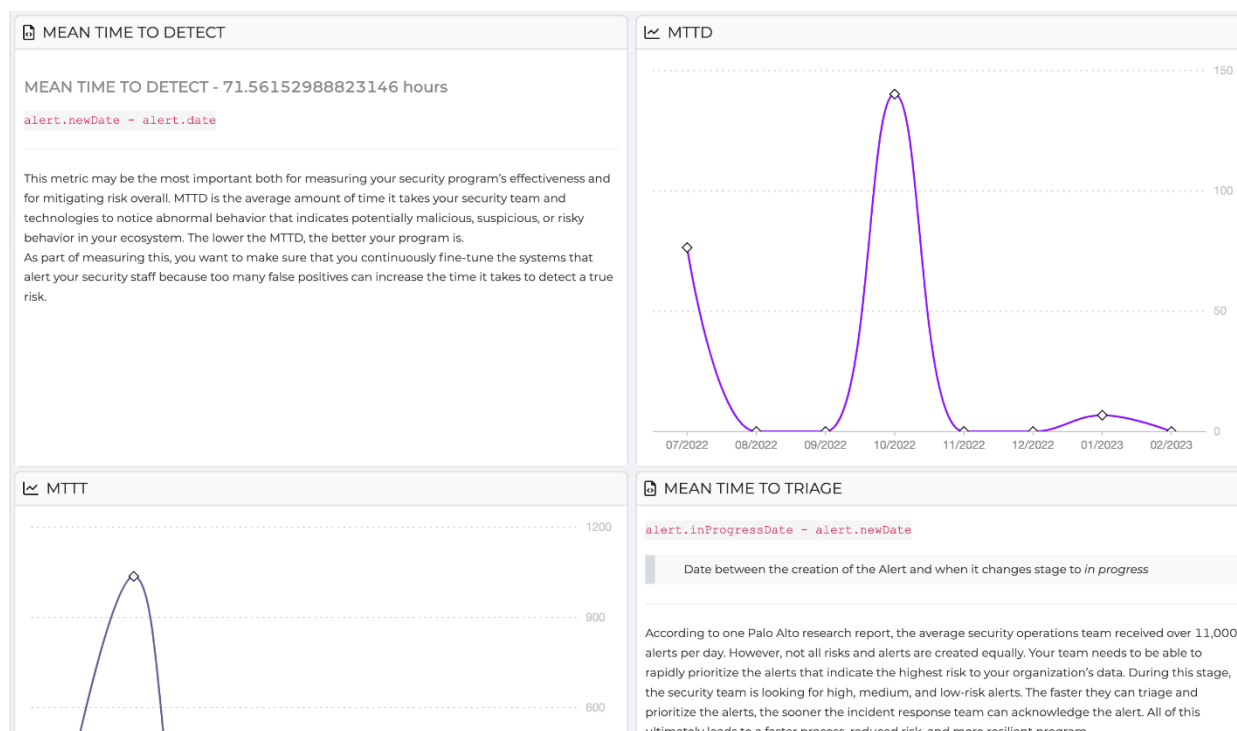


Figure 12 – Sample KPI dashboard showing the MTD metric.

2.3.3 Email and PDF reporting

Reports can either be defined per alarm, which is raised on each SIEM event but should only be configured on events with a high severity. In this first phase of an unconfirmed incident, the correlation events could automatically be sent as plaintext, HTML (HyperText Markup Language), or as an attached PDF file with the correlated event and its dataset.

On a regular basis (weekly, monthly, etc.), the KPIs should be provided to all stakeholders, which may include the asset owner, the department, the security officer, and the Use Case Factory for the continuous enhancement of the use cases.

Figure 13 shows a sample screenshot of an email notification, triggered as a response to a SIEM alert. Figure 14 presents a sample output of a SIEM alarm query, sent as a PDF report via email.

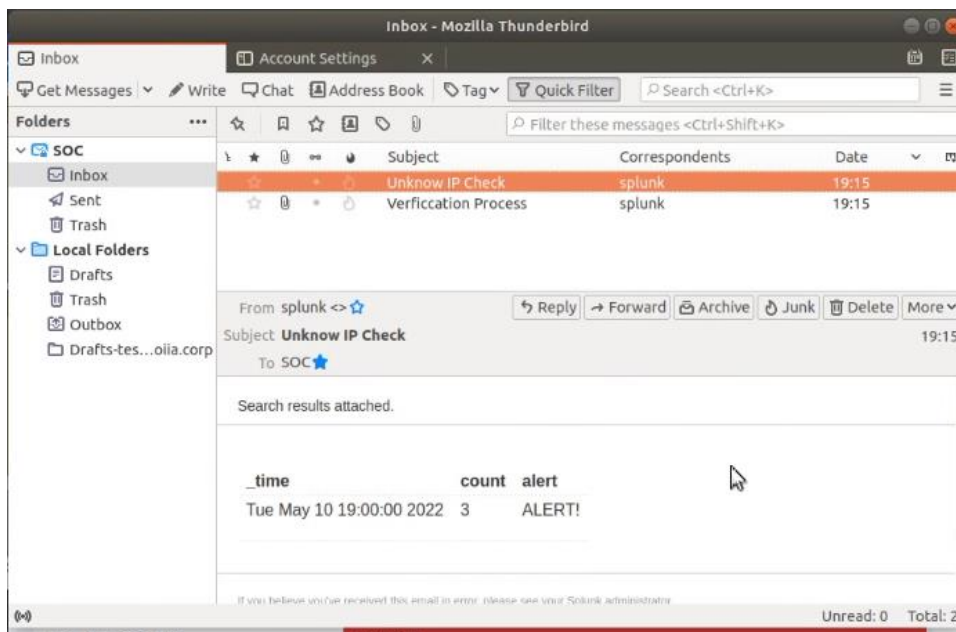


Figure 13 – Sample email notification as a response to a SIEM alert.

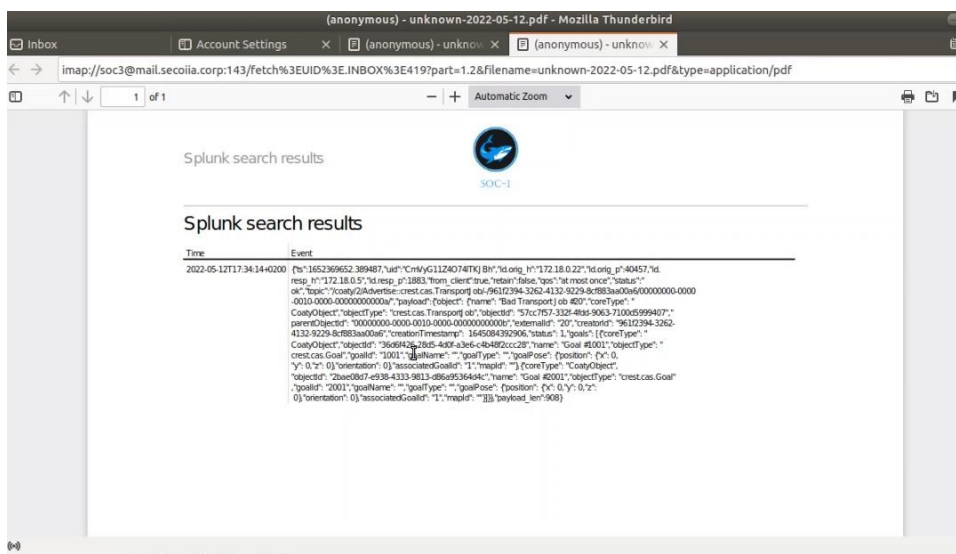


Figure 14 – Sample PDF report as a response to a SIEM alert.

2.3.4 Incident reporting to stakeholders

When an incident is confirmed during the detection phase, a report on each case should be provided to the stakeholder, such as the asset owner or security officer. These reports should contain at least the collected and enriched data, as well as the IOCs that confirmed the incident. If feasible and applicable, a recommendation of possible mitigation measures may also be provided, in the case the reported incident cannot be directly solved or needs to be escalated to the CERT. CISA (Cybersecurity & Infrastructure Security Agency) has, together with NIST, developed a Cyber Threat Indicator and Defensive Measure Submission System [20].

Reports are created and communicated to keep people in the loop. Three levels of reporting should be applied in different circumstances:

- to the asset owner or customer;
- to CISO (Chief Information Security Officer); and
- to CSIRT (Computer Security Incident Response Team) or CERT (Computer Emergency Response Team).

2.3.4.1 Reporting to the asset owner or customer

This is the most basic approach. It is also applicable for incidents of low impact or severity. Email reporting (as described in Section 2.3.3) and direct communication may be utilized. A formal report structure is not necessary.

2.3.4.2 Reporting to CISO

In the case that the administrator of the compromised service or asset determines that an incident of higher criticality occurred, the CISO must be notified. On the scale of incident severity, such an incident is generally assessed at least as moderate or important. More formal report methods and structures (such as PDF) may be used in addition to emails and direct communication for the purpose of reporting incidents to the CISO. Some KPIs from Section 2.3.3 might be relevant for the CISO and the board of directors [21]. Based on the reported incident, the CISO usually activates the incident response team. The latter should follow the recommendations of NIST on incident response [6] and should trigger potential coordination with the CSIRT/CERT.

2.3.4.3 Reporting to CSIRT/CERT

If a high criticality is determined (i.e., a very important or critical incident), the CISO or the response team must activate the crisis management team and include CSIRT/CERT in the loop. In this case, the procedures for continuous operations are triggered. The most common method of reporting an incident to CSIRT/CERT is via an online form with a predefined structure. Such a form is accessible through a web link. It collects key information, including the organization, contact person, time of the incident, description of the issue, potential impacts, and measures taken or planned to be taken. Most national CERTs provide such a reporting web form, as explained in Section 4 of this deliverable. NIST has also introduced a standard incident reporting web form. It is based on NIST's incident handling guide [6] and may be considered a reference. It is used in practice for incident reporting to CISA.

A well-designed incident reporting web form might give advice related to common incidents to make incident reporting easier.

2.3.5 Change management reporting

This kind of reporting accompanies the process of change management in the case when response action has been performed or has to be performed. When L2 or L3 SOC performs a mitigation measure, such as adding a new proxy or firewall rule, it has to be documented as defined in the regular change management process. Similarly, if the analyst does not have

sufficient rights to perform a remediation action, change requests need to be tracked in a separate ticketing system (e.g., Jira [22]).

2.3.6 API-based and automated reporting

Data on cyber incidents is usually collected from several sources, for example, based on the automated processing of alerts from integrated systems. Such automatically collected alerts can be directly reported to CERTs and other EPES stakeholders with application integration by using APIs (Application Programming Interfaces) or other means of software integration.

One approach is the integration with the MISP (Malware Information Sharing Platform) threat-sharing platform [23]. MISP can be provided by the CERT and is accessible to EPES operators via a web interface or REST (REpresentational State Transfer) API. Other types of integrations can also be implemented and customized for specific systems. They are usually based on the JSON (JavaScript Object Notation) data interchange format [24]. In the case when web applications are integrated, we sometimes refer to the webhook method [25]. Another contemporary technology that can be utilized for automated reporting is Apache Kafka [26]. It is an open-source distributed event streaming platform designed for data pipelines, streaming analytics, data integration, and mission-critical applications.

Additional types of tools for automated reporting might include [27]:

- Work management tools, such as Jira, help teams track, complete, and collaborate on their work asynchronously.
- BI (Business Intelligence) tools pull data from multiple sources and provide the ability to transform, analyze, and report it. Two major representatives of these tools are MS Power BI [28] and SAP BusinessObjects Business Intelligence suite [29].
- CRM (Customer Relationship Management) platforms allow organizations to build and manage relationships with their partners, customers, and other contacts. They support various powerful reporting features, although they might not be directly applicable to cybersecurity-related reporting.

2.4 MCDM assessment methods

The frequency and scope of reporting to CERTs and the level of coordination between EPES operators and CERTs depend on the severity of detected incidents. It is hence necessary to assess the severity and impact of each incident to be able to select and trigger the most suitable incident response procedures and reporting mechanisms. Several criteria must be considered to judge the impact with regard to technical constraints, business requirements, available resources, etc. An appropriate MCDM (Multi-Criteria Decision-Making) model for incident impact assessment must therefore be designed and used. Such a model is based on one or more MCDM methods. Because many MCDM methods exist, it is the aim of this section to give a brief overview of them and analyze their suitability for implementation in the context of incident impact assessment.

The work on the MCDM assessment is shared between tasks T4.4 and T6.4. The MCDM model for incident impact assessment is being developed for the purpose of both tasks and is used by the resulting toolsets of both D4.8 and D6.8. A thorough SOTA (State-Of-The-Art) overview and analysis of the of MCDM methods is hence provided by the CyberSEAS deliverable D4.8.

The interested reader should refer to this document for details. Here, we only recap two approaches that have been determined in D4.8 to be the most suitable for the general field of cybersecurity and for the incident impact assessment in particular. These methods are the multi-attribute additive value function and qualitative MCDM.

2.4.1 Additive multi-attribute value models

This methodological approach originates from utility and bargaining theory. MAUT (Multi-Attribute Utility Theory) [30] models the preferences of the DM (Decision-Maker) by means of the utility function. It depends on the expert's opinion to determine the attribute weight and alternative utility. Because this technique requires DMs to decide on one value based on all other attribute values, all attribute values must be considered at the same time.

MAUT is based on the formal axiomatized approach of certain equivalence. Criterion-wise values x of alternatives are monotonously projected to the $[0, 1]$ interval. The best unacceptable value and the worst still acceptable value are the extreme points that determine the standard preference lottery L . By following the concept of certain equivalence, utilities of alternatives are derived with a sequence of iterative steps so that for each value x the decision-maker is indifferent between x and L with the probability of p . A linear and transitive total order is thereby obtained. A single utility function is defined for each criterion or attribute. It can have a risk-seeking, risk-averse, or neutral form. Partial utilities are weighted and aggregated into the overall utility.

It is not natural for most DMs to model preferences by means of lotteries and uncertainties. For this reason, the value function is often used instead of the utility function. DM is able to express personal preferences for each attribute (criterion) directly with a value function. Such a function maps the domain values (e.g., time, cost, type of cybersecurity software, level of expertise, etc.) into acceptability values or scores, which are usually expressed on the $[0, 1]$ numerical interval. However, these acceptability values can also be qualitative (e.g., high, medium, low, etc.), as in the case of the DEXi (DEcision eXpert) method.

For each attribute, a corresponding value function is modeled and used. In this way, criteria-wise values of alternatives are obtained. These partial values are then aggregated into the overall value. The most common aggregation operator is the weighted sum. It is regarded as the basic additive decomposition model, but multiplicative or rule-based decomposition models can also be applied. In addition, value or utility functions can be aggregated with (partially) non-compensatory veto functions [31]. The weighted aggregation is usually known in the literature as weighted averaging (WA) or the simple additive weighting method [32]. A similar class of operators can deal with ordered weighted averaging (OWA) [33].

Additive value models represent the most common and widely applied approach to MCDM. For example, the CVSS (Common Vulnerability Scoring System) [34] score is also a case of an additive value model. This is demonstrated in Figure 15 where the scores (values) on several CVSS criteria are aggregated into the overall CVSS score (value).

D6.8 Rules & Tools for Operators' Coordination and Reporting to CERTs in Case of Incidents V2

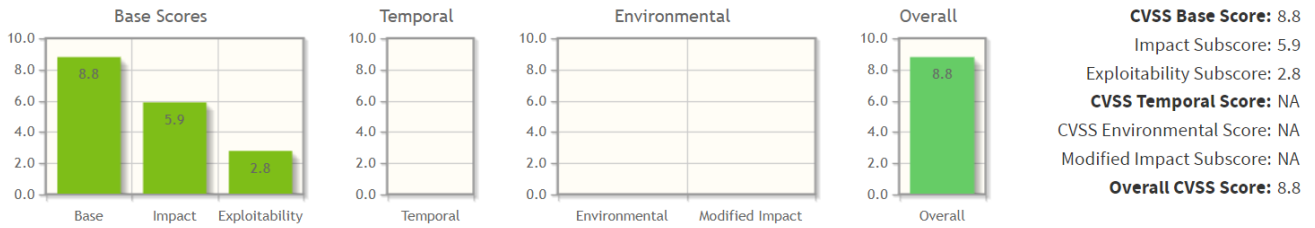


Figure 15 – Additive value aggregation in the CVSS impact assessment model.

2.4.2 Qualitative approaches

Qualitative MCDM aims to analyze and address situations utilizing data and values provided by decision-makers who are typically experts in a certain domain. Consequently, qualitative models are adequate for unstructured decision problems where approximate judgments take precedence over exact numerical calculations [35]. These methods have been used in different applications, such as ecology and e-learning [36].

For the design of the DSS (Decision Support System) in CyberSEAS, qualitative methods provide a suitable model that fits with the qualitative impact assessment for cybersecurity events. Therefore, we have decided to adopt the DEXi solution, which will be used in the decision-making process as one of the key MCDM methods, in addition to the additive value approach.

DEXi is a computer program for multi-attribute decision-making [37]. Its goal is to facilitate the interactive construction of qualitative multi-attribute decision models and the evaluation of alternatives. This is beneficial for assisting with difficult decision-making activities in which a specific alternative must be chosen from a group of available options to fulfill DM's aims. A multi-attribute model is a hierarchical structure that represents the decomposition of the decision problem into sub-problems that are smaller, less complex, and possibly easier to solve than the complete problem. The use of DEXi is demonstrated in Figure 16.

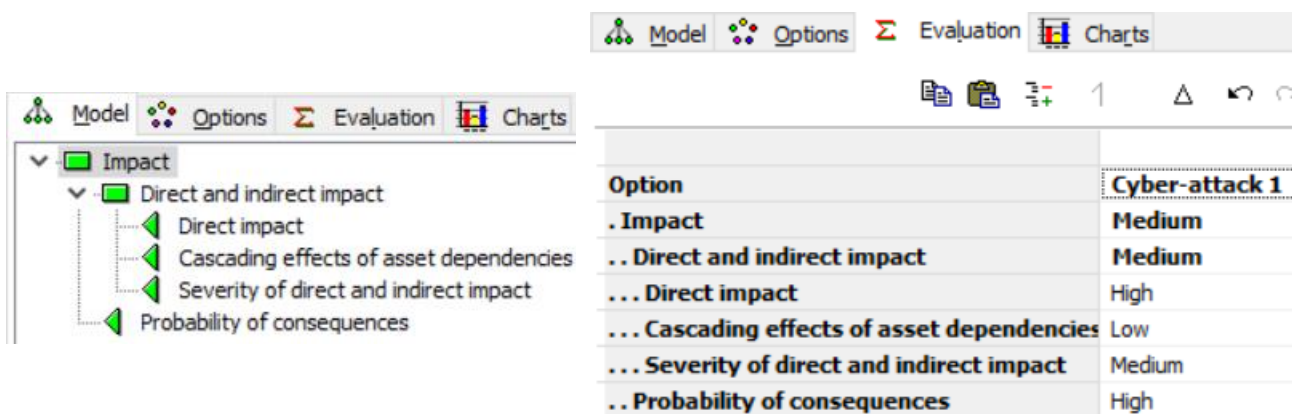


Figure 16 – An example of a DEXi decision model.

2.5 Group collaboration and coordination procedures

In the complex EPES system, many stakeholders take part in the common data space and participate in the common energy supply chains. In the case where one stakeholder faces a cybersecurity attack, this attack might as well compromise the assets, services, operations, and business processes of several other stakeholders due to cascading effects. For this reason, different stakeholders must collaborate in selecting and executing the most efficient incident response procedures and strategies that would be of considerable benefit to the entire EPES system and its infrastructure. They must also engage in a collective assessment of the impacts of detected incidents that can potentially cause harm to the IT/OT systems of connected EPES stakeholders. The implemented toolset will hence facilitate several group coordination and decision-making techniques and procedures. This section aims to give an overview and analysis of these approaches. However, this part of the methodology and toolset implementation is also shared between tasks T4.4 and T6.4. A detailed presentation of the topic is hence provided in the deliverable D4.8. Here, we briefly summarize the main concepts.

2.5.1 Group MCDM methods

Group decision-making (also known as collaborative decision-making) is a situation faced when different stakeholders are collectively included in the decision-making process. Three basic questions are considered in group decision-making: (1.) how to extract stakeholders' knowledge and preferences; (2.) how to combine these preferences and knowledge; and (3.) how to conduct discussions and resolve conflict situations [38].

Several techniques are used to acquire, extract, and represent stakeholders' knowledge and preferences in group decision-making [38], including the acquisition of domain knowledge that is facilitated by the knowledge expert, the elicitation of knowledge based on questions, and idea generation. After the knowledge is extracted, individual decisions are made by using the MCDM methods described in Section 2.4. Individual decisions and/or preferences are then aggregated into collective decisions and/or preferences. This could be either a fully consensual solution or some averaging that represents a more or less efficient compromise. Three main strategies may be used to combine the judgments and perspectives of decision-makers in group decision-making [39]: the input level aggregation strategy, the output level aggregation strategy, and the combined strategy.

2.5.2 Consensus-seeking procedures

The highest gain in group decision-making is achieved when individual preferences are not directly aggregated, but instead a true consensual solution is found. The consensus-seeking procedure might require several iterations of confirmation to unify the opinions of different stakeholders. Instead of aggregating input preferential parameters or scores of alternatives, decision-makers aim to adjust preferential parameters by considering personal judgments and constraints on the one side and following the common direction of the decision-making

group at the same time. A generic consensus-seeking procedure [40] is presented in Figure 17. It is combined with the aggregation-disaggregation analysis [41].

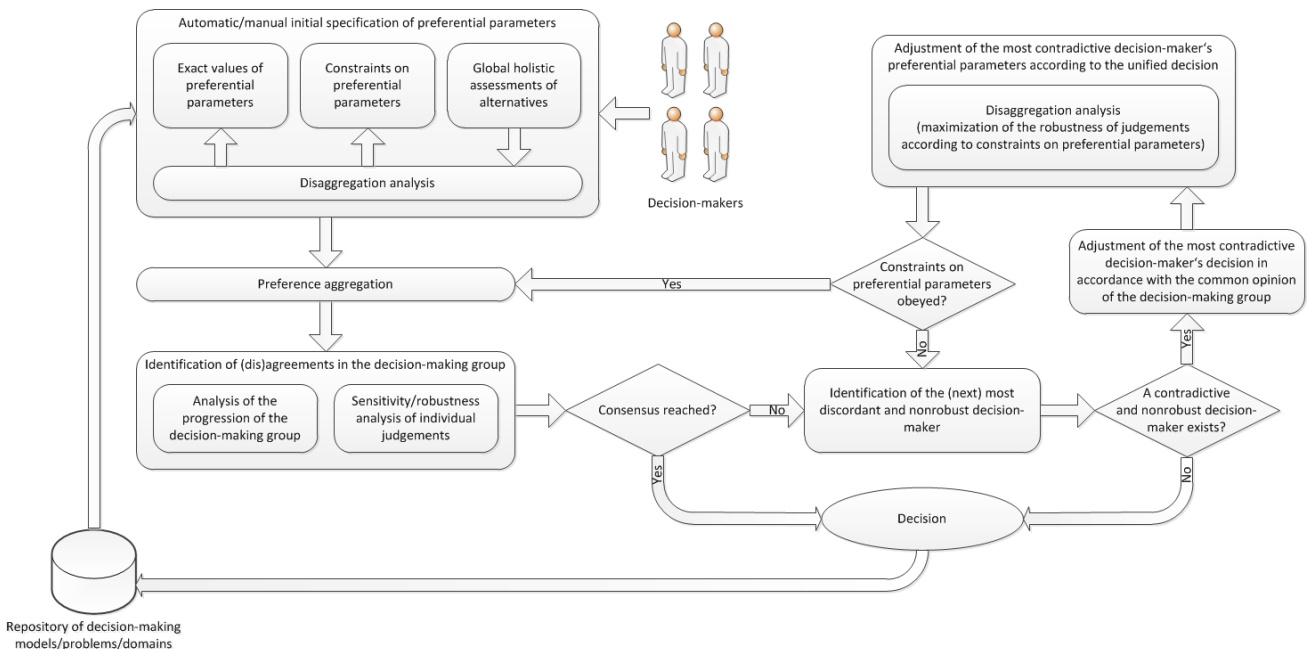


Figure 17 – Generic group consensus-seeking procedure incorporating the aggregation-disaggregation analysis.

In most cases, the consensus-seeking procedure is able to achieve full convergence towards a consensual solution by iteratively adjusting the preferential parameters of contradictory group members within the defined constraints and in accordance with the collective opinion of the decision-making group [42]. It is essential for the procedure to implement appropriate proximity metrics [40] [43] to identify (dis)agreements in the decision-making group as well as a set of robustness metrics [44] to assess the robustness of individual judgments.

2.5.3 Delphi processes

Delphi is a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem [45]. It is useful where the opinions and judgments of experts and practitioners are needed, but time, distance and other factors make it unlikely or impossible for the panel to work together in one meeting in the same physical location [46].

Delphi is suitable for applications in creative thinking, asynchronous communication, and group problem-solving. It is primarily designed to predict future events but can be adopted for different purposes, such as identification of alternative solutions, specification of common goals and values, information gathering, and MCDM. Its key characteristics are the anonymity of the participants, structured information flow of contributions made by the individuals, regular feedback, moderation, and asynchronous interaction. In a Delphi process, judgments of individual group members are aggregated over several consecutive iterations (rounds) so that participants can modify and unify their opinions on the basis of the provided feedback. Delphi hence consists of a sequence of questionnaires, in which statistics are calculated based on the answers of the last iteration. Compiled statistical information

allows each group member to analyze, reconsider, and improve personal judgments. In addition, a human facilitator is involved to aid group members in understanding their common objectives and to help identify and eliminate conflicts. In general, the Delphi process is continuously iterated until consensus is determined to be achieved, but the payoff usually begins to diminish after the third round [46]. For this reason, each Delphi study must be properly organized [47].

A generic Delphi procedure for MCDM has been defined and can be applied in practice [40]. It is shown in Figure 18.

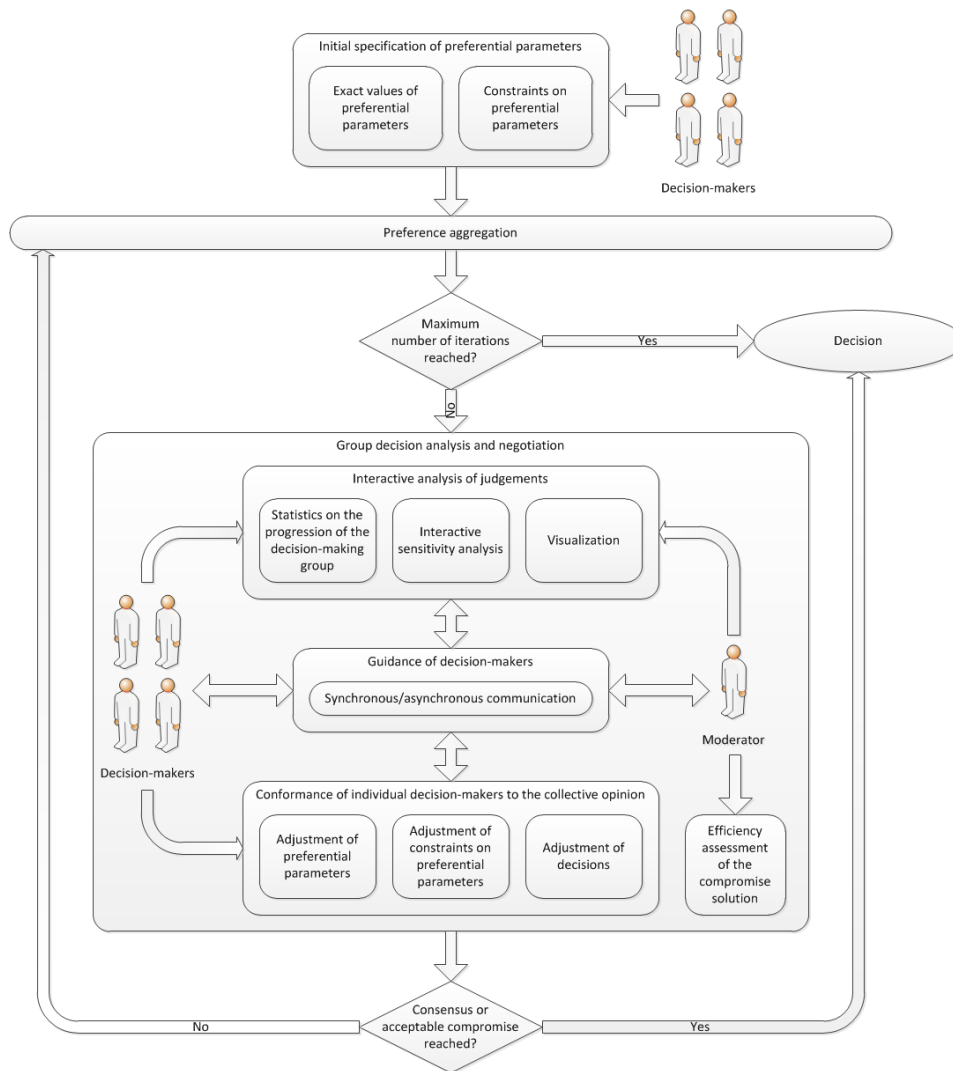


Figure 18 – Generic Delphi procedure.

2.5.4 Synchronous and asynchronous communication

In addition to group decision-making, problem-solving, and analytical MCDM functionalities, facilities for computer-mediated communication [48] have to be provided to support the exchange of CTI information and coordination between EPES operators and CERTs. A chat,

teleconferencing, or information-sharing tool may be integrated to facilitate the discussion among EPES stakeholders about the impacts of cybersecurity incidents.

Communication and collaboration software has become very popular and widespread in the last few years. There are many general-purpose tools available, such as email clients, chat tools, and teleconferencing systems (e.g., MS Teams). Many specialized tools also offer features that can be beneficially used for the purposes of collaboration and cooperation, although their primary features are related to different kinds of (possibly non-collaborative) tasks. An example of such a tool is MISP, which can facilitate collaboration via communities as well as communication through the use of sharing mechanisms. EPES operators, SOCs, and CERTs can use MISP to share similar incidents of different severity. Artifacts of TheHive [49], including IOCs to be shared, need to be mapped against the MISP attributes (type and category) [50].

In general, we can distinguish between synchronous and asynchronous communication. The first is the exchange of information between two or more people in real-time. Technologies that facilitate it include video conferencing and instant messaging [51]. The latter refers to any kind of communication where there is a delay between when a message is sent and when the person on the other end receives and interprets it. This kind of communication may be supported by email, text messaging, asynchronous meetings, and tools for asynchronous problem-solving (e.g., Delphi-based tools).

2.6 Incident response modeling

Incident response modeling includes incident classification, workflow modeling, and automated playbook execution. Incident classification involves categorizing incidents based on severity and impact, while workflow modeling involves creating a sequence of steps or actions that should be taken during incident response.

Response modeling aims to provide a structured and repeatable process for the incident response that can be customized and automated to suit specific use cases. Developing incident response playbooks will be more efficient and effective by utilizing pre-defined and standardized models. This seeks to reduce the time required to respond to incidents and increase the consistency of incident response across different scenarios or even different organizations and stakeholders in case of knowledge sharing and collaborative response.

In this section, we overview some of the standards we aim to utilize or reuse for incident response modeling.

2.6.1 BPMN 2.0 overview

The Business Process Model and Notation (BPMN) 2.0 introduced in 2011 is the successor of the initial version of the BPMN language [52]. It was introduced to address some of the limitations and shortcomings of the earlier version, such as enhancing support for process execution and automation, including resources for collaboration, expanding event types and modeling of data objects, and complex workflows for more accurate and detailed representation of the processes.

BPMN is a graphical language for representing and modeling business processes and workflows in various domains. The BPMN 2.0 specification offers a standardized syntax and semantics and provides guidelines to develop process diagrams, facilitating communication and collaboration among stakeholders in workflow management.

The ability of graph-based representation of workflows is one of the fundamental features of BPMN. This allows for simplifying complicated processes and analyzing the workflow since it enables a visual depiction of the various activities, events, and tasks involved. The specification contains details on the elements of BPMN diagrams, such as events, activities, and gateways, as well as more advanced concepts, such as data objects, message flows, and choreography diagrams, represented using various shapes and symbols.

Another important aspect of BPMN is its human- and machine-readability. This means that BPMN diagrams can be utilized not only as a graphical aid for understanding and communicating workflows but also as a foundation for automated workflow management and execution. The representation of the workflows facilitates the automation plan by utilizing software tools to interpret and execute actions in the workflow model. Moreover, the machine-readability of BPMN diagrams facilitates the integration of workflows with other systems, enabling the development of an interconnected system.

In the area of modeling cybersecurity response, BPMN is a proper approach and is vastly used by different organizations. Enterprises can create a repeatable procedure for handling cybersecurity incidents by utilizing BPMN to express processes required in detection, response, and recovery steps. Organizations also have the opportunity to link their incident response processes with other IT and business processes through the use of BPMN in cybersecurity response modeling, resulting in a more coordinated and effective response.

2.6.2 CACAO Security Playbooks 2.0 overview

Collaborative Automated Course of Action Operations (CACAO) specification is a standardization effort by OASIS to define shareable playbooks considering workflow automation, for which version 2 is released on 21 Feb. 2023 [53]. A CACAO playbook is a type of security orchestration workflow that includes a set of steps for completing specific response tasks. These playbooks can be triggered by a manual or automated event or observation. They are intended to instruct users or organizations on how to handle security incidents or attacks. Playbooks can also include other playbooks, allowing the modularity and composition of multiple playbooks of varying levels of complexity.

CACAO playbooks are categorized into two types: executable (actionable) playbooks and playbook templates. Playbooks that can be executed immediately without modification are known as executable playbooks, whereas playbook templates only provide examples of actions related to a specific security incident or operation. Depending on the type, playbooks serve different functions in the incident management lifecycle. For example, a detection playbook, contains the workflow required to detect a known security event or malware, whereas a mitigation and remediation playbook assists in dealing with the direct consequences of a security incident.

The CACAO specification defines different types of playbooks regarding the incident management lifecycle, each with its own distinct purpose. All of the playbook types are detailed in the specification. The most common types are detection playbooks, mitigation

playbooks, and remediation playbooks. Overall, CACAO playbooks are a valuable tool for security incident response and recovery and can help organizations in responding to security events quickly and effectively.

Figure 19 [53] illustrates the overview of CACAO playbook structure. The activities and logic that will be performed when a playbook is executed are defined by several building components. The playbook metadata includes crucial details about the playbook, such as whether it is an executable playbook or a template, the kinds of operational tasks it covers, and a general summary of the playbook. This information provides a quick overview of the playbook's purpose. Other useful information, such as impact, severity, and priority, can also be added. It is required to define the first step via the `workflow_start` attribute if a playbook comprises a workflow with multiple steps. Overall, this information can ensure that a playbook is utilized correctly in incident response and recovery scenarios and is essential for human readability toward understanding the purpose and function of a playbook.

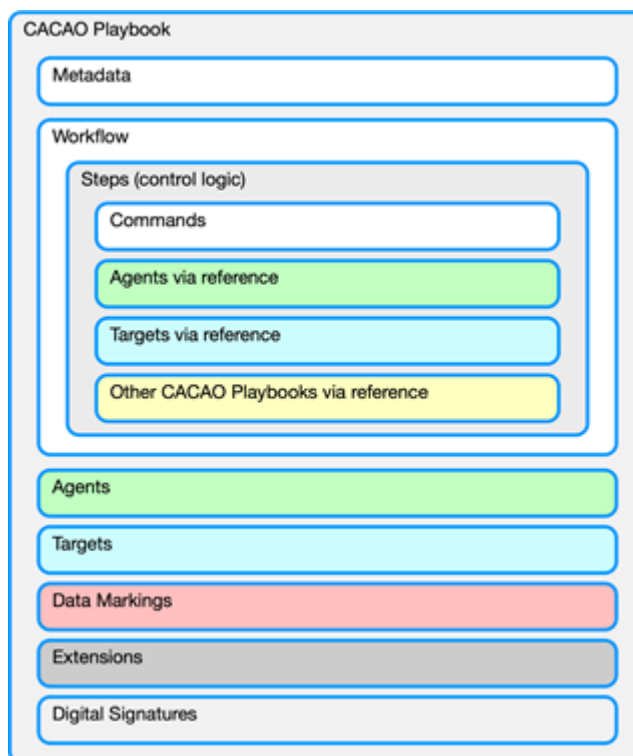


Figure 19 – CACAO playbook structure.

The main workflow of a CACAO playbook described by the CACAO specification contains several steps that are triggered by automated tools. Each step offers helpful properties for automatic processing as well as common attributes that connect multiple steps. While conditional steps and parallel steps provide a range of combinations, playbook steps allow the execution of other playbooks. The playbook is made executable using commands, for example, bash and SSH commands. Targets have detailed information on the entities carrying out workflow commands. The CACAO data model additionally provides data markers, such as TLP categorization protocol, to define handling and sharing requirements. If the basic CACAO model is insufficient, custom extensions can also be developed, though as of the time of writing, there is no official method for sharing extensions.

2.6.3 SAPPAN vocabulary overview

The SAPPAN (Sharing and Automation for Privacy Preserving Attack Neutralization) EU project has developed another vocabulary and process for modeling incident response and recovery steps using semantic web technologies [54] [55]. This approach focuses on the capturing and sharing of knowledge as well as the basic modeling for recommendations for steps to aid human operators and automation of actions without human intervention.

The methodology and structure of the playbooks in SAPPAN are relatively similar to CACAO's proposed methodology; However, SAPPAN follows a more flexible but less pragmatic approach to changes in the methodology and structure. The flexibility in modeling confidentiality levels for different resources facilitates access control, data sanitization, and the development and publication of shareable playbooks.

Developing SAPPAN vocabulary utilizes semantic web standards: RDF, RDFS, and OWL 2. It potentially provides the opportunity for easy integration of a knowledge base that follows a similar specification. It still lacks support regarding the automation of the steps. Although the missing automation vocabulary of SAPPAN (thresholds, automation privileges, impact scores, confidence scores, and risk metrics) is identified in the SAPPAN Response Automation Prototypes and will be integrated into the SAPPAN vocabulary.

The SAPPAN approach emphasizes knowledge representation, sharing, and automation to improve incident response and recovery. The vocabulary and process developed by the project can aid in the creation of incident playbooks that can be shared and executed by both humans and machines. The SAPPAN approach is an example of how semantic web technologies can be utilized to improve cybersecurity incident response and recovery.

3 Methodology

In this chapter, we define the methodology that EPES stakeholders can follow to develop incident response procedures. These procedures are the key result of the D6.8 deliverable and are presented in the next section. The methodology is compliant with the NIST Incident Response Framework [6]. It covers:

1. different types of cybersecurity incidents;
2. various levels of severity of incidents, resulting in different rules for the coordination and reporting to CERTs;
3. specifics of individual pilots and national legislation;
4. tools and data structures for the reporting of incidents to CERTs;
5. all incident response phases;
6. alignment with the overall incident response strategy and plan.

The methodology introduces the MCDM model and the decision-making process, allowing EPES stakeholders to assess the impacts of detected incidents. These impacts are the basis for selecting and applying appropriate incident response procedures, coordination rules, reports, and tools. Also, the vocabulary and notation for playbook modeling are prescribed.

3.1 Overview of the applied methodology

Rules and tools for the coordination of EPES operators and reporting to CERTs must consider several aspects:

- the general incident response policies and plans of EPES stakeholders;
- the general rules and procedures of national CERTs;
- national legislation;
- specifics of particular types of cyber incidents (e.g., malware, phishing, SQL injection, DDoS, and other) and incident response procedures used to handle these incidents.

For this purpose, we defined a comprehensive methodology based on the NIST Incident Handling Guide [6]. It incorporates three major phases:

1. **Create an incident response policy:** This is a precursor to the incident response plan that lays out the organizational framework for incident response. It specifies what EPES operators should consider a security-related incident and who is accountable for incident response. It identifies responsibilities and roles, as well as documentation and reporting requirements.
2. **Define an incident response plan:** An incident response plan is not only a list of steps to perform when an incident happens. It is a roadmap for the incident response program, including short- and long-term goals, metrics for measuring success, and requirements for incident response roles and teams.
3. **Develop incident response procedures:** These are the detailed steps that incident response teams will use to respond to an incident. They should be based on the incident response policy and plan and have to address all stages of the incident response lifecycle.

These three phases are sequential. The incident response policy phase corresponds to the highest organizational level and sets the overall picture. The incident response plan must

align with the policy, while the development of procedures should comply with both of the above phases. We provide a detailed definition of the incident response policy for EPES operators in Section 3.2 of this document and describe the incident response plan in Section 3.3. Here, we specify the steps for developing incident response procedures. NIST's incident response lifecycle, depicted in Figure 20 [6], provides the basis to do this.

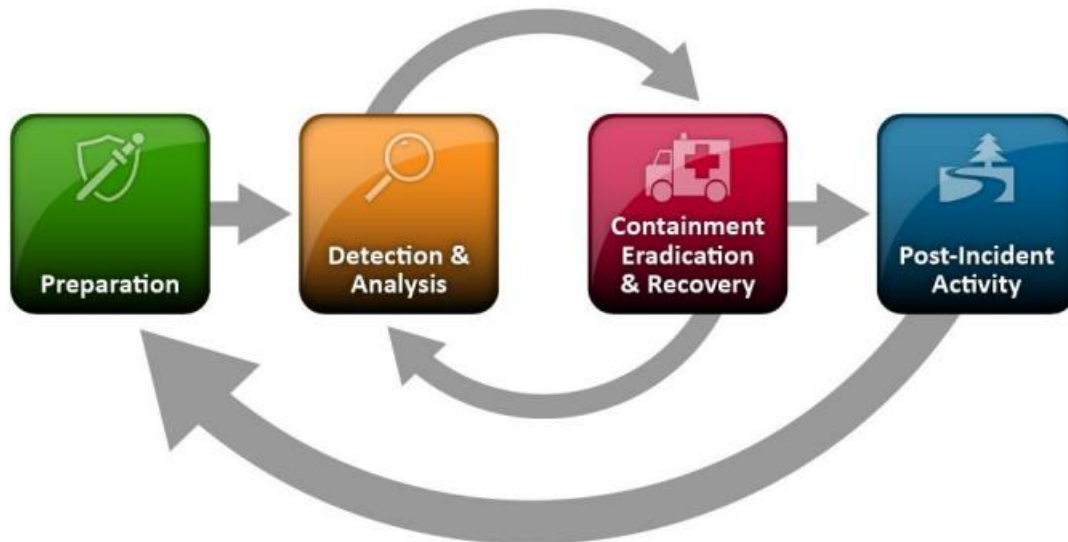


Figure 20 – Incident response lifecycle.

According to the proposed methodology, the definition of incident response procedures, coordination rules, and reporting mechanisms consists of seven steps. They are aligned with NIST's stages and are detailed below. They result in several outcomes:

1. a set of rules for the coordination of EPES operators and for reporting to CERTs when a cyber incident occurs, based on the classes of cybersecurity incidents, the effects and consequences of these incidents, and the expected outcomes of implemented rules;
2. playbooks – process diagrams of procedures for incident handling, coordination, and reporting;
3. communication strategies and information-sharing mechanisms;
4. standard reports and data structures for the exchange of information about incidents;
5. rules for decision-making and an MCDM methodology that assesses the impacts of detected relevant incidents in correlation with compromised assets and maps them to incident impact levels as prescribed by CERTs and national legislative rules.

3.1.1 Steps for pilots

CyberSEAS pilots (ITA, SLO&CRO, ROM, FIN, and EST) followed the seven proposed steps to define national incident response procedures and rules. The resulting procedures and rules are the primary outcome of D6.7. They are thoroughly presented in Section 4.

The sequence of steps can be read as instructions for pilots. They are related to the first three stages of NIST's incident response lifecycle. Details are described in Sections 3.1.2, 3.1.3, and 3.1.4 of this document. Figure 21 depicts the sequence of steps.

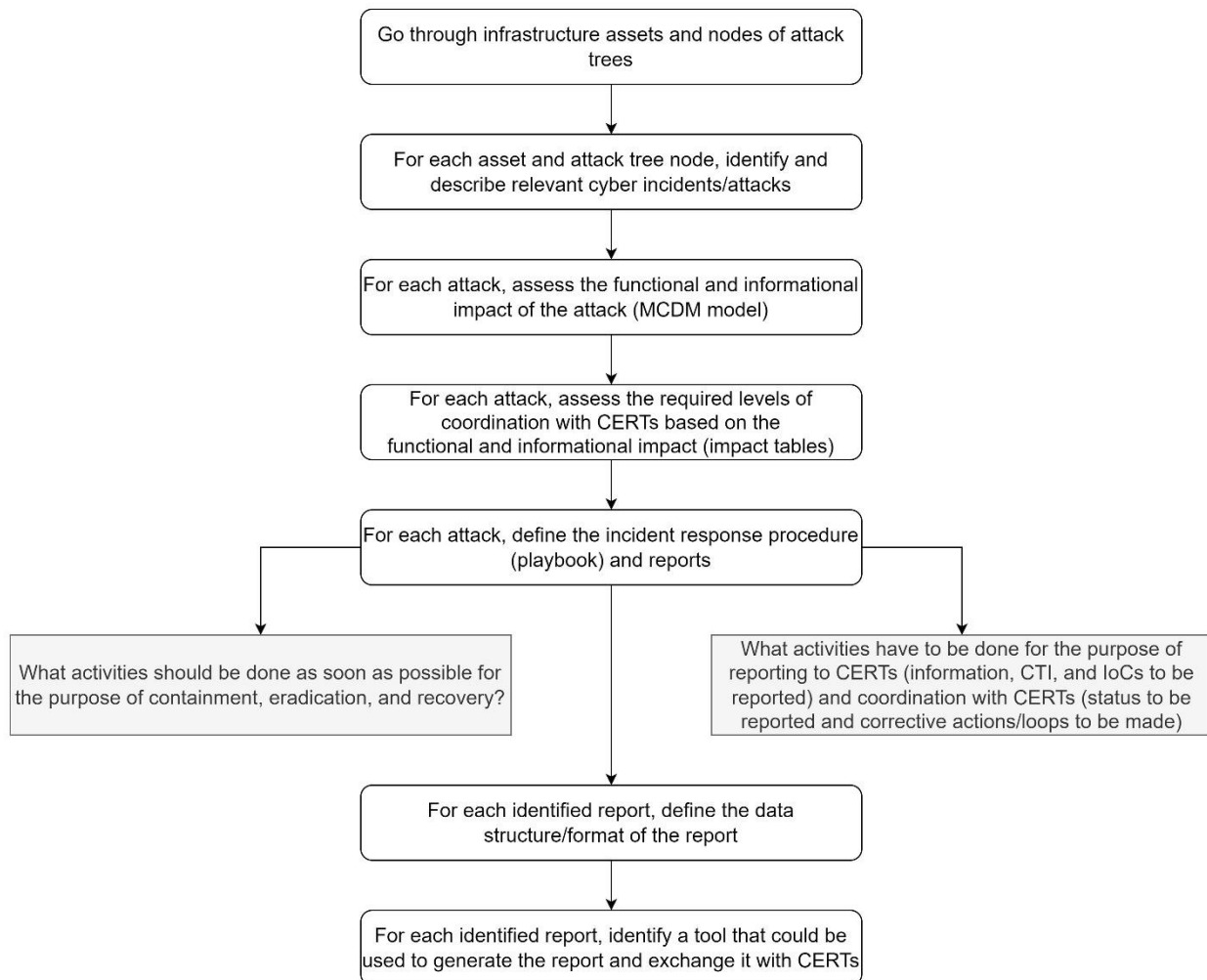


Figure 21 – Steps of the methodology to define incident response procedures and rules.

Two strategies can be applied. In the top-down approach, one general incident response procedure is initially defined that corresponds to the regulatory framework and high-level rules of national CERTs. It is then assessed and adjusted for particular attack scenarios, such that specific procedures are obtained corresponding to different types of incidents. On the other hand, the bottom-up approach starts with the definition of a specific incident response procedure for each attack scenario. Common characteristics are then identified, based on which all individual procedures are unified into a general procedure.

3.1.2 Mapping of incidents to response procedures

The general incident response, coordination, and reporting procedures are often efficient. However, in some cases, it might be insufficient to follow common rules and legislation without considering the specifics of different types of incidents. Each of them may require individual response actions and variations in reporting. A significant part of the preparation stage is thus to map possible incidents to response procedures. The mapping addresses several entities that are part of the EPES infrastructure. These entities include:

- MITRE ATT&CK assets and attack techniques,



- CyberSEAS assets and cybersecurity incidents based on pilot attack scenarios,
- general CyberSEAS vulnerabilities, and
- detected cyberattacks (in real-time, based on SIEM or other cyber threat detection systems).

Figure 22 provides a couple of mapping possibilities. The first approach maps specific attack techniques related to MITRE ATT&CK assets to possible incident response procedures, the second takes types of vulnerabilities as the source for mappings, and the third maps security-related events of pilot attack scenarios.

1. MITRE ATT&CK assets and cyber-security events

| ID | Assets | Domains | Zones | Layer | Class | Gather Victim Identity Information | Gather Victim Org Information | Phishing for Information |
|-------------------------------------|------------------------------|---------|-------|-------|-------|------------------------------------|-------------------------------|--------------------------|
| 50 | Distribution system operator | D | O | Human | Human | Y | Y | Y |
| Proposed response procedures | | | | | | IR.1, IR.5, IR.8, IR.10 | | |

2. CyberSEAS vulnerabilities

| Vulnerability | CyberSEAS vulnerability class | Proposed response procedures |
|--|-------------------------------|------------------------------|
| System permits unauthorized installation of software or firmware | Human/Organisational | IR.1, IR.10, IR.11 |

3. Pilot scenarios

| Pilot | Scenario no. | Event no. | Event description | Proposed response procedures |
|---------|--------------|-----------|--|------------------------------|
| SLO-CRO | 3 | 1 | A threat agent performs social engineering technics to obtain credentials leading to unauthorized access | IR.1, IR.2 |

Figure 22 – Mapping of security events and vulnerabilities to incident response procedures.

3.1.3 Analysis of incidents

The extent of coordination and reporting to CERTs depends on the severity of the detected incident. Therefore, each incident must be assessed so that the assessment determines the scope, impact, and extent of the damage caused by the incident. Several variations of each incident response procedure are then defined, where each variant corresponds to a certain impact level. The higher the impact level, the more frequent, comprehensive, intense, and strict coordination and reporting are required. Two key assessments pertain to the functional impact (shown in Table 1) and the informational impact (provided in Table 2). Each impact level has a well-defined consequence and must trigger the corresponding CERT response. The overall response is the union of responses that are requested for individual (i.e., functional and informational) criteria.

Table 1 – Assessment of the functional impact for the coordination with CERTs.

| Functional impact | Definition | CERT response |
|-------------------|---|--|
| None | No effect on the organization's ability to provide all services to all users. Only a single or few personal devices in the IT infrastructure are compromised (e.g., PC, laptop, workstation, etc.). | Create a ticket and assign it for remediation. |
| Low | Minimal effect: the organization can still provide all critical services to all users but has lost efficiency. | Create a ticket and assign it for |



| | | |
|---------------|--|---|
| <p>Medium</p> | <p>Several personal devices in the IT infrastructure are compromised. Some OT devices (e.g., metering device, IoT sensor, etc.) may also be affected.</p> <p>The organization has lost the ability to provide a critical service to a subset of system users. Network and server IT infrastructure is compromised (e.g., application server, DB server, etc.). Critical control, management, and transmission systems/devices in the OT infrastructure (e.g., SCADA system, etc.) may be partially affected.</p> | <p>remediation, notify CIO/CISO.</p> <p>Initiate full CERT, involve CIO/CISO.</p> |
| <p>High</p> | <p>The organization is no longer able to provide some critical services to any user. Large impact on the DSO IT infrastructure and/or OT infrastructure.</p> | <p>Initiate full CERT, involve CIO/CISO and higher management. Activate the disaster recovery plan.</p> |

Table 2 – Assessment of the informational impact for the coordination with CERTs.

| Informational impact | Definition | CERT response |
|----------------------|---|--|
| None | No information was accessed, exfiltrated, changed, deleted, or otherwise compromised. | No action is required. |
| Low | Public or non-sensitive data was accessed, exfiltrated, changed, deleted, or otherwise compromised. | Notify data owners to determine the appropriate course of action. |
| Medium | Internal Information was accessed, exfiltrated, changed, deleted, or otherwise compromised. | Notify CIO/CISO. CIO/CISO will work with legal representatives, management, and data owners to determine the appropriate course of action. |
| High | Protected data was accessed, exfiltrated, changed, deleted, or otherwise compromised. | Notify CIO/CISO and higher management. CIO/CISO will work with legal representatives to determine the appropriate notification requirements. |

In most cases, it is sufficient to assess incidents qualitatively on functional and informational criteria. However, a more comprehensive MCDM (Multi-Criteria Decision-Making) impact assessment model can be used. We define this model in detail in Section 3.4. It considers almost 20 criteria, which are mostly taken from the NESCOR methodology for cybersecurity failure scenarios and impact analysis for the electric sector [56]. When we work with so many criteria, we aggregate individual criteria-wise assessments into the overall impact score. A hierarchical qualitative aggregation model based on the DEXi method was already briefly

shown in Figure 16 in Section 2.4.2. Alternatively, a quantitative additive value model can be applied. We will introduce it in Section 3.4 and demonstrate it in Section 6.

It should be noted that each national CERT might use a specific impact scale. In Slovenia, for example, incident impact levels are denoted and handled according to the Slovenian Information Security Act [57]. Possible levels are C1 (critical incident), C2 (very important incident), C3 (important incident), C4 (moderate incident), C5 (minor incident), and C6 (security event). This means an additional mapping between the assessed impact score and the national impact scale is necessary.

3.1.4 Definition of playbooks and rules for incident response and reporting

This activity is the central part of the presented methodology. It produces playbooks and rules corresponding to the containment, eradication, and recovery stages of the incident response lifecycle defined by NIST. It may result in some general rules and recommendations for cooperation and reporting in the case of incidents. However, the preferred outcome is a set of thoroughly defined and detailed incident response procedures aligned with pilots' attack scenarios, the infrastructure of EPES operators, and national legislation.

Each incident response procedure consists of a sequence of actions. Several action types must be covered. They are aligned with NIST's framework and are defined in Table 3.

Table 3 – Types of incident response actions.

| Action type | Description |
|-----------------------|--|
| Preparation | The preliminary actions required as a prerequisite to perform other actions |
| Identification | The actions required to identify, analyze, and/or investigate the incident |
| Containment | The actions required to prevent the incident or event from spreading across the network |
| Eradication | The actions that are required to completely wipe the threat from the network or system – after the incident has been contained, all elements of the incident are removed from the environment |
| Recovery | The actions required to bring back the network or system to its former functionality and use – involves the steps required to restore data and systems to a healthy working state allowing business operations to return |
| Internal coordination | The actions required to coordinate the incident response internally (e.g., within the operator's system), as well as for internal reporting |
| External coordination | The actions required to coordinate the incident response with CERTs, as well as for reporting to CERTs |
| Lessons learned | The actions that improve the knowledge about the incident enabling to respond more efficiently in the future |

Incident response procedures may be general or specific. In the latter case, they address individual incident types, such as phishing, DDoS, SQL injection, etc. It means a separate IR procedure is defined and used for each type of incident. Each IR procedure may also have several variations. Depending on the impact of the incident, some actions are unnecessary or may be simplified.

A standard notation and vocabulary should be used to model incident response procedures (playbooks). In this way, playbooks can be easily comprehended, shared, and exchanged. They can also be partially unified, reused, and automated. As explained in Section 2.6, the BPMN notation and the CACAO or SAPPAN vocabularies are advised. Section 3.5 provides additional details on modeling. Figure 23 shows an exemplary malware incident response procedure modeled in the BPMN notation.

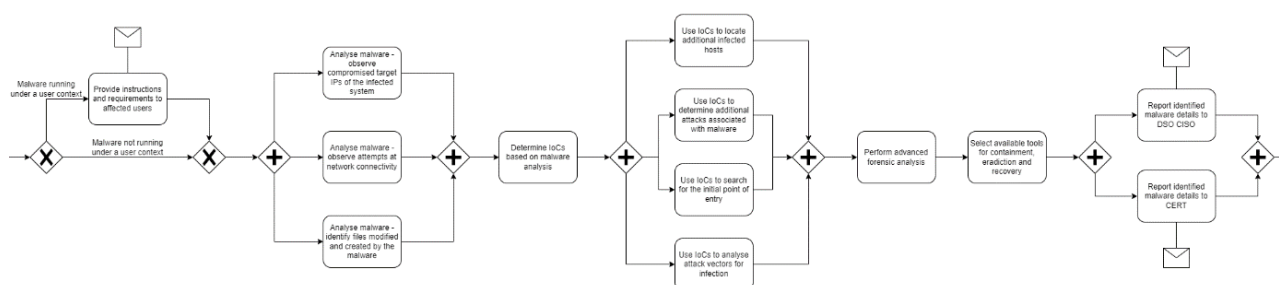


Figure 23 – Example of a standardized malware incident response procedure in the BPMN notation.

In relation to incident response procedures, we separately define standard reports for CERTs. We align these reports with particular reporting activities defined in IR procedures. Reports should be adjusted for different types of cybersecurity incidents and based on standard data structures and formats. These structures are prescribed by CERTs.

Because reports and IoCs are exchanged between SOCs and CERTs, appropriate sharing platforms and tools, such as MISP (Malware Information Sharing Platform), and CTI (Cyber Threat Intelligence) exchange standards and technologies, such as STIX and TAXII, should be utilized. They were described in Sections 2.2 and 2.3. In addition, reporting tools can be based on the capabilities and functionalities of SIEM systems and data management systems.

3.2 Incident response policy

In this section, the cybersecurity management model developed by KYBER-ENE is briefly described. It is worthwhile to mention that KYBER-ENE is a program with the aim at developing cybersecurity in the Finnish energy sector. The model indicates the following elements for managing cybersecurity incidents.

Team assembly and information sharing: Any organization must identify and commit necessary key personnel who are responsible for cybersecurity development of the organization as well as support groups with a positive attitude towards cybersecurity development.

Studying reasons and prerequisites for cybersecure operation: Understanding cybersecurity holes and weaknesses is necessary to improve the current situation.

Map and manage critical systems, interfaces, risks and threats: Identifying critical systems, interfaces, risks and threats for the business and managing the life cycle of the critical systems in a good fashion are critical for security and continuity of services.

Build protection instructions: In cybersecurity studies, the most important threats for the system should be identified. Then, the most important operating methods that improve the protection against cybersecurity threats are devised to increase cybersecurity. The most important security practices include but not limited to secure communication architecture, secure remote connections, access rights management and disruption situation management and training.

Develop contingency plans: The critical systems should have already developed plans to ensure predefined contingencies do not cause significant losses or disruption to the society functions. The plans can be based on providing enough spare for critical parts of the system.

Recognize violations and react accordingly: The systems for identifying cybersecurity breaches are divided into two main types namely the systems that analyze network traffic and the systems that analyze terminal device events. However, in the energy sector, the systems cannot identify all attacks. In order to ensure cybersecurity, in addition to the systems, suspicious contacts, emails, contacts on social media channels, phone calls, random conversations in public environments like airports as well as suspicious company visitors, sales representatives, subcontractors deputies and educational institution visitors should be observed carefully.

Report and minimize damages: Documentation of events is necessary to learn from cybersecurity incidents that have already taken place in the past. It is also valuable to be familiar with previously carried out attacks regarding other companies. These help to know about the tools attackers have used and the traces they left.

Restore normal operation: Once a cyber incident is revealed, having accurate information about the infected systems and the time they became contaminated is required for a fast restoration process. Having an understanding of a clean normal state is also necessary. This includes but is not limited to the software version information, installed patches, system settings, and backup and recovery systems with instructions.

Interested readers are referred to CyberSEAS D6.1 for more detailed information about the policies for managing incidents in different European countries.

3.3 Incident response plan

In this section, a brief overview of an incident response plan provided by the National Cyber Security Centre Finland is provided. It is important to note that the incident response plan offers general guidelines while more specific detailed incident response plans are developed by organizations according to their technological and operational environment. According to the incident response plan provided by the National Cyber Security Centre Finland, incident management is done in five main steps, including preparation, detection, containment, recovery, and review. The five steps are briefly described below.

Preparation step: In this step, the aim is to protect against incidents, reduce severity of incidents and enable fast recovery after incidents. In this step, organizations are recommended to assess their readiness using cyber security evaluation tools and develop

their incident response plan. In order for organizations to be well prepared, different measures categorized into administrative measures and technical measures.

Detection step: In this step, the aim is to ensure that the organization is able to detect cyber security incidents. There is a diverse range of approaches to detect an attack since there are many ways an attacker can use to penetrate to a system. Observation of an unexpected process and observation of an alarm are two sample ways to detect an attack.

Containment step: In this step, the aim is to investigate the incident. During an incident, it is important to keep a precise event log of all taken measures with information about the party that implemented the measure and timestamp. During this step, documentation is crucial. It is important to document any potential evidence with detailed information about the body that gathered the data, what the data was and when and how the data was gathered. The documents and logs facilitate the investigation as well as cooperation with police and information security investigators. In the containment step, some immediate measures are necessary to protect the critical data in the environment, stop the malware from spreading, prevent the attackers from gaining a foothold in the network and prepare for the next step which is recovery.

Recovery step: This step begins from the systems which are the most critical to the business. In this step, infected systems are restored from backups. It is worthwhile to mention that the process should be done as safely as possible to ensure that the attacker cannot get back into the system. In addition, login information of all of the potentially infected IDs is changed so that the attacker can no longer use the IDs to access the systems. In order to avoid similar attacks in the future, it is recommended to make user login requirements stricter. Once the systems are restored and the IDs are changed, database can be restored from a backup copy to invalidate potential changes made by the attackers.

Review step: In this step, the measures taken during the event are studied to see how the plans and the security level can be improved. In the study, root causes of the incident and effectiveness of the organization protection plan are examined carefully. It is important to note that sharing the most important lessons learned from incidents to help other organizations can be part of the step.

Interested readers are referred to CyberSEAS D6.5 for more detailed information about the guidelines for incident management and incident response plan development in different European countries.

3.4 MCDM model for impact assessment

After an incident is detected, we must assess its impact because it determines the required level of coordination with EPES stakeholders and the rules for reporting to the CERT. It thereby provides the basis for choosing the appropriate incident response procedure.

This section introduces the MCDM model for impact assessment. It is an integral part of a broader decision-making process. This methodology also underlies the selection of mitigation measures. Therefore, we define and reuse it for two CyberSEAS tasks: T4.4 and T6.4. A detailed description is available in the D4.8 deliverable. Here, we summarize only the fundamental concepts for T6.4.

The decision-making process consists of two sequential phases. It starts with the incident impact assessment phase and then continues with the follow-up mitigation assessment and implementation phase. Only the first phase is relevant for T6.4. Figure 24 depicts the flow of its activities.

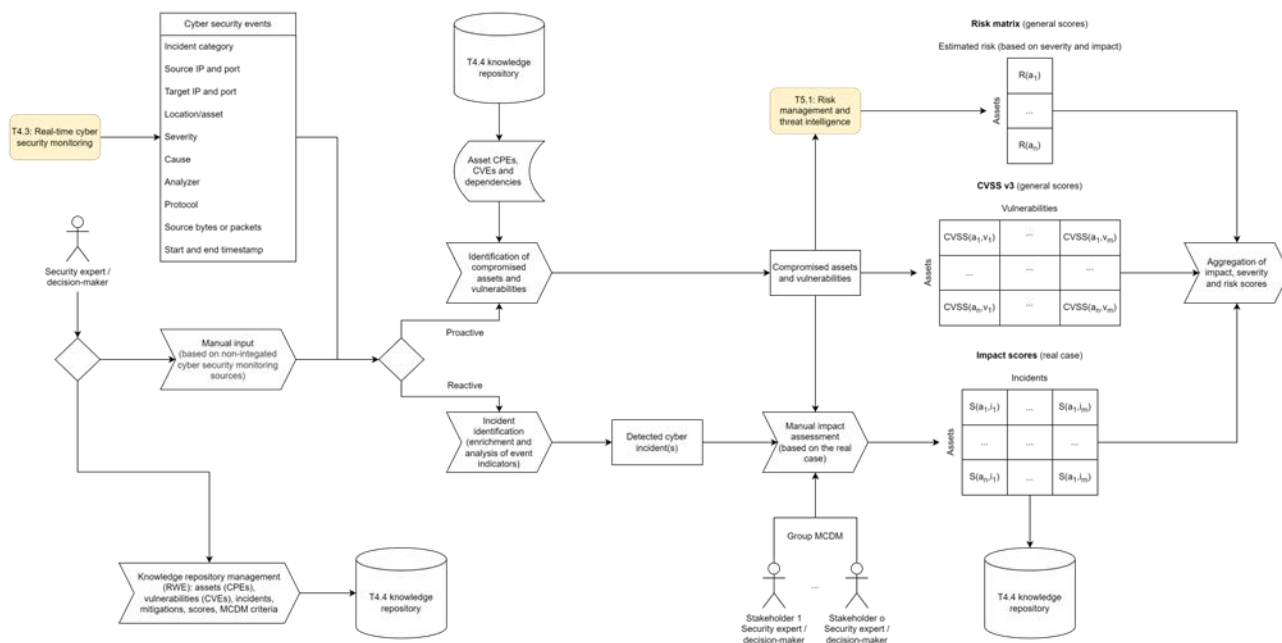


Figure 24 – Incident impact assessment phase of the decision-making process.

The decision-making process starts with cybersecurity data gathering and investigation. Information on security-related events can be obtained from a SIEM system, but integration with SIEM is not mandatory, which means that MCDM analysis can be based entirely on manually provided and processed information. Also, if data is imported from SIEM, no real-time data flow is required. The information, which is obtained from SIEM, may include (but is not limited to):

- network flow data, such as the number of transmitted packets and the timestamps of the first and last received packets;
- source and target IPs and ports;
- protocol type, e.g., TCP/IP (Transmission Control Protocol/Internet Protocol);
- the triggered correlation rules, if applicable;
- type of the detected incident, if applicable;
- the magnitude of the incident, if applicable, and based on the capabilities of the used SIEM system (e.g., IBM Security QRadar SIEM [58] can assess or estimate incident relevance, severity, and credibility in some cases).

Because SIEM information is limited, the enrichment and analysis of attack indicators are part of the information intelligence phase. Based on the enriched information and reported target IPs, the security expert can identify compromised assets and actual cybersecurity incidents. At this point, two different strategies can be taken, which can also be combined. The first possibility is a reactive strategy. In this case, only actual incidents that are detected by SIEM or other cybersecurity threat detection systems are considered. The impact of these real-time incidents is assessed by decision-makers. The second strategy is proactive. In this case, the targeted assets are the basis for assessing the impact of relevant vulnerabilities that

apply to these assets, either directly or indirectly through connections and dependencies. By following the mapping mechanism defined in D4.8, CVEs (Common Vulnerabilities and Exposures), CVSS (Common Vulnerability Scoring System) scores, and MITRE ATT&CK techniques are obtained. We generally get a couple of combinations, of which each combination consists of an asset, an incident that compromises this asset, and one or more standard MITRE ATT&CK techniques employed to realize this incident.

From the proactive strategy, we automatically obtain the average CVSS score, which represents one standard factor involved in the impact assessment. From the reactive strategy, we can take the incident magnitude, if it can be provided by the SIEM system. If it is available, it is considered the second impact assessment factor. Otherwise, it might be discarded from the assessment. These two precalculated objective criteria are then combined with several additional criteria that are considered by the decision-maker to make impact assessments. Most of these criteria are taken from the NESCOR methodology for cybersecurity failure scenarios and impact analysis for the electric sector [56]. They also address the relevance of compromised assets for the EPES infrastructure and the current state of security or resilience (e.g., applied or installed patches, updates, and security policies). The set of criteria for the incident impact assessment is shown in Table 4.

Table 4 – Incident impact assessment criteria.

| High-level criteria | Sub-criteria |
|---------------------|---|
| Measured impact | SIEM magnitude CVSS V2.0/V3.1 |
| Safety concern | Public safety concern Workforce safety concern |
| Ecological concern | |
| System scale | |
| Impact on EPES | Negative impact on generation capacity Negative impact on energy market Negative impact on transmission system Negative impact on customer service Destroys goodwill toward utility Privacy loss of stakeholders |
| Financial impact | Financial impact on utility Restoration costs Immediate economic damage Long term economic damage |
| Asset criticality | Resilience of the compromised asset Relevance of the compromised asset |

The MCDM impact assessment is, in its most basic form, performed by an individual decision-maker. However, several EPES stakeholders might be targeted by a single attack due to cascading effects, connected assets, and participation in common energy supply chains. Appropriate group decision-making procedures are therefore applied that allow many stakeholders to come to the collective impact assessment. The recommended approach is the Delphi technique, which also supports asynchronous communication and coordination.

Based on asset dependencies, compromised assets are organized into several levels. The impact assessments may initially be performed by decision-makers only for directly attacked assets on level 1. The scores of assets on lower levels may then be approximated by means of the Level Impact Reduction Index (LIRI). In its basic form, LIRI is a coefficient by which the scores are constantly reduced at each consecutive level. It gives approximations for lower dependency levels, which means that approximated scores must be checked by decision-makers and properly adjusted if required.

In general, the strength of any DSS is that it can provide the decision-maker with several different MCDM methods. The decision-maker can choose to use any of these methods according to personal preferences, requirements, and experience. For the assessment of incident impacts, two MCDM methods will be supported:







- additive value function (quantitative) and
- DEXi (qualitative).

Let $s^l(A_l)$ denote the impact score of the l -th incident and w_j the weight of the j -th criterion. The overall impact score of the l -th incident is then calculated with the weighted sum:

$$s^l(A_l) = \sum_{j=1}^n w_j s_j^l(A_l)$$

This simple aggregation method is used to make the decision-making model suitable and comprehensive for security experts without a particular background in the theory of decision analysis. The evaluation scoring scale, 0 to 10 on the quantitative scale and none to severe on the qualitative scale, indicates the severity of negative impacts as defined in Table 5. The scoring system also provides a user-friendly labeling method to characterize the impact with different colors. The color scale is taken from the OWASP project [59].

Table 5 – Incident impact scoring system.

| Qualitative rating | Numerical score | Color |
|--------------------|-----------------|---|
| None | 0.0 |  |
| Very low | 0.1 – 1.0 |  |
| Low | 1.1 – 4.0 |  |
| Medium | 4.1 – 7.0 |  |
| High | 7.1 – 9.0 |  |
| Critical | 9.1 – 10.0 |  |

For appropriate coordination with CERTs, we must map internal impact scores to standard impact levels considered by CERTs. In Slovenia, SI-CERT follows the Information Security Act

[57] to handle incidents based on severity. Table 6 shows an exemplary mapping for the case of Slovenia.

Table 6 – Exemplary mapping of assessed impact ratings to Slovenian national impact levels.

| Internal impact rating | Impact level according to the Slovenian Information Security Act |
|------------------------|--|
| None | Security event (C6) |
| Very low | Minor incident (C5) |
| Low | Moderate incident (C4) |
| Medium | Important incident (C3) |
| High | Very important incident (C2) |
| Critical | Critical incident (C1) |

3.5 Common CACAO vocabulary for BPMN modeling

While not directly translatable, the CACAO language provides some easy conversions between CACAO step objects and BPMN symbols. Specifically, parallel, if, and switch conditions can map directly to BPMN gateways, while action and playbook steps can be mapped to Tasks and Subprocesses, respectively.

Other CACAO terms have less obvious equivalents. In particular, CACAO makes extensive use of branches that terminate in an end step, for if/switch and while conditions, before proceeding from the condition steps. There are still useful methods for expressing these in BPMN diagrams, but they leave more significant ambiguity without official guidance.

Details on BPMN modeling and CACAO may be found in Section 2.6.

4 Incident response procedures and rules

This section defines incident response procedures and playbooks, recommendations for the required coordination between EPES operators and CERTs, and rules for reporting to CERTs. It also specifies the corresponding communication strategy, information-sharing mechanisms, and data structures, formats, and tools for reports. It represents the main result of D6.8.

Five CyberSEAS pilots (ITA, SLO&CRO, ROM, FIN, and EST) strictly followed the methodology introduced in Section 3 to compile national procedures and rules. This approach covers the specifics of different European countries and their legislative frameworks. We will make a detailed analysis of specific national procedures in Section 5 of this deliverable to identify common characteristics and requirements. We will then infer unification patterns, on the basis of which we will propose standard coordination and reporting procedures and rules for the common European EPES space.

4.1 Italian pilot scenarios

In this section, a summary of the relevant Italian Pilot Scenarios is described.

The first one is related to a cyber/physical attack, that is an improper access to the MV/LV cabin with a potential tampering of smart meters measurements through the access to the concentrator. Specifically, a night shift employee forgets to activate the security alarm system of the building. So, an intruder takes the opportunity to jump over the building perimeter fence and enters the premises. The intruder accesses the network internal to the cabin to identify the connected devices and takes control of the DCU concentrator. At this moment, the IT personnel receives an alert due to anomalous traffic on the network. In the meantime, the attacker can perform a series of actions on the device to modify smart meter data. Thanks to the correlation of events and threat intelligence information, the IT personnel receives more detailed alerts. Finally, based on the analysis, the IT personnel kicks off the response strategy depicted based on the collaborative decision support solution.

The second scenario is regarding a cyberattack where a malicious user is capable of stealing credentials of the SCADA management system for remote access via Social Engineering conducted on operators. In this way, malicious software is installed on the server which will be used for a reconnaissance activity of the server and network. The IT personnel receives notification of anomalous actions performed on the SCADA server. Then, the malicious user discovers a Network Attached Storage (NAS) where thresholds used by the SCADA server may be kept and he logs to the NAS and tries to search and modify the thresholds. In this case, thanks to the Advanced Tamper Resistant Storage the data is inaccessible to the malicious user who cannot modify the data.

The third one is a physical attack where a malicious user is capable of damaging the disconnecter, physically. He can arrive to the disconnection point and breaks it. In this case, the IT personnel receives notification of anomalous actions performed on the disconnecter. Also, the whole municipality can see the problem since damages to the disconnecter lead to a long time out of service. So the personnel is able to change the connection between one disconnecter and another to avoid a long out of service and then substitute the damaged disconnecter in a short time.

The scenario number four is related to a cyberattack where a malicious user is capable of stealing credential of the software management system for remote access via Social Engineering conducted on operators. So a malicious software is installed on the server and the IT personnel receives notification of anomalous actions performed. Like the second scenario, the intruder tries to modify smart meters data, but the IT personnel kicks him off.

Again, in the fifth scenario is described a cyberattack, but in this case to a single smart meter. The attacker remotely accesses the meter, exploiting the vulnerability of the SIM or in advance through the concentrator. In this case, the IT personnel receives notification of anomalous actions performed on the smart meter. The intruder takes control over the measurement part. The IT personnel receives another alert (interruption of the measurement). The attacker is intended to disconnect the meter, extract meter password, and steal data. Thanks to the correlation of events and threat intelligence information, the IT personnel receives more detailed alerts to kick off the response strategy.

The sixth and seventh scenarios depict a cyberattack to protection and control devices. In these cases, the malicious user remotely accesses the Smart Grid devices with the stolen credentials and gets control over them. The Protection and Control devices send an event (Login successful) and the IT personnel is informed of unexpected action. The malicious user makes an unexpected modification of the disconnecter threshold values and the service is disrupted to a disconnecter trip. In this case, the personnel is able to change the connection between one disconnecter and another to avoid a long out-of-service.

Finally, the last scenario depicts an improper access to the MV/LV Cabin and potential tampering of smart meters measurements and disconnecter control disruption. The intruder tampers the MV Protection and Control device. The IT personnel receives another alert (unauthorized physical access detected) and is able to kick off the response strategy.

4.1.1 Underlying national regulations

The Italian regulations in terms of cybersecurity is currently under the so called NIS Directive (Direttiva 2016/1148). Following the adoption of the NIS legislative decree (decreto legislativo 18 maggio 2018, n. 65), Italian cybersecurity regulations were strengthened through the establishment of the national cybersecurity perimeter and its implementing decrees. Nevertheless, it may soon be necessary to update the rules of the NIS legislative decree, since the European Commission has submitted a proposal to substantially revise the NIS Directive. Energy is one of the sectors covered by this decree. Both the NIS Directive and the implementing decree require that the national cybersecurity strategy set out in particular measures for the preparation, response and recovery of services following cyber incidents, the definition of a cybersecurity risk assessment plan and cybersecurity training and awareness-raising programmes, and a cybersecurity research and development plan. The "Dipartimento delle informazioni per la sicurezza" (DIS) is in charge of performing liaison functions towards the European Union and coordination with cybersecurity authorities in other Member States.

For what concerns the substation security, Benetutti meets the IEC 78-17 standard which sets out the technical prescriptions for the safe execution of maintenance work on LV and MV electrical substations and the electrical installations supplied from them. As the Pilot has 5 substations, this regulation is applied on each of them.

4.1.2 Mapping of assets and security events

In the case of Benetutti Pilot, Table 7 summarizes the mapping between the assets of the infrastructure and the security events based on MITRE ATT&CK techniques and mitigations.

Table 7 – Mapping between assets and security events for the ITA pilot.

| Event # | MITRE ATT&CK Techniques | MITRE ATT&CK Mitigations | Assets |
|---------|---|--|---|
| 1 | Phishing (T1566) | <ul style="list-style-type: none"> • Antivirus/Antimalware (M1049) • Network Intrusion Prevention (M1031) • Restrict Web-Based Content (M1021) • Software Configuration (M1054) <ul style="list-style-type: none"> • User Training (M1017) | <ul style="list-style-type: none"> • Server • Data Management System |
| 2 | Phishing for Information (T1598) | <ul style="list-style-type: none"> • Software Configuration (M1054) <ul style="list-style-type: none"> • User Training (M1017) | <ul style="list-style-type: none"> • Server • Data Management System |
| 3 | Exploitation for Privilege Escalation (T1068) | <ul style="list-style-type: none"> • Application Isolation and Sandboxing (M1048) • Execution Prevention (M1038) • Exploit Protection (M1050) • Threat Intelligence Program (M1019) • Update Software (M1051) | <ul style="list-style-type: none"> • Concentrator • Disconnecter <ul style="list-style-type: none"> • Server • Data Management System • Smart Meter |
| 4 | System Firmware (T0857) | <ul style="list-style-type: none"> • Access Management (M0801) <ul style="list-style-type: none"> • Audit (M0947) • Boot Integrity (M0946) • ... • Update Software (M0951) | <ul style="list-style-type: none"> • Server • Data Management System • Concentrator |

4.1.3 Required coordination with CERTs

CERTs are the point of reference for network users for solving any computer security problem. CERTs are made up of people specialised in systems administration, network administration, computer security and computer forensics. The tasks of the CERT are therefore: searching for anomalies; responding to user reports; analysing hardware and software systems; issuing IT security bulletins. The legislative decree on the NIS Directive also provided for the establishment at the Presidency of the Council of Ministers of a single Computer Security Incident Response Team, known as the Italian CSIRT, called upon to perform tasks and functions that were previously the responsibility of the National CERT and CERT-PA. These are mainly tasks of a technical nature related to computer incident prevention and response, carried out in cooperation with the other European CSIRTs. The Italian CSIRT started operating

on 6 May 2020 and at the same time the National CERT and CERT-PA ceased to exist as autonomous entities.

Operators of essential services are required to take 'appropriate' technical and organisational measures to manage risks and prevent cyber incidents. Similar security obligations apply to digital service providers, who are required to take technical and organisational measures to manage risks and reduce the impact of any computer incidents.

With regard to notification obligations, the transposition decree specifies that operators of essential services will have to forward to the Italian CSIRT (and for information to the competent NIS authority of their sector) notifications of IT incidents with a significant impact on the services provided. A similar obligation is also envisaged for digital service providers. The decree does not set a strict time limit for notifications, but requires that they be made 'without undue delay'.

Benetutti is currently referring to the Italian CSIRT for any relevant notification about the status of the infrastructure.

4.1.4 Defined incident response procedures and rules

The "Regolamento generale sulla protezione dei dati" (GDPR – General Data Protection Regulation) states that companies and organisations are obliged to inform the national supervisory authority as soon as possible in the event of serious data breaches, so that users can take appropriate measures.

Referring to standard ISO 27001 and ISO 27035, the IT governance determines the implementation of an effective approach against cyber incidents. The first phase is the preparation, which aims at critically preliminary evaluating the entity of an attack. Then, an analysis of the cyber threat will be performed to evaluate the involvement of the personnel, processes, technologies and information. This will lead to create an adequate control structure, controlling the response status. Secondly, the response will be performed by identifying the episodes related to cybersecurity in order to define the objectives and study the situation. It will be done to take appropriate measures to recover systems, data and connectivity. Finally, a follow-up will be taken into consideration to alert relevant stakeholders on the episode, to perform a post-situation control and learn from the experience. This is done to update the key information, controls and processes avoiding future attacks.

On the other hand, the National Institute of Standard and Technology (NIST) defines the process of incident response which includes different phases:

- **Preparation:** This phase includes all preparatory and ongoing actions aimed at creating the best conditions to manage the incident appropriately. Every useful element should be traced back to this phase, be it logistical, hardware, software, communication and process.
- **Detection & Analysis:** in view of the heterogeneity and intrinsic dynamism of attack vectors (internal, external, technological, process, human) it is possible to isolate, for each type of attack, precursors and indicators. These elements are technological (logs, specialised security apparatuses, SIEMs, network traffic flows), informational (retrieval of vulnerability news, information sharing with designated structures) and human (reports from internal staff or external organisations). Precursors and indicators determine the ability to detect potential incidents while defining the visibility perimeter

and the effective operational margin. The analysis, which immediately follows, is particularly complex and is broken down into further specialised activities (profiling, understanding of 'normal' behaviour, definition of reference baselines, correlation of security events, maintenance of an up-to-date and easily usable knowledge base, ability to collect and filter large amounts of data). The result of the analysis phase is the complete documentation of the incident, described in the fundamental attributes of impact category on organisational functions (high, medium or low severity), on the security dimension of the information concerned (Privacy Breach, loss of confidentiality, integrity, availability) and in the estimate of resources needed to overcome the problem. In this way, it is possible to assign the correct priority to the incident and direct operational efforts accordingly.

- **Containment Eradication & Recovery:** Containment is the phase that provides the time needed to define the best possible strategy. These strategies are variable depending on several factors, and different ones can be developed depending on the category of attack: containing an ongoing attack via the e-mail vector is different from containing a DDoS attack or undue extraction of sensitive data. At this stage, it is necessary to collect all possible evidence of the incident through appropriate tools and technologies aimed at safeguarding the integrity of the data collected, identifying the source of the attack and monitoring its activity. After an incident has been contained, it is necessary to proceed with the possible eradication of some components of the incident itself (malicious code, compromised accounts) and the restoration of normal operations. This restoration may involve systemic activities (backup&restore, installation of systems and applications from scratch, installation of critical patches) and security activities (review of firewall policies, changes in log production). For large-scale incidents, it should be remembered, the Recovery phase can last for months.
- **Post-Incident Activity:** this phase is about learning and improvement. Each managed incident represents an opportunity for growth and should be addressed collectively by the team through meetings (Lesson Learned) aimed at analysing, commenting and possibly correcting the implemented behaviour. There are several significant indicators in this regard: number of incidents managed in a given timeframe, time spent to resolve each incident, revisiting the documentation of each incident.

There is the need to report the incident. The Incident Report should incorporate all relevant information about the incident and the operations implemented to manage it.

In the case of Benetutti, the operators follow these rules to notify the specific entities which will be in charge of operating on the infrastructure in the case of a cyber event.

4.1.5 Data structures, formats, and tools for reports

In Italy there is currently no standards for data structures, format and tools for report. Benetutti, like all the Italian municipalities, refers to international standards. These are STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Intelligence Information). STIX and TAXII are standards developed to improve the prevention and mitigation of cyber attacks. STIX defines the threat intelligence information and TAXII the way it is transmitted. Unlike previous sharing methods, STIX and TAXII use standardised formatting and are therefore easily automated. STIX is a standardised language developed by MITRE

and the OASIS Cyber Threat Intelligence (CTI) Technical Committee to describe cyber threat data. Adopted as an international standard by various intelligence-sharing organisations and communities, it is designed for sharing via TAXII, but can also be shared by other means. STIX is structured to allow users to describe motivation, ability, capability and response. On the other hand, TAXII defines how cyber threat data is shared via services and message exchanges. It is specifically designed to support STIX data by defining an API compatible with common sharing models. The three main TAXII models are Hub and Spoke, Source/Subscriber, and Peer-to-peer.

In addition, in Italy the TLP (Traffic Light Protocol) is widely used. It is a protocol used for the exchange of information to ensure its dissemination in a controlled manner. The standard provides a simple and intuitive scheme to define the level of sharing of potentially sensitive information. The scheme is composed by four levels of sharing: RED, AMBER, GREEN, CLEAR.

4.1.6 Communication strategy and information sharing mechanisms

Communication of an occurred cyber-event and about its consequences has a strategic value. Public and private stakeholder – when public awareness is needed – have to share precise, correct, and transparent information without generating unnecessary alarms nor increasing economic and social impacts.

The strategic and operational communication of Benetutti consists of developing coordination capacity on situational awareness in order to increase communication efficiency, to facilitate response and remediation activities, to assess when dissemination to the public is needed, and to identify appropriate communication channels.

In the CSIRT website it is possible to compile an online format specifying the characteristics of cyber attack one has faced.

On the other hand, if an incident occurs, the PA Information Security Contact Person of Benetutti involves the Regional CERT, sending, through shared channels, a formal request for support in handling the incident in progress. The request must include all the details necessary for the Regional CERT to be able to carry out the analysis and provide the information needed to process the incident. At the same time as the request for support, the Security Contact Person submits the operational plan to the Regional CERT.

4.2 Slovenian and Croatian pilot scenarios

In this section, Slovenian and Croatian incident response procedures, and regulations regarding the coordination and reporting to national CERTs (SIGOV-CERT and SI-CERT) are presented. These procedures and rules are related to pilot use cases and attack scenarios.

4.2.1 Underlying national regulations

Information Security Act (ISA), which implements the EU NIS Directive in Art. 28, defines SI-CERT as the national CSIRT and in Art. 29 SIGOV-CERT as the governmental CSIRT. ISA defines obligatory reporting for governmental institutions and operators of essential services (OES) for

more important incidents. Similar provisions in reporting to the national CSIRT are defined for operators of electronic communications in the Electronic Communications Act (version 2) while voluntary reporting (government institutions to SIGOV-CERT, everyone else, including SMEs, public sector institutions, and individuals to SI-CERT) is recommended in line with provisions of ISA. The renewed Personal Data Protection Act (version 2) requires the respect of provisions of ISA for reporting relevant data breaches.

4.2.2 Mapping of assets and security events

This section defines the mappings between SLO-CRO attack scenarios and incident response procedures. It sets the context for incident response and for reporting to the national CERT in relation to use cases that are addressed by the pilot. It specifies which incident response procedures are executed for different cyber security events that are identified within individual attack scenarios. In relation to events, it also determines which procedure is utilized for which SLO-CRO pilot assets.

4.2.2.1 Use case 1 – Data poisoning of SUMO weather station data

In the attack scenario, a threat agent gains physical access to a weather station and poisons the weather data. These data are used for dynamic line rating calculations and errors in these calculations can result in higher operating costs or potentially adversely affect the stability of the grid. Given that an AI tool is used to detect the data anomaly, a "data anomaly from an unknown source" is the initial trigger to a potential incident response. This requires a specific procedure "security incident from detected data anomaly".

4.2.2.2 Use case 2 – Securing balancing service platform

Use case 2 Virtual power plant platform VE.TER (BSP) infrastructure can be part of any of the security incident scenarios:

- Data loss, destruction, or abuse
- Information system damage, abuse, infection, or intrusion
- Information System Operation Prevention
- Violations of the Legislation
- Disregard of Security Policies

4.2.2.3 Use case 3 – Cybersecurity cooperation governance

Use case 3 establishes a platform for the exchange of cyber security feeds, events, and incidents between different EPES stakeholders (such as TSO, DSO and BSP), with the purpose to improve the cyber security cooperation governance. The main data source is MISP (Malware Information Sharing Platform), which is managed by SI-CERT. MISP allows to exchange CTI (Cyber Threat Intelligence) by sharing IoCs (Indicators of Compromise) and IoAs (Indicators of Attacks).

Incident response procedures for use case 3 are limited to the infrastructure of DSOs and Informatika. Informatika provides the SOC (Security Operations Center) for the Slovenian

electricity energy sector, in order to strengthen the cyber security of DSOs on both the IT (Information Technology) and OT (Operational Technology) levels.

Use case 3 pertains to all cyber security events that can be prevented by means of MISP, i.e. by exchanging CTI/IoCs on known threats. For example, an employee might receive an email with a malicious URL. The employee opens this URL, which triggers a malware infection that causes damage to several assets in the interconnected DSO and Informatika network. The first infected asset is the employee's workstation, which can in turn propagate the infection to the IBM WebSphere application server and the IBM DB2 database server.

However, if SOC is integrated with MISP, information on known malicious URLs/IPs can be obtained with CTI exchange. SOC is hence able to update rules on the Forcepoint NGFW firewall. This prevents malware to be executed, and consequently protects IT and OT assets behind the firewall. This concept is shown in Figure 25.

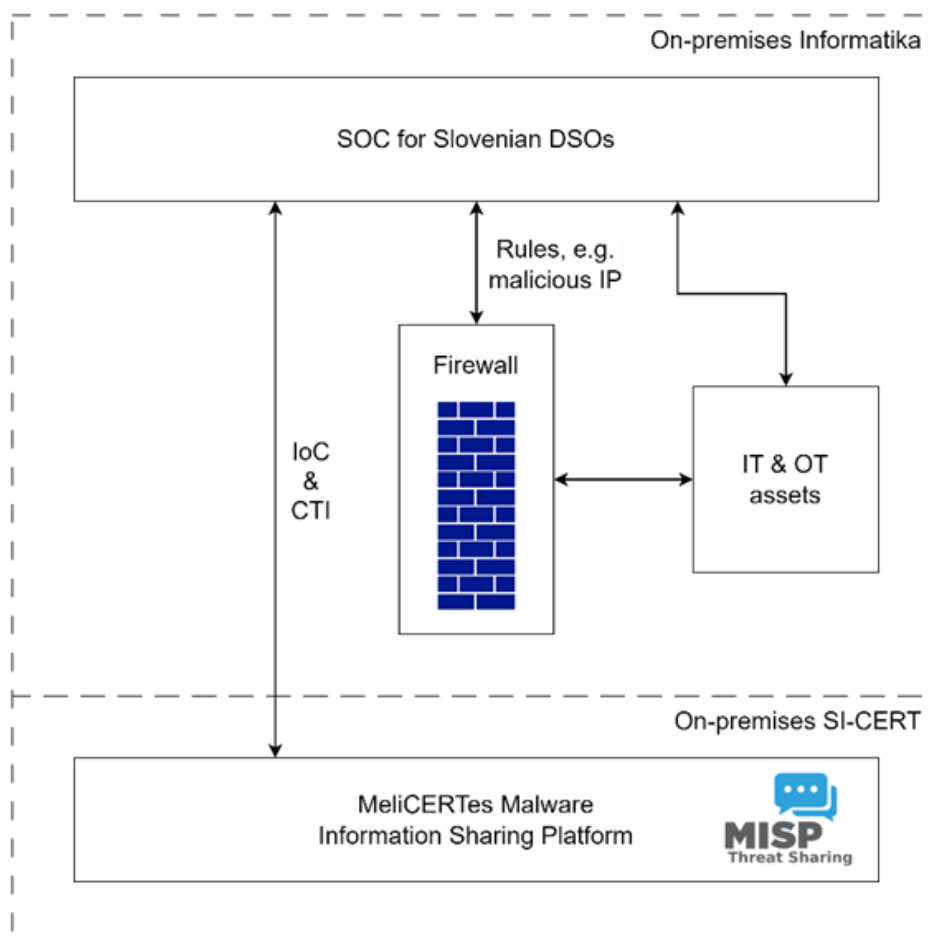


Figure 25 – Cyber security cooperation governance use case.

Based on the above explanation, three incident response procedures are defined for use case 3. These procedures are implemented by Informatika's SOC. In addition, a generic high-level incident response procedure is defined that is based on national regulations, and follows the rules for reporting and coordination with the national CERT (SI-CERT). The internal incident response procedures for use case 3 are:

1. malware infection incident response procedure, which responds to the MITRE ATT&CK technique T1588 (obtain capabilities), and its sub-technique T1588.001 (malware) in particular;
2. ransomware incident response procedure, as a special sequence of malware response actions; and
3. phishing incident response procedure, established to target the MITRE ATT&CK techniques T1566 (phishing) and T1598 (phishing for information), and their sub-techniques T1566.001 (spearphishing attachment), T1566.002 (spearphishing link), T1566.003 (spearphishing via service), T1598.001 (spearphishing service), T1598.002 (spearphishing attachment) and T1598.003 (spearphishing link).

Table 8 specifies how internal incident response procedures are applied to assets that take part in use case 3, in relation to security events that might compromise these assets.

Table 8 – Mapping of incident response procedures for the SLO-CRO use case 3.

| Asset | Security event | Relevant IR procedures |
|---|---|-----------------------------------|
| DB server 1 – TimescaleDB | Spread of infection from the user's infected workstation | Malware, ransomware, and phishing |
| DB server 2 – IBM DB2 LUW | Spread of infection from the user's infected workstation | Malware, ransomware, and phishing |
| Application server 1 – Microsoft Windows Server 2019 | Spread of infection from the user's infected workstation | Malware, ransomware, and phishing |
| Application server 2 – IBM WebSphere Application Server | Spread of infection from the user's infected workstation | Malware, ransomware, and phishing |
| Switch – Cisco Catalyst C9500-24Y4C | Spread of infection from the user's infected workstation, when specifically targeted at the switch and the switch is not properly patched | Malware, ransomware, and phishing |
| Firewall – Forcepoint NGFW | Does not block malicious content if firewall rules and anti-malware services are not up to date | N/A |
| VPN connection | Entry point to the DSO and Informatika infrastructure | N/A |

4.2.2.4 Use case 4 – Cross-border cooperation and cyber security cooperation governance

Both TSOs, ELES and HOPS, have developed a strong cross-border collaboration that includes a common Virtual Cross-border Control Center (VCC) for voltage control and loss optimization in both transmission systems. In order to enable voltage control and loss optimization, network models of both networks must be exchanged on a 15-minute basis. This is achieved using SFTP exchange of CIM XML files, as shown in Figure 26.

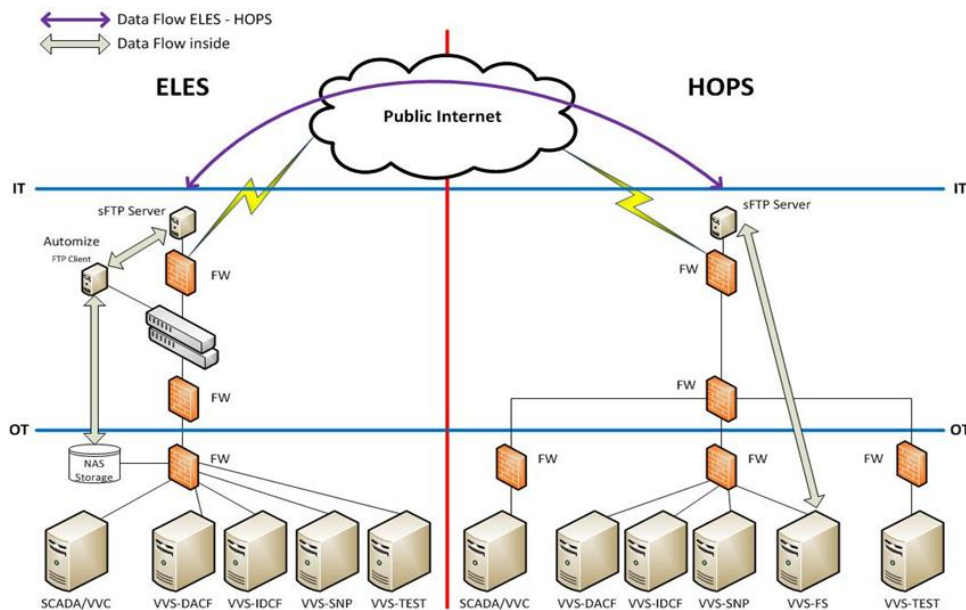


Figure 26 – Cross-border cooperation and cyber security cooperation governance use case.

In the attack scenario, a threat agent manipulates VCC, in order to disrupt service and cause grid instability. The agent performs social engineering technics to obtain credentials leading to unauthorized access. It then performs a privilege escalation, which results in the installation of malware that is programmed to execute commands leading to grid instability. This malware can compromise the following assets: Microsoft Windows Server 2019, /n software SFTP Server 2022, and FileZilla and WinSCP viewers for ELES SFTP.

The initial MITRE ATT&CK attack technique is T1589 (gather victim identity information). In order to respond, the disgruntled employee incident response procedure is utilized. Depending on the state of the attack, the malware incident response procedure can also be applied, which is defined in the section for use case 3.

4.2.3 Required coordination with CERTs

CERTs/CSIRTs provide essential support with specialized know-how on various types of incidents and are also the link to a wider CSIRT community, where information exchange can be utilized to shorten phases of incident handling after its detection. For these reasons the NIS and NIS2 Directives recognize coordination with CSIRTs as an essential part of responding more efficiently to various incidents. Another part of this coordination is vulnerability handling and coordinated vulnerability disclosure (CVD) where again CSIRTs are being recognized as entities that need to provide coordinating activities and have the necessary infrastructure as well as the CVD procedures defined.

If an incident occurs, it is of utmost importance to keep the operational bodies properly up to date. Any incident with a significant impact affecting the ability to provide essential services that the providers of essential services are obliged to provide needs to be immediately reported to the national CSIRT. Further activities are implemented in accordance with the Slovenian Information Security Act (ZInfV).

4.2.4 Defined incident response procedures and rules

This section defines the high-level national incident-handling process, as well as specific incident response procedures and rules for all pilot use cases and attack scenarios. The latter are aligned with specific requirements and characteristics of different SLO-CRO infrastructure providers in the electricity energy sector. These procedures include a number of internal technical actions but are also aligned with general national regulations.

4.2.4.1 National incident-handling process

National Cybersecurity Incident Response Plan [60] (NOKI, *Načrt odzivanja na kibernetiske incidente*) specifies details for reporting, such as the taxonomy for categorization of incidents, definitions of severity levels, methods for determining the severity of incidents, and reporting timeframes for obligatory reporting. Several parameters, including the correct taxonomy assigned to the incident, are determined by the receiving CSIRT during the triage phase of the incident.

The flowchart presented below in Figure 27 is the simplified form of the incident-handling process developed by SI-CERT. Additional information for reporting parties is available on the SI-CERT web page [61], including:

- the difference between mandatory and voluntary reports (based on the legal status of the reporting entity and links to relevant laws),
- the most common examples of incidents to report (malware infection, system and account compromise, phishing attacks, DDoS attacks, vulnerable systems and services, identity theft),
- what to expect after the report has been sent to SI-CERT, and
- where to find additional information for cases of fraud attempts (self-help, part of the SI-CERT awareness-raising program).

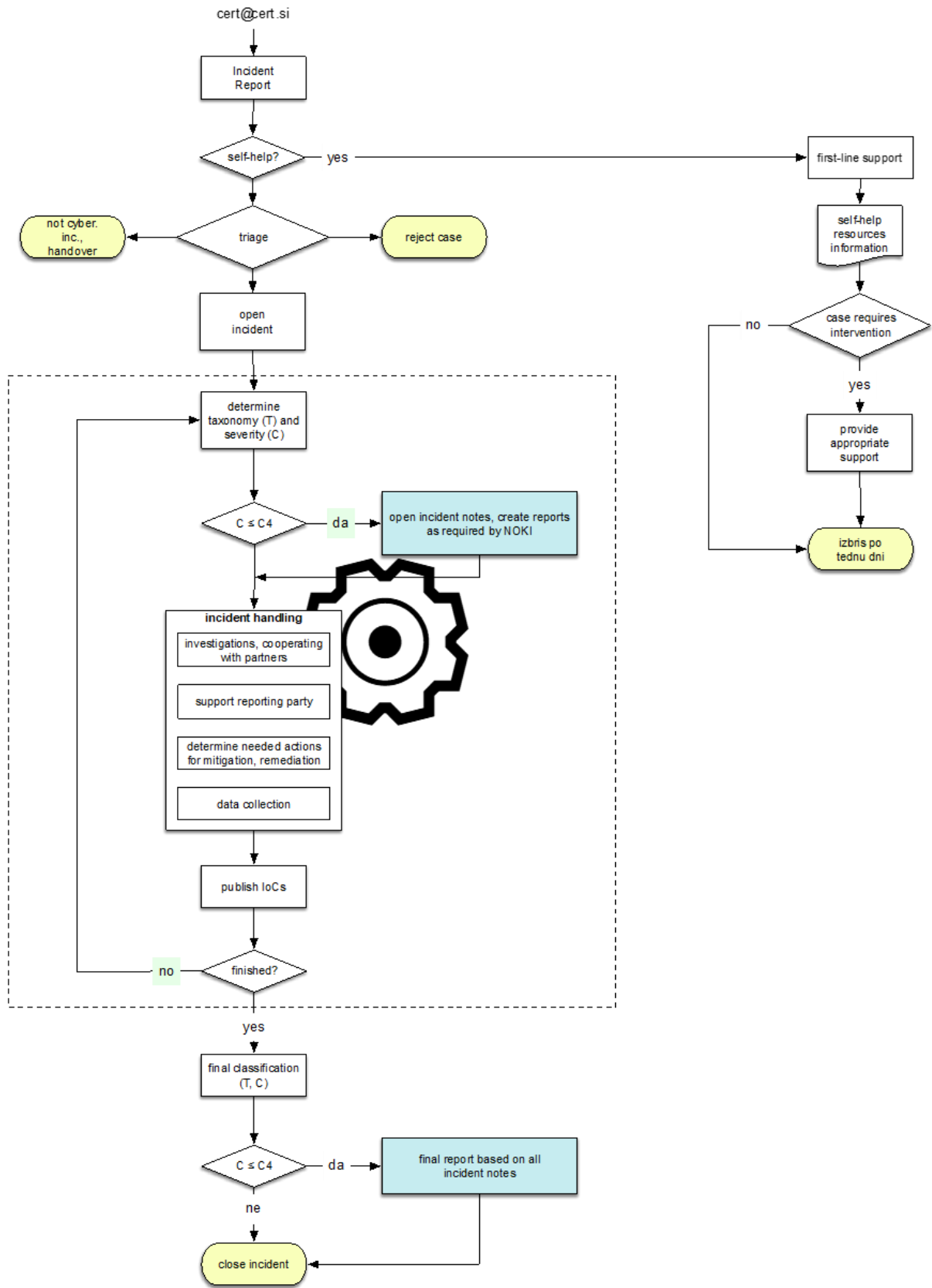


Figure 27 – SI-CERT Incident-handling flowchart.

4.2.4.2 Use case 1 – Data poisoning of SUMO weather station data

The incident response procedure for “security incident from detected data anomaly” is applied for use case 1. It is defined in Table 9.

Table 9 – Incident response procedure for the security incident from detected data anomaly.

Preparation

Regularly evaluate AI system performance and ratios of false positives and negatives, and potentially retrain the model for evolutions in the data (e.g., because of changing climate)

Evaluate and secure critical systems

Train operators to act immediately upon detection

Identification

Check the system access logs of the affected weather station

Report the occurrence of the anomaly to TSO, request inspection of the site

Provide information to TSO IT system administrator and initiate collaboration

Manually compare anomaly data with other weather data (national service) nearby weather data stations and determine malicious intent

Containment

Inform the TSO, signal to stop using the DLR results on the affected line

Quarantine the suspected data

Eradication

Rebuild/replace impacted systems, hosts, and devices (weather station, modules)

Remove the suspected data from the operation systems

Recovery

Restore impacted systems, hosts, and devices from an image

Lessons learned

Analyze what was detected

Analyze and discuss the efficiency/success of actions taken

Assess the damage

Report on the closed incident to TSO CISO

Provide an executive summary to the management

Inform and train end users

4.2.4.3 Use case 2 – Securing balancing service platform VE.TER at Petrol

According to the NIST framework, the incident management and response process includes the following activities:

- The **preparation** features all activities for the implementation of suitable processes and means, and the training of the incident response management group members
- Incident **detection and analysis**
- **Containment, eradication, and recovery** the consequences of the incident
- **Post-incident activities** in order to introduce improvements

All the incident response activities shall be executed properly and recorded for any disciplinary or legal proceedings. These may differ based on the type of incident.

4.2.4.3.1 Data loss, destruction, or abuse

Short description: An incident that could or has caused a loss, destruction, or abuse of personal data or trade secrets (electronic data, printed documents, etc.)

Consequence: The consequences of the incident depend on the scope of such an attack and can result in:

- Data loss or destruction
- Unauthorised access
- Disclosure of confidential information or personal data
- Legislation violations and fines
- ...

Detection: The incident can be detected by:

- Audit trail tools
- Security operations centre
- Users (internal and external)
- Media
- External partners

Analysis: Within the incident analysis, the response management group members in cooperation with the information system administrators:

- Identify the source of the incident by reviewing the audit trails and provided reporting information
- There is an attempt to find out who and when caused the data loss, destruction, or abuse
- The scope of data abuse is assessed (scope and sensitivity of data)
- Based on the data collected, it is assessed how critical the incident is and the company's management is notified if necessary
- The course of the incident is monitored

Notification: Notification procedures are executed in accordance with the manual II Procedures and Notifications in Case of Incidents. If personal data is abused, the Information Commissioner of the Republic of Slovenia is notified within 72 hours of detecting the incident.

Containment: After the source of the incident has been identified, the remaining data is properly protected with suitable measures, which can be executed by all competent employees (IT officers, general sector staff, security guards, etc.).

Eradication: The possibility to resolve the incidents is assessed in cooperation with the information system administrators, which may include:

- If data is lost or damaged, it is restored from the available backups.
- The audit trails are examined in order to find out how the unauthorised access was possible and the data could be abused.
- If rights are violated, they are restored and monitored more closely.
- In case of an information system intrusion, the emergency response plan for intrusions is followed as defined further in this document.

Recovery: After the data has been successfully restored and the reasons for the security incident were resolved, the leader of the information security incident response management group coordinates the incident report preparation.

Post-incident activities: The following is necessary within these activities:

- Any incident prevention improvements are assessed, such as:
 - Review of user access authorisations
 - Review of DLP solution effectiveness
 - Improvements of the information system vulnerability management solution and process
- Securing of all evidence gathered during the incident handling (logs, screenshots, files, emails, etc.)
- Presentation of the incident report to the company's management and relevant stakeholders

Reporting and escalation: Notification procedures are executed in accordance with the manual IT Procedures and Notifications in Case of Incidents.

4.2.4.3.2 Information system damage, abuse, infection, or intrusion

Short description: The information system is damaged, violated, infected, or intruded when an unknown party bypasses the company's information system security and accesses the data for which they are not authorised. A malware infection happens when a user deliberately or not opens, accesses, or starts a file or a web link exploiting known vulnerabilities and protocols which means a programme code is entered into the information system. Such incidents can be caused by external individuals or organisations, contractors, or employees.

Consequence: The consequences of the incident depend on the scope of such an attack and can result in:

- Partly or fully disabling the information system and blackmailing
- Disclosure and/or theft of personal and business data that represents the company's trade secret
- An intrusion into the information system
- Financial fraud and business losses
- ...

Detection: The incident can be detected by:

- Tools and solutions for detecting information system intrusions (IPS/IDS, firewalls, etc.)
- Malware detection tools
- Security operations centre
- Users
- Information system administrators
- Contractors
- Customers
- Media

Analysis: Within the incident analysis, the response management group members in cooperation with the information system administrators:

- Identify the source of the incident (infected workstation or server, known information system vulnerabilities, errors in the information system settings, known attack vectors, etc.) When establishing the source of the incident, all existing audit trails need to be reviewed in order to prevent any malware, emails, access to online content, usage of portable media, web servers, operating system ...
- If malware is suspected to have caused an intrusion into the information system, an IoC analysis is mandatory. If there is a sample of the suspicious or malicious software or online link available, it can be submitted for analysis to available online services, such as Virus Total, IBM X force portal, Hybrid Analyses, Zulu URL Risk Analyzer, or various online forums. Based on the information obtained from these websites, the course of the incident is assessed in order to examine if there are any patterns in the information system audit trails indicating an information system infection. IoCs simplify the identification of the scope of the incident.
- Verify if the vulnerability incident cause lies on the system or application level, and if there have been any patches provided by the developer.
- Examine if the incident was caused by erroneous settings of telecommunication and safety devices, such as: routers, switches, firewalls, IPS/IDS solutions.
- Examine if the incident pertaining to the company's information system has spread via the services provided by respective providers or contractors.
- Examine the physical information system security.
- Based on the existing database audit trails, they examine the impact on the disclosure, integrity, and availability of data at risk during the incident.
- If necessary, specialists or contractors with experience in the analysis of such events are hired and the evidence is forensically secured.
- Based on the data collected, it is assessed how critical the incident is.
- The company's management is notified of the findings of the analysis.
- The course of the incident is monitored.

Notification: Notification procedures are executed in accordance with the manual II Procedures and Notifications in Case of Incidents.

Containment: Based on the identified source of the incident, limitation activities are executed:

- Isolation of the workstation, server, or other network communication equipment within the scope of the incident. This prevents the security incident from spreading and

continuing. It is recommended that the systems are not shut down in order to secure the evidence.

- Based on known IoCs, the access to malicious online content and servers from which attackers are supposed to initiate the incident and/or steal personal and critical operational data of the company is limited.
- Based on the IoCs, forwarding and receiving malicious emails is prevented (limiting recipients, emails with suspicious content, types of attachments, etc.).
- Installation of security patches in the information system
- Prevention of domain or local user accounts in the information system for which there is no clear operational purpose and were added in a time period when the incident supposedly happened
- Prevention of domain or local user and service accounts in the information system for which there is supposedly or certainly a suspicion that there were compromised due to the incident
- Change of the passwords of all domain or local user and service accounts in the information system for which there is supposedly or certainly a suspicion that there were compromised due to the incident
- Removal of all domain or local information system settings that are or could be a consequence of the incident
- Predict an activation of specialised contractors for the analysis and securing of the evidence of the incident
- Predict the possibility to include law enforcement into the analysis phase. Based on specific know-how, they would provide for the evidence to be secured in accordance with the legislation, which could then be used as exhibits during the proceedings or any future lawsuits by the company.

Eradication: The possibility to resolve the incidents is assessed in cooperation with the information system administrators, which may include:

- Restoration of the operation of the affected part of the information system from the available backups created before the incident supposedly happened.
- Restoration of the system software from the developer's matrices.
- Restoration of communication links.
- Update of the tools for the protection from malicious software.
- Update and resetting of firewalls, IPS/IDS solutions, routers.
- Review of the audit trails of the affected parts of the information system or information solutions.
- We must verify that the incident in the affected part of the information system did not:
 - Install unwanted or unplanned software
 - Add or change user settings, users, user groups, or rights
 - Change any security settings, e.g. disable logons, antivirus software, remove security patches ...

If there are any discrepancies compared to the previous state found in the information system, it is recommended to suitably forensically secure evidence of the impact of the incident, which can then be used in further law enforcement actions or proceedings.

- Review of the vulnerabilities in the affected part of the information system and the installation of missing patches.

Recovery: After all the activities for the limitation and resolution of the causes for the incident have been implemented, the affected services are re-included into the communication network (depending on how critical the incident is) and the availability of the service is monitored together with the administrators of the information system. Within the restoration, the leader of the information security incident response management group coordinates the incident report preparation.

Post-incident activities: The following is required:

- Any incident prevention improvements are assessed, such as:
 - The ATP solution configuration is adapted
 - Improvements of the information system vulnerability management solution and process
 - The solution for the detection and prevention of intrusions into the information system is improved,
 - ...
- Securing of all evidence gathered during the incident handling (logs, screenshots, files, emails, etc.)
- Presentation of the incident report to the company's management and relevant stakeholders
- Cooperation with investigation authorities, card payment systems, regulators, and other stakeholders.

Reporting and escalation: Notification procedures are executed in accordance with the manual IT Procedures and Notifications in Case of Incidents.

4.2.4.3.3 Information system operation prevention

Short description: An attack on DoS or DDoS prevents the information system services from accessing public networks and publicly accessible services of the company.

The **consequences** depend on the scope of such an attack and can result in:

- Disabling the access to the company's online services and sites
- Inability to receive or forward emails
- Inability to access online content
- Limited or disabled payments with cards due to the inability to communicate with the card payment processor and the payment service provider
- Disabled business processes related to data exchange and support provided by the contractors and data processors

Detection: The incident can be detected by:

- DoS protection in the firewall level
- DDoS protection with the telecommunication services provider
- System for monitoring information support security events (e.g. SIEM)
- Security operations centre
- Customers
- Users
- Telecommunication services providers
- Media and other authorities (SI-CERT)
- Threats by the offenders, including blackmailing for ransom

Analysis: Within the security incident analysis, the response management group members in cooperation with the information system network administrators:

- Identify the origin of the security incident and thus the provider of telecommunication services
- Identify the service and scope of the information system affected in the attack
- Examine if the cause of the incident is a vulnerability in the system or telecommunication equipment for which the provider made the patch
- Based on the data collected, assess how critical the incident is
- Notify the company's management of the findings of the analysis
- The course of the incident is monitored

Notification: Notification procedures are executed in accordance with the manual II Procedures and Notifications in Case of Incidents.

Containment: Based on the identified origin and the provider of telecommunication services via which the incident takes place, it is necessary to:

- Examine if the incident origin's access to the breached services can be limited at the firewall or other communication equipment.
- Temporarily shut down the breached services. Such incidents can also be used to execute other malicious activities, such as intrusions into the information system. If the communication availability of the affected service is not provided via another operational provider of telecommunication services, the affected information system and service will not be available and will not be operational. The temporary shutdown prevents any other abuses that could exploit or accompany such breaches. This prevents unnecessary loads of the information system and audit trail monitoring systems.
- Check whether the affected part of the information system is vulnerable to such incidents and check if there are any security patches by the developer. If it is, it must be ensured that security patches to resolve vulnerabilities possibly leading to incidents are installed in the affected systems. In order to ensure the responsiveness and implementation, the affected part of the information system needs to be temporarily removed from the network part affected by the incident.
- If the attack is executed via the telecommunication services provider, it shall be verified if the provider and the affected communication routes can be shut down.
- The telecommunication services provider needs to be notified of the attack and requested to isolate the origin of the attack from their network in order to ensure the availability of the service.
- If the telecommunication services provider features solutions for the detection of such incidents, an agreement can be made to include protection of the provider's information services.

Eradication: The possibility to resolve the incidents is assessed in cooperation with the telecommunication service provider and the information system administrators, which may include:

- The installation of relevant security patches of the developer
- The introduction of monitoring of DoS and DDoS attacks, preparation of an action plan, and updates of the response plans

- Review of the audit trails of the affected part of the information system or information solution. We must examine within this activity if the incident in the affected part of the information system did not:
 - Install unwanted or unplanned software
 - Add or change user settings, users, user groups, or rights
 - Change any security settings, e.g. audit trail recording, antivirus software, remove security patches ...

If there are any discrepancies compared to the previous state found in the information system, it is recommended to suitably forensically secure evidence of the impact of the incident, which can then be used in any further law enforcement actions or proceedings.

- Review of the vulnerabilities in the affected part of the information system and the installation of missing patches.
- If it cannot be verified that the information system has not been altered or otherwise compromised, it is recommended to restore the affected part from the last available backup.

Recovery: After all the activities for the limitation and resolution of the causes for the incident have been implemented, the affected services are re-included into the communication network (depending on how critical the incident is) and the availability of the service is monitored together with the telecommunication services providers. Within the restoration, the leader of the information security incident response management group coordinates the incident report preparation.

Post-incident activities:

- Examine if the incident caused an unwanted disclosure, alteration, or a permanent deletion of personal data or the card payment system support data. This is executed with the review of the available audit trails of databases and systems affected or which the affected systems could access. If there have been such changes, the relevant emergency response plans need to be activated immediately.
- Any incident prevention improvement possibilities are assessed, such as:
 - Improvements of the information system vulnerability management solution and process
 - The solution for the detection and prevention of attacks
- Securing of all evidence gathered during the incident handling (logs, screenshots, files, emails, etc.)
- Presentation of the incident report to the company's management and relevant stakeholders

Reporting and escalation: Notification and escalation procedures are executed in accordance with the manual IT Procedures and Notifications in Case of Incidents.

4.2.4.3.4 Violations of the legislation

Short description: Violation of the legislation resulting in fines or even a ban on further operations of the organisation (GDPR, ZVOP-2, ZinfV, etc.)

Consequence:

- Fines

- Repossession of property
- Legal entity dissolution
- Ban on the disposal with securities owned by the legal entity
- Loss of goodwill

Detection:

- Customers
- Users (internal and external)
- External partners
- Media and other authorities

Analysis: Within the incident analysis, the response management group members in cooperation with the Data Protection Officer (DPO) and the legal department:

- Identify the data or resources that were used during the execution of the offence or criminal act
- Based on the data collected, assess how critical the incident is
- Notify the company's management of the findings of the analysis
- The course of the incident is monitored

Notification: Notification procedures are executed in accordance with the manual IT Procedures and Notifications in Case of Incidents. The management of the organisation shall immediately notify the relevant authorities (the Police or Information Commissioner of the Republic of Slovenia) and proceed in accordance with their instructions.

Containment:

- Examine if all the technical and organisational measures have been implemented as required by the legislation
- Verify the efficiency of the introduced safety mechanisms
- If necessary, temporarily limit access to the services that represent a violation of the legislation

Eradication:

- If necessary, the introduction of additional technical and organisational measures required by the legislation
- Adjustment of the security settings of the introduced safety mechanisms
- Harmonisation of services to make them in-line with the legislation if necessary
- Update of the security policies and other legal acts if necessary
- Raising awareness of employees on regulatory requirements

Recovery: Within the recovery, the leader of the information security incident response management group coordinates the incident report preparation.

Post-incident activities:

- Securing of all evidence gathered during the incident handling (logs, screenshots, files, emails, etc.)
- Implementation of sanctions for the persons responsible for the incident
- Presentation of the incident report to the company's management and relevant stakeholders

Reporting and escalation: Notification and escalation procedures are executed in accordance with the manual IT Procedures and Notifications in Case of Incidents.

4.2.4.3.5 Disregard of security policies

Short description: Incidents that could be or are a consequence of disregard of security policy provisions

Consequence:

- Data loss or destruction
- Unauthorised access
- Disclosure of confidential information or personal data
- Partly or fully disabling the information system and blackmailing
- An intrusion into the information system
- Legislation violations and fines

Detection:

- Audit trail tools
- Customers
- Users (internal and external)
- External partners
- Media and other authorities

Analysis: Within the incident analysis, the response management group members in cooperation with the information system administrators and DPO:

- Identify the data or resources that were part of the security policy violation
- Based on the data collected, assess how critical the incident is
- Notify the company's management of the findings of the analysis
- The course of the incident is monitored

Notification: Notification procedures are executed in accordance with the manual IT Procedures and Notifications in Case of Incidents.

Containment:

- Protection of other data and the information system from further violations of the security policies
- Verify the efficiency of the introduced safety mechanisms (authentication and authorisation mechanisms)
- If necessary, temporarily limit access to the services that represent a violation of the security policies (e.g., the installation of unauthorised hardware and software)

Eradication:

- If necessary, the introduction of additional technical and organisational measures for the prevention of security policy violations
- Adjustment of the security settings of the introduced safety mechanisms
- Update of the security policies and other legal acts if necessary

Recovery: Within the restoration, the leader of the information security incident response management group coordinates the incident report preparation.

Post-incident activities:

- Securing of all evidence gathered during the incident handling (logs, screenshots, files, emails, etc.)
- Implementation of sanctions for the persons responsible for the incident
- Presentation of the incident report to the company's management and relevant stakeholders

Reporting and escalation: Notification and escalation procedures are executed in accordance with the manual IT Procedures and Notifications in Case of Incidents.

4.2.4.4 Use case 3 – Informatika SOC for Slovenian DSOs

4.2.4.4.1 General incident response procedure and rules

As a part of the system of continuous operations of critical services, Slovenian DSOs aim to identify incidents that may be a consequence of extraordinary cyber security events. These incidents can cause damage to infrastructure providers or users. With the purpose of managing cyber security incidents, DSOs have introduced the Cyber incident response process which is placed under the System of continuous operations. The Cyber incident response process is established to ensure information security and operational security of all systems, with an emphasis on systems that set the basis for essential services. This process includes all standard incident response phases:

1. preparation,
2. identification,
3. containment,
4. eradication,
5. recovery,
6. lessons learned, and
7. reporting about cyber incidents to internal and external stakeholders.

The process implements the regulatory requirements of the Critical Infrastructure Act [62] and the Information Security Act [57], including related regulatory decrees, such as the Rules on security documentation and security measures of operators of essential services [63], the National Cyber Incident Response Plan [60], and the Regulation on the determination of essential services and a more detailed methodology for determining providers of essential services [64].

Informatika provides IT services, IT infrastructure, and the Security Operations Center (SOC) for five Slovenian DSOs. SOC operates 24/7 at three levels of support – L1, L2 and L3. L1 provides the services for the identification of cyber incidents, while L2 and L3 are authorized to:

- analyze cyber security incidents and respond to them, and
- report about cyber security incidents.

The general incident response procedure that is followed by SOC for all types of cyber incidents and information incidents is presented in the BPMN notation in Figure 28.

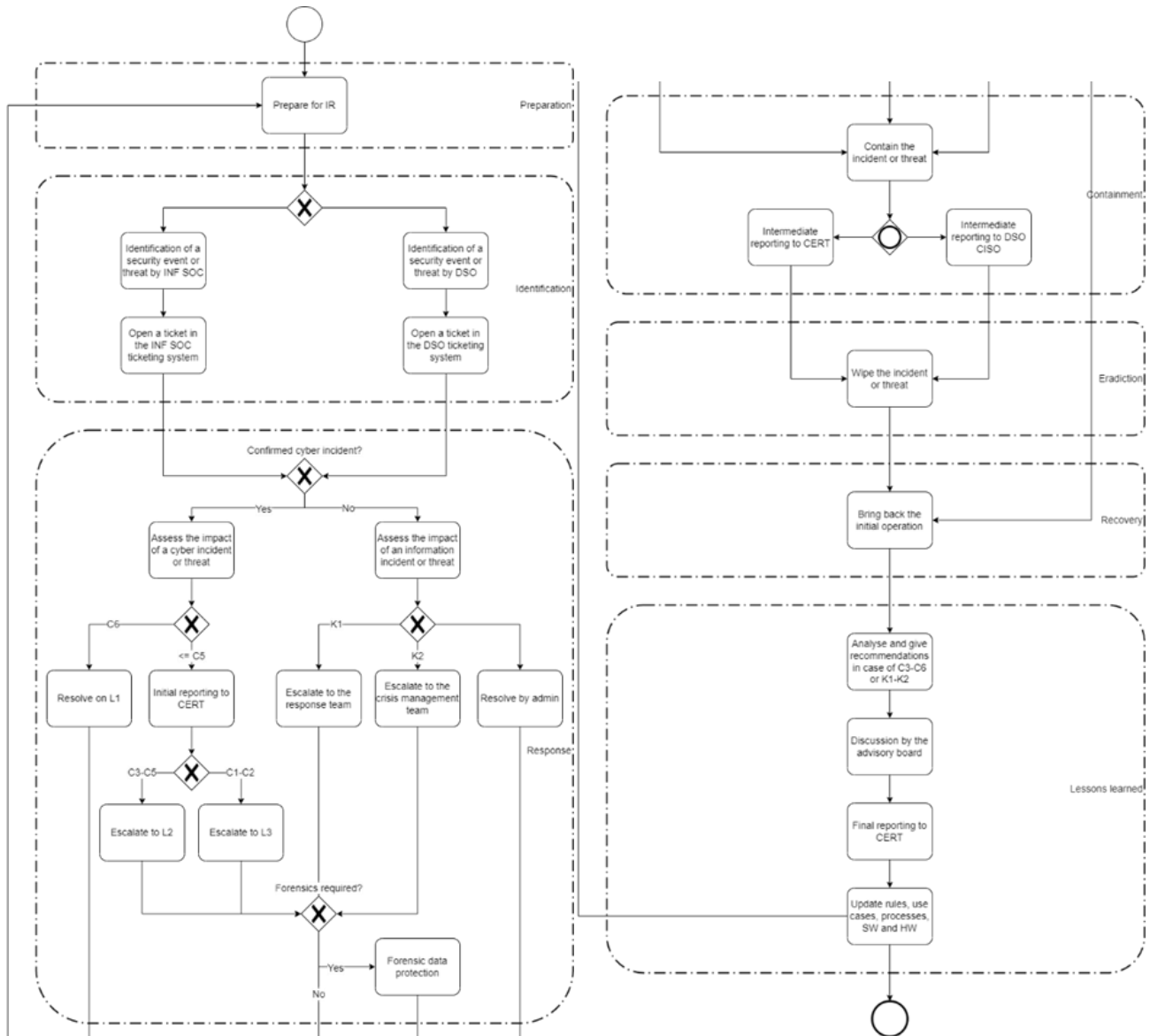


Figure 28 – General incident response procedure for Informatika SOC.

In case a cyber incident is detected and confirmed, SOC assesses the impact of this incident based on the impact level classification defined in the Information Security Act, and also in the National Cyber Incident Response Plan, respectively. This level is expressed on the scale of C1 to C6 and is subsequently mapped into the internal score of 1 to 4, and into the internal criticality up to K2. The impact mapping rules are summarized in If the security event is well known and is already described in the knowledge base, and also has a low criticality score, it is managed by L1 SOC. In other cases, a ticket is opened by L1 SOC in the incident management system, which activates L2SOC and triggers the response of the affected DSO. Cyber incidents are responded to at L2 or L3 SOC, while information incidents are addressed by the DSO response team. The detailed communication rules and mechanisms that align with different security roles and correspond with the general SOC incident response procedure are described in subsection 4.2.6.

Table 10. The mapping is done for each affected service or asset by the administrator of this service/asset.

If the security event is well known and is already described in the knowledge base, and also has a low criticality score, it is managed by L1 SOC. In other cases, a ticket is opened by L1 SOC in the incident management system, which activates L2 SOC and triggers the response of the affected DSO. Cyber incidents are responded to at L2 or L3 SOC, while information incidents are addressed by the DSO response team. The detailed communication rules and mechanisms that align with different security roles and correspond with the general SOC incident response procedure are described in subsection 4.2.6.

Table 10 – Impact mapping table.

| Impact level according to the Information Security Act | Internal impact score | Criticality |
|--|-----------------------|-------------|
| Critical incident (C1) | 4 | K2 |
| Very important incident (C2) | 4 | K2 |
| Important incident (C3) | 3 | K1 |
| Moderate incident (C4) | 2 | K1 |
| Minor incident (C5) | 1 | / |
| Security event (C6) | 0 | / |

The activities of different SOC levels and roles within the general incident response procedure are defined in the RACI matrix, which is presented in Table 11, where RACI stands for:

- R – Responsible: a person or a group that is due to execute an action or process;
- A – Accountable: a person who makes sure the assigned action or process completes;
- C – Consulted: a person or a group that is entitled to give an opinion;
- I – Informed: a person or a group that gets informed.

Table 11 – RACI matrix for security levels and roles.

| Activity | L1 SOC | L2 SOC | L3 SOC | SOC manager |
|-------------------------------------|--------|--------|--------|-------------|
| Definition of asset policies | | C | R | R |
| Reporting to CERT | | C | R | R |
| Incident classification | R | R | R | R |
| Activation of L2 SOC | R | | | I |
| Activation of L3 SOC | | R | | I |
| Regular internal/external reporting | R | | | A |
| Reporting on major incidents | R | R | R | A |
| Crisis declaration | | C | C | C |
| Recommendations on policy changes | RC | RC | RC | R |

| | | | | |
|------------------------------------|---|----|----|---|
| Active identification of threats | I | R | R | A |
| Post-incident activities | R | | R | R |
| Determination and exchange of IoCs | R | | R | A |
| Protection of proofs | I | R | RC | A |
| Incident containment | I | R | RC | A |
| Incident removal | I | R | RC | A |
| Arranging additional services | I | RC | | R |

Service Level Agreements (SLAs) on incident response procedures are defined and must be followed. The response of L1 SOC is immediate, while L2 SOC is due to respond in 4 hours. The response plan has to be prepared in 24 hours. The recovery plan that also contains the incident analysis is required to be provided within 10 working days.

4.2.4.4.2 Malware incident response procedure

Malware is a “sizable” umbrella term, which is formed from “malicious” and “software” [65]. It refers to any intrusive, unwanted software that is designed to compromise, damage, or destroy a computer, device, network, or the data contained within. The most common examples of malware include viruses, worms, trojans, ransomware, file-less malware, adware, malvertising, and spyware.

Malware incident response procedure is defined in Table 12. It covers all phases: preparation, identification, containment, eradication, recovery, reporting, and lessons learned.

Table 12 – Malware incident response procedure.

Preparation

Evaluate and secure critical system backups

Train and inform end users

Identification

Get hash values of malware files

Investigate malware to determine if it is running under a user context

Analyze malware – observe compromised target IPs of the infected system

Analyze malware – observe attempts at network connectivity

Analyze malware – identify files modified and created by the malware

Determine IoCs based on malware analysis

Use IoCs to locate additional infected hosts

Use IoCs to determine additional attacks associated with malware

Use IoCs to search for the initial point of entry

Use IoCs to analyze attack vectors for infection

Perform advanced forensic analysis

Select available tools for containment, eradication, and recovery

Report the occurrence of malware incident to DSO CISO

Provide information to DSO IT system administrator and initiate collaboration

Containment

Put malware into the sandbox

Preserve an archive copy of malware files

Isolate infected systems, hosts, and devices

Disable compromised user accounts

Provide instructions and requirements to affected users

Report identified malware details to DSO CISO and CERT

Close gaps based on IoCs – endpoint protection

Close gaps based on IoCs – firewall configuration/rules

Close gaps based on IoCs – email rules

Close gaps based on IoCs – controls for attack escalation prevention

Close gaps based on IoCs – user education

Implement network rules, procedures, and segmentation to contain malware

CTI exchange – submit hash values to community sources to aid in future detection

Eradication

Preserve artifacts, systems, and backups

Preserve volatile data collected during the identification and containment phases (log files, memory images, backups, malware samples, etc.)

Rebuild/replace impacted systems, hosts, and devices

Recovery

Restore impacted systems, hosts, and devices from a clean backup

Restore impacted systems, hosts, and devices from an image

Remediate identified vulnerabilities and gaps

Recover user accounts – reset passwords

Recover user accounts – create replacement accounts

Recover user accounts – disable accounts permanently

Provide instructions on new account/system rules to affected users

Lessons learned

Analyze what was detected

Analyze and discuss the efficiency/success of actions taken

Assess the damage

Report on the closed malware incident to DSO CISO and CERT

Provide an executive summary to the management

Inform and train end users

4.2.4.4.3 Ransomware incident response procedure

Ransomware is a specific type of malware that infects target devices, locks or encrypts files and programs to prevent their use, and demands a ransom in return for their release. The ransomware incident response procedure is presented in Figure 29.

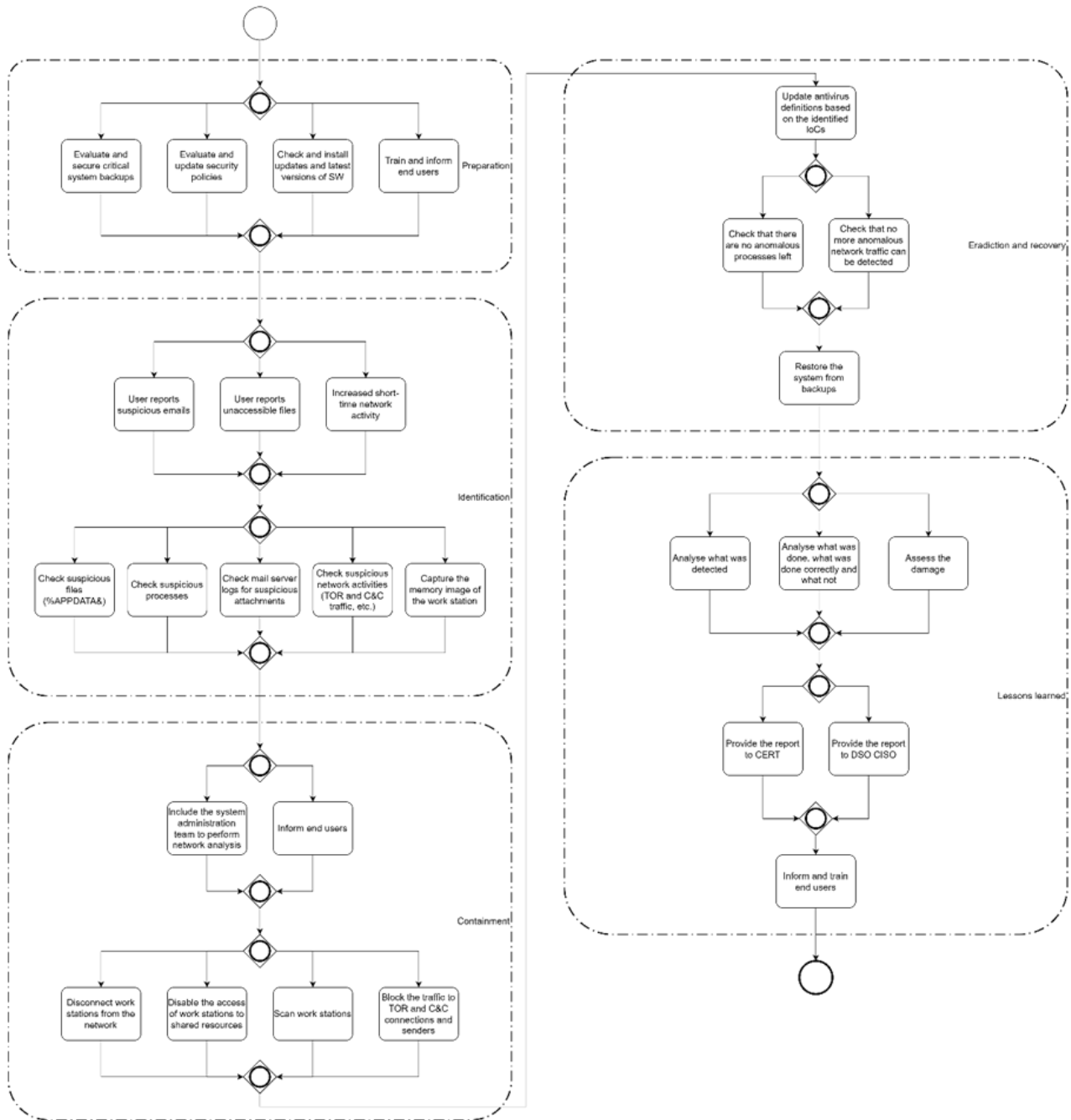


Figure 29 – Ransomware incident response procedure.

4.2.4.4.4 Phishing incident response procedure

Phishing attacks deliver malware that masquerades as a communication from a trusted or reputable source, where the communication channel is an email, a phone call or a text message. Figure 30 depicts the phishing incident response procedure.

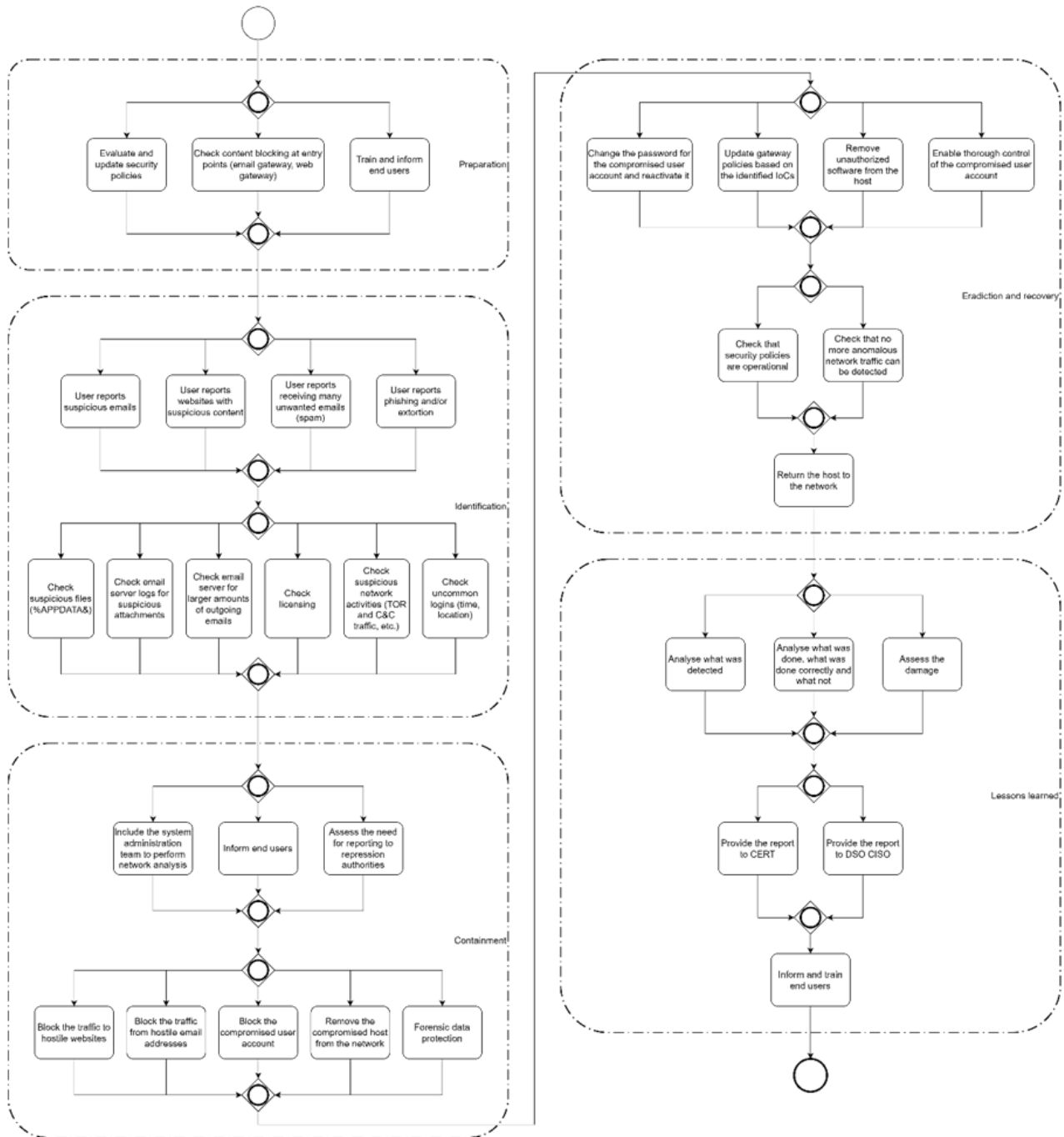


Figure 30 – Phishing incident response procedure.

4.2.4.5 Use case 4 – Cross-border cooperation and cyber security cooperation governance

The incident response procedure for the disgruntled employee is applied for use case 4. It is defined in Table 13.

Table 13 – Disgruntled employee incident response procedure.

Preparation

Evaluate and secure critical system backups

Train and inform end users

Identification

Check the size of the damage caused by the manipulation of the document or system

Check the system access logs

Report the occurrence of the incident to TSO CISO

Provide information to TSO IT system administrator and initiate collaboration

Containment

Disable user account of the disgruntled employee

Disable VPN user account of the employee

Report identified malware details to TSO CISO and CERT

Notify SFTP partner about cybersecurity incident

Eradication

Rebuild/replace impacted systems, hosts, and devices

Recovery

Restore impacted systems, hosts, and devices from a clean backup

Restore impacted systems, hosts, and devices from an image

Lessons learned

Analyze what was detected

Analyze and discuss the efficiency/success of actions taken

Assess the damage

Report on the closed malware incident to TSO CISO and CERT

Provide an executive summary to the management

Inform and train end users

4.2.5 Data structures, formats, and tools for reports

SI-CERT follows several data feeds for systems in Slovenia that show newly discovered vulnerabilities or unusual behavior that may be the result of cybersecurity incidents. Reports can be sent via e-mail and currently information is supplied in the format determined by the reporting party. NOKI provides templates for reporting as the suggested format although it is

expected that in future a common platform will also be used for more structured reporting. Experience shows that it is wise to be as flexible as possible in accepting reports, especially with first reports where all details are not available yet and the reporting party can be under significant strain due to the consequences of the incident.

4.2.6 Communication strategy and information sharing mechanisms

4.2.6.1 SI-CERT recommendations

Information sharing is important for various stages of incident handling. For this purpose, SI-CERT advises OESs and the public of currently observed threats. In communication between OESs and SI-CERT, the TLP protocol is used, which is also recognized in NOKI as the de-facto standard in the cyber-security community. OESs (and other entities, such as government institutions) are encouraged to join the local MISP network for faster IoC sharing.

4.2.6.2 Use case 2 - Securing balancing service platform VE.TER at Petrol

4.2.6.2.1 Response management group

There is an appointed information security incident response management group with the necessary know-how and competencies in the company. In accordance with the security policy, this group features the staff and contractors, if necessary. Group members are appointed by the Management Board with a resolution. Contacts are listed in the manual IT Procedures and Notifications in Case of Incidents.

The group members are ready 24/7 as they also have their deputies appointed for when they are unavailable. If necessary and with regard to the character and the consequences of an information security incident, also other company's staff members can be included in the group by request of the group leader.

Any employee can be a member of the group should the necessity arise. The group leader can also include other external partners into handling an information security incident in accordance with the company's security policy.

The group shall be provided all the necessary conditions for resolving an information security incident (the necessary space, IT infrastructure documentation, proper IT equipment, and all necessary access rights).

If an incident occurs, it is of utmost importance to keep the operational bodies properly up to date.

4.2.6.2.2 Requirements pertaining to the company's communication with external stakeholders

Protection of personal data: If an incident that impacts the confidentiality, integrity, or availability of personal data is detected, the company's DPO shall be notified immediately

so they can instigate further measures based on their authorizations and in accordance with the legislation.

Critical infrastructure: Any incident with a significant impact affecting the ability to provide essential services that we as the providers of essential services shall provide needs to be immediately reported to the national CSIRT. Further activities are implemented in accordance with the Slovenian Information Security Act (ZInfV).

Notification of business partners and individuals: If an incident with a high risk of posing a significant threat to the information system and the data of business partners and individuals is detected, it must be reported immediately in order to limit the consequences.

4.2.6.3 Use case 3 – Informatika SOC for Slovenian DSOs

Several rules are established to implement the communication strategy between L1 SOC, L2 SOC, L3 SOC, DSOs, and the national CERT.

1. In case that the service/asset administrator makes a judgment that neither K1 nor K2 criterion is met, the administrator can directly resolve the incident and immediately restore the initial operation.
2. In case that the administrator of the compromised service or asset determines that an information incident of K1 criticality occurred, the Chief Information Security Officer (CISO) is notified. CISO activates the response team and coordinates it, in order to respond to the information incident.
3. In case that a cybersecurity incident of K1 criticality is detected, L2 SOC notifies the response team and initiates the incident response procedure. The response team coordinates the response and provides sufficient resources to resolve the cybersecurity incident.
4. If a possibility of K2 or higher criticality is assessed, the CISO or the response team must activate the DSO crisis management team. In this case, the security incident has a direct influence on essential services, hence the procedures of continuous operations are activated. SOC is responsible for reporting to the national CERT, while the response team is accountable for this.
5. SOC does not report to the national CERT on cybersecurity events of levels C5 and C6. For reporting, K1 or K2 criticality criteria have to be met.
6. In case the incident cannot be resolved at L1 SOC, it is always reported to L2 SOC by means of an opened ticket in the incident management system and an additional telephone call. Communication channels between L2 SOC and L3 SOC are specified in the operational instructions on providing the services of L1, L2, and L3 SOC.

4.3 Romanian pilot scenarios

In this section, a summary of the relevant Romanian Pilot Scenarios is described.

4.3.1 Underlying national regulations

Romania has implemented different laws and regulations related to cyber security and incident response. Because of the fact that Romania is an EU country, its regulations are a

child of the GDPR and NIS (NIS Directive — ENISA (europa.eu)). The EU directive 2016/1148 on Security and Information Systems (The NIS Directive) regulates the main EU legislative framework, which aims to achieve a high common level of network and information systems security across the European Union. NIS directive applies to Operators of Essential Services (“OESs”) and to Digital Service Providers (“DSPs”). NIS and GDPR represent the legal basis for cybersecurity law in Romania. In furtherance of the GDPR, Law no. 190/2018 was issued to guarantee, between others, the following:

- The correct processing of genetic, biometric, or health-concerning data
- The processing of a national identification number
- The processing of personal data in the context of employment
- The processing of personal data and of special categories of personal data for the performance of a task carried out in the public interest

The Romanian cybersecurity strategy has both short and long-term objectives. The goal is to develop a dynamic information environment based on interoperability and on the provision of IT services while protecting citizens' rights. Under Law no.362/2018, the Romanian National Computer Security Incident Response Team (CERT-RO) is the national authority that deals with IT systems and national network security. In Romania, CERT-RO has primary responsibility for incident response, however, all organizations with critical infrastructure, and others, are also expected to have their own incident response plan and team. There is a National Cyberint Center (CERT-RO) at which incidents that should be reported. CERT-RO operates 24/7 and can be reached through various contact channels including email, telephone, and other social media. CERT-RO encourages all individuals and organizations to report any cyber incidents that may have an impact on national cyberspace to them.

Furthermore, Law no. 362/2018 requires OESs and DSPs to:

- Take appropriate technical and organizational measures to secure their networks and information systems;
- Prevent security incidents in order to guarantee service continuity
- Notify CERT-RO of any security incidents having a significant impact on service continuity;
- Cooperate with CERT-RO.

In accordance with the law examined before there is a wide range of violations that may constitute contraventions, the fines being set between specific thresholds of 3.000 and 100.000 Lei.

4.3.2 Required coordination with CERTs

Directive (EU) 2016/1148 of the European Parliament takes into account the risks associated with cyber security incidents, having the effect of disrupting economic activities, financial losses of companies, citizens, and institutions, as well as intentional or unintentional disruptions of the IT systems that support the essential services. Following the European directive, CERTs are created in EU countries. A Computer Emergency Response Team is a group of experts in cybersecurity that are capable of managing adverse events regarding cyber-attacks. CERTs also plan policies about mitigation and data protection and analysis in order to assure compliance with the EU directives. In Romania, CERT-RO is the main authority.

4.3.3 Defined incident response procedures and rules

The incident response procedures in Romania generally follow a similar framework to those in other countries, which include the following steps:

1. **Preparation:** This includes developing incident response plans, establishing incident response teams, and training employees on incident response procedures.
2. **Identification:** This involves detecting and identifying a potential cyber incident.
3. **Containment:** This step involves taking measures to stop the incident from spreading and limit the damage caused.
4. **Eradication:** This step involves removing the incident's source and cleaning up any remaining artifacts.
5. **Recovery:** This includes restoring normal operations and services and implementing measures to prevent future incidents.
6. **Lessons learned:** This includes conducting a post-incident review to identify what went well and what could be improved in the incident response process.

In Romania, CERT-RO has primary responsibility for incident response, however, all organizations with critical infrastructure, and others, are also expected to have their own incident response plan and team. All incidents should be reported to the National Cyberint Center (CERT-RO). In addition to the incident response procedures outlined by the CERT-RO, organizations in Romania are also required to have incident response plans in place to address cybersecurity incidents. These plans should outline the procedures and responsibilities for detecting, responding to, and mitigating cybersecurity incidents.

These incident response plans should also include procedures for:

1. Notifying relevant authorities and stakeholders in the event of an incident, including the CERT-RO
2. Communicating with employees, customers, and other stakeholders about the incident, including any potential impact and mitigation measures
3. Preserving evidence related to the incident, including logs and other relevant data
4. Conducting a post-incident review to identify the cause of the incident, assess the effectiveness of the response, and identify areas for improvement

There's also an emergency ordinance that establishes the Cyberint National Centre, in order to ensure the protection and resilience of the cyber-space, with the main responsibilities to identify, prevent, detect and respond to malicious cyber activities that threaten the national security and defence, and also to provide a safe and secure environment for its citizens and economic operators.

Also, for the incident response in the critical infrastructure sector, like energy and finance, there is a framework for Risk Management and Crisis Management with regular testing, exercises and training, incident reporting, and incident response plans in place.

In summary, Romania's cybersecurity law and incident response procedures are designed to protect the country's information infrastructure and maintain national security by implementing strict regulations, oversight, and incident response mechanisms. The CERT-RO and the Cyberint National Centre play a critical role in incident response and risk management, with the collaboration between the public and private sectors, to help prevent and respond to cybersecurity incidents in a timely and effective manner.

4.3.4 Data structures, formats, and tools for reports

CERT-RO collects data about cyber security incidents or alerts from different sources:

1. Alerts collected via automated systems. Those types of reports could be sent only by a few specialized organizations which have their incident detection systems. The number of these alerts is significantly higher than other types.
2. Individual alerts. Those reports are sent by individuals or legal persons from Romania and abroad.
3. Information collected by CERT-RO. This information is collected by various sources, public or restricted. An example could be a specialized website or a security company that can gain information about vulnerabilities or cyber security threats and incidents.

Alerts sent by the automated system require automatic processing. The received data can be resumed as a list of IPs detected as doing malicious activities over the net and other extra details. These alerts are processed by CERT-RO and are sent to the internet service providers linked to the network that contains the suspicious user. The ISPs have the responsibilities to send an alert to the client.

Individual alerts are also collected by CERT-RO, even if the numbers of these alerts are less than the previous ones, they are significantly more detailed. For this reason, the processing is done by CERT-ROs analysts that could analyze and take precious information from those reports. It's possible to report cyber-security incident directly by phone calling the DNSC (Directoratul National de Securitate Cibernetica) at 1911, or filling the available form, as shown in Figure 31 below.

4.3.5 Communication strategy and information sharing mechanisms

Information exchange among teams and companies improves reaction time to security incidents. Sharing correct and transparent information without generating alarming could bring several benefits. In Romania, as reported in the previous section, it is possible to provide information and reports directly to the CERT. The analysis of data, performed by experts in the cyber-security sector, allows the possibility to have clear statistics and a wider vision of the current situation in terms of cyber-attacks, threats, and vulnerabilities.

| | |
|---|--|
| <p>First name</p> <input type="text"/> | <p>Our contact details</p> <p>Secretariat and public relations</p> <p>Phone: (+40) 316-202.187</p> <p>Fax: (+40) 316-202.190</p> <p>Email: office[@]dnsc.ro</p> <p>Relations with the press</p> <p>Email: media[@]dnsc.ro</p> <p>Phone: (+40) 316-202.152</p> <p>Designated person: Mihai Rotariu</p> <p>Human resources</p> <p>Email: hr[@]dnsc.ro</p> <p>Phone: (+40) 316-202.197</p> <p>Address: Strada Italiană nr. 22, Sector 2, Postal Code 020976, Bucharest</p> <p>Reporting cybersecurity incidents</p> <p>Incidents: alerts[@]dnsc.ro</p> <p>PGP Key: Fingerprint=9201 878E BA41 9E1E A83C 8CBA 93DC 90A3 A319 65AD</p> <p>Coordinated Vulnerability Reporting - CVD</p> <p>Email: View the reporting guide</p> <p>Single National Contact Point</p> <p>Email: spoc[@]dnsc.ro</p> <p>Audience schedule - Mon:15-18 (with prior appointment)</p> <p>Phone scheduling audiences: (+40) 316-202.187</p> <p>Opening hours: Mon-J:08:00-16:30, V:08:00-14:00</p> |
| <p>Name</p> <input type="text"/> | |
| <p>Email</p> <input type="text"/> | |
| <p>Message</p> <div style="border: 1px solid #ccc; height: 150px; width: 100%;"></div> | |
| <p>Select a department</p> <ul style="list-style-type: none"> Incident reporting (alerts@dnsc.ro) CSIRTs National - Rapid Response Team (csirt@dnsc.ro) Secretariat and public relations (office@dnsc.ro) Single National Contact Point (cooperation@dnsc.ro) Relations with the press (media@dnsc.ro) <p>Select a department ▼</p> | |

Figure 31 – ROM incident reporting form.

4.4 Finnish pilot scenarios

This section describes Finnish regulations regarding cybersecurity incident response procedures and rules. In addition, the scenarios defined to study the Finnish pilot are discussed in the section. The summary of the scenarios defined for the Finnish pilot is as follows:

- **Scenario 1:** This scenario focuses on a situation where a malware is brought to the companies network or system by an employee who unintentionally downloads and installs the malware. The scenario is initiated by spearphishing attachments, links or via services.
- **Scenario 2:** This scenario focuses on a situation where a malware is brought into the companies network or system by an employee who connects a compromised device (e.g., mobile and computer) to the the system or network.
- **Scenario 3:** This scenario focuses on a situation where spoofing messages causes interruption in system services. This scenario can be initiated through network access which is provided to trusted partners.
- **Scenario 4:** This scenario focuses on a situation where spoofing messages causes interruption in system services. This scenario can be initiated by an individual who has access to a network connected to the companies network.

- **Scenario 5:** This scenario focuses on a situation where electricity supply contract of a consumer is terminated by an attacker who has stolen companies system credentials from an authorised user and has access to the companies network.
- **Scenario 6:** This scenario focuses on a situation where electricity supply contract of a consumer is terminated by an attacker who has used spearphishing to install a malware in the companies system or network to steal companies system credentials. The attacker has network access which is provided to trusted partners.
- **Scenario 7:** This scenario focuses on a situation where electricity supply contract of a consumer is terminated by an attacker who has cracked the password for the companies system or network. The attacker has network access which is provided to trusted partners.
- **Scenario 8:** This scenario focuses on a situation where consumer data is compromised (i.e., GDPR is violated) by an attacker who has stolen an authentication token to obtain credentials for the companies system or network. The attacker has network access which is provided to trusted partners.
- **Scenario 9:** This scenario focuses on a situation where consumer data is compromised (i.e., GDPR is violated) by an attacker who has used spearphishing to acquire background info thereby obtaining credentials for the companies system or network. The attacker has network access which is provided to trusted partners.
- **Scenario 10:** This scenario focuses on a situation where a consumer tampers with the electricity meter and modifies the data to get benefit by reducing his electricity bill. The tampering can be achieved by bypassing the meter where a bypass wire is used to feed a load inside the property. This has negative consequences for the company since it loses reputation if the meter data manipulation has happened because of the lack of implemented security means. The DSO (i.e., distribution system operator) suffers financial losses since the consumption of the bypassed load is considered in the network losses.

These scenarios are defined to study different cybersecurity aspects of the Finnish pilot, as part of a critical infrastructure, in the hope of facilitating development and evaluation of relevant cybersecurity enhancement tools and technologies.

4.4.1 Underlying national regulations

The legislations regarding cybersecurity which are in place in Finland are listed and briefly described in bellow:

- **Act on Electronic Communications Services (917/2014):** The key piece of regulation on digital communications in Finland is the Act on Electronic Communications Services (917/2014). The Act contains provisions on matters related to e.g., information security and the security of confidential communication channels. The Act applies to telecommunications operators, communications providers, corporate or association subscribers and domain name registrars.
- **The EU Directive on network and information security (NIS Directive):** The EU Directive on network and information security aims to ensure a high level of security in the networks and information systems used throughout the European Union. The Directive contains provisions on information security obligations and disruption reporting practices. The Directive mandates that key service providers and some specific

digital service providers must maintain a comprehensive level of network and information security-related risk management; manage the continuity of their services during incidents; and that they must report about any security deviations to the responsible authorities in case the deviation could hinder or even threaten the continuity of their operations. The obligations in the Directive are directed towards the fields that are vital for the functionality of society. In Finland, these obligations have entered into force through sector-specific legislation, and their compliance is monitored by the authorities responsible for each sector. Energy supply is one of the sectors and energy authority is the responsible party for that.

- **General Data Protection Regulation of the EU:** The General Data Protection Regulation of the EU (GDPR) sets the requirements concerning the collection, storage, and management of personal data by companies and organizations. These requirements apply to both European organizations that process personal data within the EU and organizations outside the EU that process the personal data of EU residents. The GDPR applies if a company processes personal data and has a location in the EU. This is done irrespective of where the data itself is processed or if the company is located outside the EU but processes personal data that is related to the provision of goods or services to people within the EU, or if a company monitors the behavior of individuals within the EU.
- **Data Protection Act (1050/2018):** The Data Protection Act specifies and supplements the GDPR. The Act applies to the processing of personal data in general. As it has been designed to specify and supplement the GDPR, the Act does not form an independent and comprehensive set of regulations and is instead meant to be applied in conjunction with the GDPR.
- **The Criminal Code of Finland (39/1889):** The Criminal Code of Finland does not contain the term cybercrime, and cybercrimes are instead typically classified as technical or information network crimes. These are specified in detail in chapter 38 of the Criminal Code. In addition, the other chapters of the Criminal Code contain provisions on other crimes related to cybercrime. For example, provisions on business secret violations and misuses are presented in chapter 30 of the Criminal Code, which focuses on business offences.

In addition to the above regulations, in Finland, the first cybersecurity strategy was published in 2013. The strategy was part of the national security strategy implementation. The main target for the strategy is to increase comprehensive security as well as to initiate nationwide contingency management planning. To put the strategy into practice, an action plan consisting of 74 actions was prepared in 2014. The second action plan consisting of 22 actions was prepared in 2017. The updated cybersecurity strategy was published in 2020.

The Finnish cybersecurity strategy developed and published in 2013 contains ten alignments out of which six alignments set requirements to the national critical infrastructures including energy sector. The alignments are listed here:

- An efficient cooperation model will be set up between the authorities and the different actors to promote cyber threat prevention.
- The overall cyber security situational awareness of the vital functions of society will be increased.

- The ability to detect and combat cyber threats and incidents of vital functions of society as a part of economic continuity management will be maintained and further developed.
- The understanding and competence of all actors in society over cybersecurity will be improved.
- Cybersecurity will be ensured via enforcing national law.
- Relevant service models, common fundamentals and responsibilities will be assigned to authorities and business operators to manage cybersecurity.

The second action plan published in 2017 had two main goals for critical infrastructures:

1. The adequate level of security of supply based on energy and climate strategy must be secured by the ministry of economic affairs and employment of Finland.
2. The cybersecurity of the companies critical to the security of supply must be improved by Finnish National Emergency Supply Agency (huoltovarmuuskeskus (HVK)). This is done by providing resources for a program called KYBER2020 which aims to improve cybersecurity of companies.

Ensuring the security of supply is one of the main goals for the second action plan published in 2017 [66]. From energy perspective, the Finnish National Emergency Supply Agency (HVK) assures an uninterrupted availability of energy where ecological sustainability and competitive pricing are among goals too. It is worthwhile mentioning that HVK is an administrative institution of the Ministry of labor and economy. The mission of the institute is to plan and operate the maintenance and development of the activities regarding security of supply in the country. HVK designed sector specific pools where preparedness of the companies in the sector is continuously monitored and developed. It is worthwhile to mention that energy production, transmission and distribution system operators are in the same pool.

4.4.2 Mapping of assets and security events

In Finnish pilot, eight different assets have been identified, as shown in Table 14. Three of them are information systems developed by Enerim. There are also two database servers, one IXS database server, one application server, and one VPN (Virtual Private Network) connection.

Vulnerabilities were identified by means of penetration testings performed on Task 2.2 of the CyberSEAS project and also by researching information from vendors and NVD (National Vulnerability Database).

Table 14 – Mapping of FIN assets and vulnerabilities.

| ID | Asset | CPE v2.3 | Attack Vector | CVE |
|-------|--------------------|---|---------------|--|
| FIN.1 | CIS software | N/A | Network | N/A |
| FIN.2 | Database server 1 | cpe:2.3:a:postgresql:postgresql:12.1:*:*:*:*:* | Network | CVE-2021-43767, CVE-2021-23222, CVE-2021-32028, CVE-2021-32029 |
| FIN.3 | Database server 2 | cpe:2.3:a:mongodb:database_tools:3.6.5:-:*:*:*:* | Network | CVE-2020-7924 |
| FIN.4 | Application server | cpe:2.3:a:microsoft:remote_desktop:1.2.2860:*:*:*:*:windows:* | Network | CVE-2022-24503 |

| | | | | |
|-------|---------------------|--|---------|--|
| FIN.5 | VPN connection | N/A | Network | N/A |
| FIN.6 | IXS software | N/A | Network | N/A |
| FIN.7 | IXS platform | N/A | Network | N/A |
| FIN.8 | IXS database server | cpe:2.3:a:postgresql:postgresql:12.1:*:*:*:*:* | Network | CVE-2021-43767, CVE-2021-23222, CVE-2021-32028, CVE-2021-32029 |

Each asset is mapped to the MITRE ATT&CK Techniques and the corresponding MITRE ATT&CK Mitigations. Table 15 shows the mapping of FIN assets.

Table 15 – FIN mitigation measures.

| ID | Asset | Techniques | Mitigations | Source |
|-------|---------------------|--------------|--|--------|
| FIN.1 | CIS software | T1189 | <ul style="list-style-type: none"> Stop service running on port 3001 | PoC |
| FIN.2 | Database server 1 | T1552 | <ul style="list-style-type: none"> M1027 Password Policies M1026 Privileged Account Management M1022 Restrict File and Directory Permissions M1051 Update Software M1017 User Training | MITRE |
| FIN.3 | Database server 2 | T1587.003 | <ul style="list-style-type: none"> M1056 Pre-compromise | MITRE |
| FIN.4 | Application server | T1505.005 | <ul style="list-style-type: none"> M1047 Audit M1024 Restrict Registry Permissions | MITRE |
| FIN.5 | VPN connection | T1133, T1572 | <ul style="list-style-type: none"> M1042 Disable or Remove Feature or Program M1035 Limit Access to Resource Over Network M1032 Multi-factor Authentication M1030 Network Segmentation M1037 Filter Network Traffic M1031 Network Intrusion Prevention | MITRE |
| FIN.6 | IXS software | T1554 | <ul style="list-style-type: none"> M1045 Code Signing | MITRE |
| FIN.7 | IXS platform | T1027 | <ul style="list-style-type: none"> M1049 Antivirus/Antimalware M1040 Behavior Prevention on Endpoint | MITRE |
| FIN.8 | IXS database server | T1552 | <ul style="list-style-type: none"> M1027 Password Policies M1026 Privileged Account Management M1022 Restrict File and Directory Permissions M1051 Update Software M1017 User Training | MITRE |

4.4.3 Required coordination with CERTs

In Finland, critical infrastructure operators and service providers can voluntarily notify any security incidents in their networks and information systems to the National Cyber Security Centre Finland (NCSC-FI) at the Finnish Transport and Communications Agency TRAFICOM. The voluntary notification is either in the hope of receiving an assistance from the NCSC-FI or to sharing information within a trust network to enhance the national cybersecurity level. In

energy sector, electricity transmission system and high-voltage distribution network operators, Fingrid (main electric grid operator) and Gasgrid Finland Oy (natural gas transmission system operator) are critical infrastructure operators and service providers.

It is worthwhile to mention that in addition to the above mentioned voluntary notification, critical infrastructure operators and service providers must notify any security incident in their networks and information systems to the relevant supervisory authority in the sector. The national energy authority is the supervisory authority in the energy sector.

4.4.4 Defined incident response procedures and rules

The National Cyber Security Centre Finland (NCSC-FI) of the Finnish Transport and Communications Agency TRAFICOM published a report containing instructions for managing data breach incidents [67]. It is indicated that the instructions offer general guidance and recommended organizations to develop a more detailed incident response plan according to their technological and operational environment.

According to the instructions, incident management can be done in five main steps, namely preparation, detection, containment, recovery, and post-incident review:

- The first step is preparation. In this step, the aim is to protect against incidents, reduce severity of incidents and enable fast recovery after incidents. In the step, organizations are recommended to assess their readiness using cyber security evaluation tools and develop their incident response plan. In order for organizations to be well prepared, different measures categorized into administrative measures (e.g., development of the organization incident response plan, training personnel and monitoring the news by the National Cyber Security Centre Finland to be aware of emerging risks and threats) and technical measures (e.g., conducting regular and automatic backup of any critical system in the organization and conducting regular testing of the functioning of the backups) are proposed. The measures are recommended to be taken into apply by organizations during normal situation when there is no ongoing cyber incident. The measures aim at either protecting against cyber incidents to happen, mitigating their consequences or facilitating their detection and management.
- The second step, detection step, is to ensure that the organization is able to detect cyber security incidents. There is a diverse range of approaches to detect an attack since there are many ways an attacker can use to penetrate to a system.
- The third step is the containment step. During this step, the aim is to investigate the incident. The National Cyber Security Centre Finland (NSCS-FI) provided a workflow for investigating a data breach event. It is also recommended to keep a precise event log of all taken measures with information about the party that implemented the measure and timestamp. During this step, documentation is crucial. It is recommended to document any potential evidence with detailed information about the body that gathered the data, what the data was and when and how the data was gathered. The documents and logs facilitate the investigation as well as cooperation with police and information security investigators.

In the containment step, some immediate measures such as stopping the attack from progressing by isolating infected devices are necessary to protect the critical data in the environment, stop the malware from spreading, prevent the attackers from

gaining a foothold in the network and prepare for the next step which is recovery. In addition to the immediate measures, identification information is collected and used to determine the extent of the attack and its impact on the organization. In addition, the actions are necessary to ensure that potential malware and backdoors are removed. Identification information includes but not limited to the time when the incident occurred, when a login to the server occurred and when a certain command was run on the server. Collecting identification information helps to identify harmful activities and thus ensure that all infected devices and identifiers are found and cleaned.

- The fourth step is recovery. The recovery step begins from the systems which are the most critical to the business. In this step, infected systems are restored from backups. It is worthwhile to mention that the process should be done as safely as possible to ensure that the attacker cannot get back into the system. In addition, login information of all of the potentially infected IDs is changed so that the attacker can no longer use the IDs to access the systems. In order to avoid similar attacks in the future, it is recommended to make user login requirements stricter. Once the systems are restored and the IDs are changed, database can be restored from a backup copy to invalidate potential changes made by the attackers.
- The fifth step is to review the attack. This review can be used to update the organization incident response plan to ensure that the organization is protected against a similar incident. In this step, the measures taken during the event are studied to see how the plans and the security level can be improved. In the study, root causes of the incident and effectiveness of the organization protection plan are examined carefully. The National Cyber Security Centre Finland (NCSC-FI) recommends organizations to share their most important lessons learned from incidents to help other organizations too.

4.4.5 Data structures, formats, and tools for reports

In Finland, two reporting processes for incidents exist. The first process is general and applicable to any incident to any individual and organization. This reporting is voluntary. The second process is for some specific essential critical infrastructure operators and service providers. This later incident reporting is mandatory. In the following sections, the two processes are described.

4.4.5.1 Voluntary incident reporting

In Finland, individuals, businesses and organisations can report any realized or attempted information security incidents to the National Cyber Security Centre Finland (NCSC-FI) at the Finnish Transport and Communications Agency Traficom. This way, the NCSC-FI investigates information security violations and disseminates information on security matters to raise general awareness about information security. In addition, NCSC-FI provides support in the technical investigation of severe information security violations.

Reporting an incident is via an online form through the link [Report to us | NCSC-FI \(kyberturvallisuuskeskus.fi\)](https://www.ncsc.fi/kyberturvallisuuskeskus.fi). The process starts by selecting whether the reporter is an individual or representative of an organization. It is worthwhile to mention that the reporting can be done by an anonymous individual as well. The form gives advice on the most common

information security incidents, which makes incident reporting easier. Once the reporting is done, a brief advice is provided. It also provides a link to an online form for reporting the incident to police. Then, finally, the form asks if the reporter would like to receive advice. In order to receive any advice, you have to provide more detailed information about the following items:

- Observation which can be a scam phone call, a data breach, a data leak, etc.
- Organization's industry which can be selected from a predefined list of energy, food supply, finance, high-technology industry, etc.
- The date and time the incident was noticed
- Description of the issue
- Potential impacts of the issue
- Measures taken or planned to be taken
- If an external information security company is hired to investigate the case
- If police report has been filed or not

4.4.5.2 Mandatory incident reporting

In Finland, essential critical infrastructure operators and service providers must notify any security incidents in their networks and information systems to the supervisory authorities in the relevant sector. The supervisory authority in energy sector is the national energy authority. The operators and service providers can also submit a voluntary notification on the incident to NCSC-FI (which was described earlier in this section). The voluntary notification can be done in the hope of receiving an assistance from the NCSC-FI as well as to sharing information within a trust network.

The notification obligation applies to the operators and service providers of the following critical infrastructures:

- Energy
- Digital infrastructure
- Digital services
- Financial sector
- Financial sector infrastructure
- Transport
- Health sector
- Water supply

In energy sector, electricity transmission system and high-voltage distribution network operators, Fingrid (main electric grid operator) and Gasgrid Finland Oy (natural gas transmission system operator) are essential critical infrastructure operators and service providers. The form for reporting the incident is depicted in Figure 33 and Figure 33. According to the form, information of the incident includes an informal description of the matter, the service which has been affected by the incident as well as the date and time of the incident or incident detection. The form has two sections, basic information section and information on the incident section. The two sections of the form are depicted in the following figures.

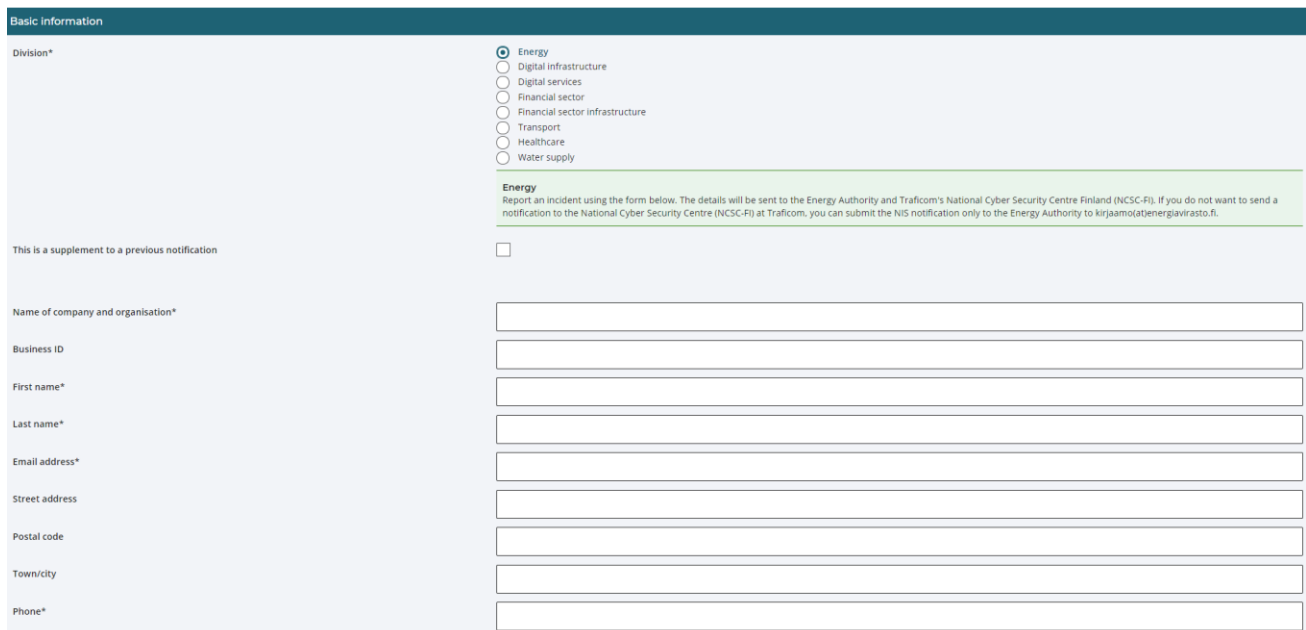


Figure 32 – FIN incident reporting form – basic information.

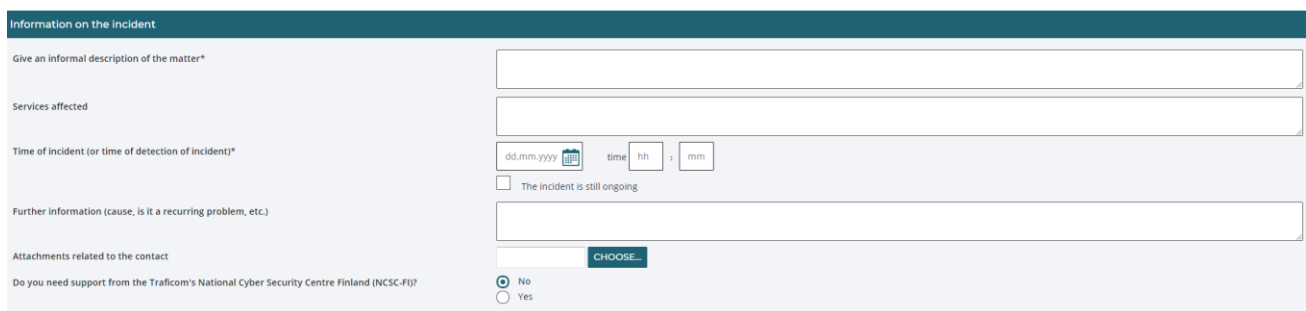


Figure 33 – FIN incident reporting form – information on the incident.

The form can be accessed through the link [Report a security incident \(NIS notification obligation\) | Traficom](#). Essential critical infrastructure operators and service providers can submit a voluntary form to NCSC-FI too.

4.4.6 Communication strategy and information sharing mechanisms

In 2011, the Finnish Transport and Communications Agency (Traficom) produced HAVARO as a service. HAVARO is used for detecting serious information security threats affecting Finnish companies and for issuing related alerts [68]. At the core of the HAVARO service is a technical monitoring system that utilises sensors to observe a customer company's telecommunications. The system detects serious information security threats, such as Advanced Persistent Threats (APT), and data-stealing malware. Data on the anomalies is analysed and, if an anomaly turns out to be an information security threat, the customer organisation is warned about the threat. The HAVARO service is based on maintaining national situational awareness of cyber security and ensuring the security of supply. The service is primarily aimed at companies and organisations critical for the security of supply,

but it can also be offered to other organisations. However, customers must meet certain conditions, including that all parties need to fulfil the obligations of the GDPR and other data protection legislation.

HAVARO generates data on the detection of common and serious information security threats in Finland. With the information, the NCSC-FI builds nationwide situational awareness of cyber security, which is used to improve the reliability and security of communications networks and services and to increase understanding of information security for the benefit of all participating organisations. HAVARO is not intended as the only information security solution of an organisation. It complements other information security solutions in a security-aware organisation. HAVARO is a part of the overall information security solution in a company. All Finnish organisations that want to improve both the level of their own information security and the national cyber security can become HAVARO users. Organisations are free to decide whether they want to make it publicly known that they are using the service.

In addition to HAVARO, the National Cyber Security Centre Finland (NCSC-FI) recommended organizations to report data breach incidents to them once the incident is detected. This is to support the national information security situation awareness as well as to help and warn other potential victims. The National Cyber Security Centre Finland also provides confidential and free of charge advice on how to limit the damage, assess the incident and take recovery measures.

In addition to that, the National Cyber Security Centre Finland (NSCS-FI) recommends organizations to review incidents they experienced and use that review to update their incident respond plan. The National Cyber Security Centre Finland (NSCS-FI) recommends the organizations to share their most important lessons learned from the experienced incidents to help other organizations too. This way, the National Cyber Security Centre Finland (NSCS-FI) aims at enhancing the national cybersecurity level.

Finally, TRAFICOM provided information exchange practices for cooperation groups [69] to ensure that information is distributed and processed in an appropriate way. According to TRAFICOM, information processing and dissemination in cooperation groups should be according to the Traffic Light Protocol (TLP) classification system and the Chatham House Rule. These are rules that are based on voluntary participation, with the aim of encouraging open information exchange. The Chatham House Rule governs information exchange in the context of meetings and briefings, whereas the Traffic Light Protocol system relates to the exchange of documents and information in a more general sense. All those who take part in the processing of information must take care to ensure that the rules are observed. Furthermore, the recipient of the information must obtain the consent of its originator in order to carry out more extensive processing of the information. The classifications are not legally binding, but based on mutual trust among people and organisations.

4.5 Estonian pilot scenarios

This section describes Estonian regulations and how CERTs interact with vital service providers. Additionally, we bring out different mappings based on our assets and security events. The summary of those Estonian pilot's scenarios are following:

- **M1032: Privilege access management (PAM) – Multi-factor Authentication:** This scenario requires multi-factor authentication for all delegated administrator accounts, which helps to ensure that only authorized individuals have access to sensitive systems and data.
- **M1018: Identity access management (IAM) – User Account Management:** This scenario focuses on adequately managing accounts and permissions used by parties in trusted relationships to minimize potential abuse by the party and if an adversary compromises the party. This is important to prevent unauthorized access to sensitive systems and data.
- **M1027: Process management – Password Policies:** This scenario focuses on changing default usernames and passwords immediately after installing applications and appliances and before deployment to a production environment. This helps to prevent unauthorized access and to protect sensitive systems and data.
- **M1053: Backup Management – Data Backup:** This scenario highlights the importance of implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data. This helps to ensure that essential data can be restored during a cyber incident.
- **M1041: Information Management – Encrypt Sensitive Information:** This scenario recommends encrypting vital information to reduce an adversary's ability to perform tailored data modifications. This is important to protect sensitive information from unauthorized access and manipulation.

These scenarios are designed to protect critical infrastructure and vital services from cyber threats by implementing best practices for incident response, such as multi-factor authentication, proper account management, protection of sensitive information, and by having disaster recovery plans that include regular data backups and encryption of sensitive data. These scenarios are also subject to regular updates in order to keep pace with the evolving threat landscape.

4.5.1 Underlying national regulations

Estonia has implemented several laws and regulations related to cybersecurity incident response to protect its critical infrastructure and vital services from cyber threats. The primary legislation is the Cyber Security Act of the Republic of Estonia, passed in 2017 [70]. This law establishes a national cybersecurity strategy, a framework for incident response, and the responsibilities of various government agencies and private sector organizations in protecting critical infrastructure and vital services from cyber threats.

The law establishes the Computer Emergency Response Team Estonia (CERT-EE), responsible for coordinating the response to cyber incidents and providing guidance and support to organizations affected by cyber threats. CERT-EE is also a main point of contact for national and international cyber incident response [70].

The law also requires organizations that operate critical infrastructure or provide vital services to have incident response plans and to report certain types of cyber incidents to the authorities. The law also allows the authorities to take specific measures, such as shutting down networks or blocking access to certain websites, in order to protect against cyber threats [70].

In addition, Estonia has implemented the EU's Network and Information Systems (NIS) Directive (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union) [71], which requires certain types of organizations to take appropriate security measures to protect their networks and information systems and report certain incidents to the authorities.

Overall, Estonia has put in place a robust legal framework for cybersecurity incident response, which includes clear roles and responsibilities for government agencies and private sector organizations, as well as incident reporting and incident response requirements. These laws and regulations provide a framework for effective incident response and help to ensure the security and resilience of Estonia's critical infrastructure and vital services.

4.5.2 Mapping of assets and security events

Each group of EST assets is mapped to relevant MITRE ATT&CK Mitigations, which correspond to appropriate incident response procedures. This mapping is presented in Table 16.

Table 16 – Mapping of EST assets to applicable mitigation measures.

| Mitigation ID | Asset Group | Mitigation | Description |
|-----------------------|-----------------------------|---|---|
| M1032 | Privilege Access Management | Multi-factor Authentication | Require MFA for all delegated administrator accounts. |
| M1030 | Firewall | Network Segmentation | Network segmentation can be used to isolate infrastructure components that do not require broad network access. |
| M1018 | Identity Access Management | User Account Management | Properly manage accounts and permissions used by parties in trusted relationships to minimize potential abuse by the party and if the party is compromised by an adversary. In Office 365 environments, partner relationships and roles can be viewed under the "Partner Relationships" page. |
| M1027 | Process Management | Password Policies | Applications and appliances that utilize default username and password should be changed immediately after the installation, and before deployment to a production environment. When possible, applications that use SSH keys should be updated periodically and properly secured. |
| M1026 | Privilege Access Management | Privileged Account Management | Audit domain and local accounts as well as their permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account. These audits should also include if default accounts have been enabled, or if new local accounts are created that have not been authorized. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers. |

| | | | |
|-----------------------|--------------------------|---|---|
| M1053 | Backup Management | Data Backup | Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.[48] Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery. |
| M1028 | Configuration Management | Operating System Configuration | Consider technical controls to prevent the disabling of services or deletion of files involved in system recovery. |
| M0805 | Layers Management | Mechanical Protection Layers | Protection devices should have minimal digital components to prevent exposure to related adversarial techniques. Examples include interlocks, rupture disks, release valves, etc. |
| M0812 | Systems Management | Safety Instrumented Systems | Ensure that all SIS are segmented from operational networks to prevent them from being targeted by additional adversarial behavior. |
| M1041 | Information Management | Encrypt Sensitive Information | Consider encrypting important information to reduce an adversary's ability to perform tailored data modifications. |
| M1029 | Storage Management | Remote Data Storage | Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data. Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and manipulate backups. |
| M1022 | Permissions Management | Restrict File and Directory Permissions | Ensure least privilege principles are applied to important information resources to reduce exposure to data manipulation risk. |
| M1051 | Software Management | Update Software | A patch management process should be implemented to check unused dependencies, unmaintained and/or previously vulnerable dependencies, unnecessary features, components, files, and documentation. |
| M1016 | Scanning Management | Vulnerability Scanning | Continuous monitoring of vulnerability sources and the use of automatic and manual code review tools should also be implemented as well. |

4.5.3 Required coordination with CERTs

Estonia has implemented a robust legal framework for cybersecurity incident response, which includes the establishment of the Computer Emergency Response Team Estonia (CERT-EE) as the main coordination point for incident response. CERT-EE is responsible for coordinating the response to cyber incidents and providing guidance and support to organizations affected by cyber threats, including vital services such as healthcare and energy.

CERT-EE also acts as the point of reference for network users for solving any computer security problem. This allows organizations to quickly and effectively respond to cyber incidents and

minimize the impact of such incidents on critical infrastructure and vital services. In addition to coordinating incident response, CERT-EE also plays a key role in the development and implementation of national cybersecurity policies and strategies [70].

CERT-EE also cooperates with other national and international CERTs, such as the European Union's Computer Emergency Response Team (CERT-EU) and the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), to share information and best practices and to coordinate incident response efforts. This cooperation allows Estonia to respond effectively to cross-border cyber incidents and to enhance the security and resilience of its critical infrastructure and vital services.

Estonia's incident response framework is also aligned with international standards and best practices, such as the ISO/IEC 27035 standard for incident management [9] and the NIST Cybersecurity Framework (CSF) [72]. This alignment helps to ensure that incident response efforts are effective and efficient and that they meet the needs of organizations operating critical infrastructure and vital services.

Overall, Estonia's CERT-EE plays a vital role in ensuring the security and resilience of the country's critical infrastructure and vital services by coordinating incident response efforts and providing guidance and support to organizations affected by cyber threats.

4.5.4 Defined incident response procedures and rules

In Estonia, the Cyber Security Act defines incident response procedures and rules for vital services and aligned with international standards and best practices. The main elements of these procedures and rules are as follows:

- Organizations that operate critical infrastructure or provide vital services must have incident response plans, which include procedures for identifying, assessing, and responding to cyber incidents. These plans should be regularly reviewed and updated to remain adequate and relevant.
- Organizations are required to report certain types of cyber incidents to the authorities, including those that significantly impact the availability, integrity, or confidentiality of the organization's networks or information systems.
- The authorities can take specific measures, such as shutting down networks or blocking access to certain websites, to protect against cyber threats.
- Organizations must comply with international standards and best practices, such as the ISO/IEC 27035 standard for incident management and the NIST Cybersecurity Framework, to ensure that incident response efforts are effective and efficient.
- The incident response procedures and rules are regularly reviewed and updated to keep pace with the evolving threat landscape and ensure that they remain effective and relevant.

4.5.5 Data structures, formats, and tools for reports

In Estonia, the data structures and formats for incident reports for vital services are defined by the Cyber Security Act [70] and the EU's Network and Information Systems (NIS) Directive [71]. Organizations are required to report certain types of cyber incidents to the authorities,

including those that significantly impact the availability, integrity, or confidentiality of the organization's networks or information systems.

To facilitate incident reporting, the Cyber Security Act and the NIS Directive require organizations to use standard incident reporting forms and to provide specific information about the incident, such as the date and time of the incident, the type of incident, the affected systems and networks, and the impact of the incident.

For example, the Estonian Information System Authority (RIA) provides an incident reporting form on its website (<https://raport.cert.ee/>), which organizations can use to report cyber incidents. The form requires organizations to provide information such as the date and time of the incident, the type of incident, the affected systems and networks, and the impact of the incident. Organizations must also provide contact information so that RIA can follow up with them regarding the incident.

In addition to standard incident reporting forms, organizations are also required to use specific tools for incident reporting, such as the EU's CSIRT (Computer Security Incident Response Team) Notification Format [73], which is a standardized format for reporting cyber incidents to national and international incident response teams. This format helps to ensure that incident reports are complete, accurate, and consistent, which is essential for effective incident response.

Overall, the data structures and formats for incident reports in Estonia are designed to facilitate incident reporting and to ensure that incident reports are complete, accurate, and consistent. These structures and formats help to ensure that organizations can effectively respond to cyber incidents and minimize the impact of such incidents on vital services.

4.5.6 Communication strategy and information sharing mechanisms

The Computer Emergency Response Team Estonia (CERT-EE) has several communication strategies and information-sharing mechanisms to effectively coordinate incident response efforts and provide guidance and support to organizations affected by cyber threats, especially vital services. The most important points include the following:

- **Real-time incident response:** CERT-EE uses real-time incident response mechanisms to quickly and effectively respond to cyber incidents, such as by providing guidance and support to organizations affected by the incident and coordinating with other national and international CERTs to share information and best practices.
- **Information sharing:** CERT-EE uses various information-sharing mechanisms to disseminate information about cyber threats, vulnerabilities, and incidents to organizations, including vital services. These mechanisms include email alerts, RSS feeds, and social media.
- **Technical support:** CERT-EE provides technical support to organizations affected by cyber incidents, including vital services such as healthcare and energy, by guiding how to mitigate the incident and assisting with incident response efforts.
- **Coordination with other CERTs:** CERT-EE coordinates with other national and international CERTs, such as the European Union's Computer Emergency Response Team (CERT-EU) and the NATO Cooperative Cyber Defence Centre of Excellence

(CCDCOE), to share information and best practices and to coordinate incident response efforts.

- **Public awareness:** CERT-EE also raises public awareness about cybersecurity and cyber threats by providing information and guidance to individuals and organizations on protecting themselves from cyber threats.

5 Common procedures and rules (new)

This section proposes unified procedures, tools, and rules for coordination and reporting to CERTs in the common EU space aligned with EU legislation, the established standards, and the national specifics described in Section 4.

5.1 Comparative overview of rules and tools

Section 4 defined incident response procedures and rules thoroughly on the national level based on the contributions of CyberSEAS pilots. We compiled the practices for all pilots and their countries: ITA, SLO&CRO, ROM, FIN, and EST.

There are many parallels between national incident response procedures, rules, strategies, acts, and decrees. This is due to the common obligations in alignment with the NIS Directive. We can therefore make a comparative overview of rules and tools. This allows us to analyze the similarities, parallels, and differences. On their basis, we can establish unification patterns, recommendations, and common rules for the EU space.

Section 5.1 provides a compact comparative presentation (in the structured tabular format) of incident response procedures and rules defined in Section 4 on the national level based on the contributions of five CyberSEAS pilots. We analyze to what extent they match. For the comparison, we consider five aspects:

- Underlying national regulations
- Required coordination with CERTs
- Incident response procedures and rules
- Data structures, formats, and tools for reports
- Communication strategy and information-sharing mechanisms

Table 17 compares the underlying national regulations of five pilot countries. The regulations determine how rules and tools for coordination between EPES operators and national CERTs should be implemented.

Table 17 – Comparison of pilot countries according to underlying national regulations.

| Country | Underlying national regulations |
|---------|---|
| ITA | Under the EU NIS Directive Italian cybersecurity regulations are further strengthened through the establishment of the national cybersecurity perimeter and its implementing decrees |
| SLO | Information Security Act (ISA) implementing the EU NIS Directive Electronic Communications Act (Version 2) General Data Protection Act (version 2) |
| ROM | Under the EU NIS Directive and the General Data Protection Act (Version 2) |

| | |
|-----|---|
| | The National Law No. 362/2018 establishes CERT-RO and sets the requirements for OESs and DSPs to implement IR, ensure continuous operations, and report to CERT-RO |
| FIN | Under the EU NIS Directive General Data Protection Act (Version 2) Data Protection Act (1050/2018) supplementing GDPR Act on Electronic Communications Services (917/2014) Criminal Code of Finland (39/1889) |
| EST | Under the EU NIS Directive The National Cyber Security Act of the Republic of Estonia establishes CERT-EE and sets the requirements to implement IR, secure the infrastructure, and report to CERT-EE Best practices including ISO/IEC 27035 and the NIST Cybersecurity Framework (CSF) |

There are no significant discrepancies to be noticed between different EU countries. They are all under the EU NIS Directive [5]. Some other acts are also followed in most countries, most notably the General Data Protection Regulation (GDPR) [74], the European Electronic Communications Code [75], and several national laws establishing national CERTs and their responsibilities. In addition, some common practices and standards are considered, such as ISO/IEC 27035 [9] and the NIST Cybersecurity Framework (CSF) [6]. This means that EU countries are well-prepared to implement operators' coordination and reporting to CERTs in case of cybersecurity incidents. To address this aspect, Table 18 compares the practices of EU countries regarding the required coordination with CERTs.

Table 18 – Comparison of pilot countries according to the required coordination with CERTs.

| Country | Required coordination with CERTs |
|---------|--|
| ITA | Italian CSIRT is a single authority under the NIS Directive Italian CSIRT cooperates with other EU CSIRTs Operators of essential services (OESs) and digital service providers (DSPs) must forward to the Italian CSIRT notifications of IT/OT incidents with a significant impact on the services provided |
| SLO | Slovenian CSIRT provides essential support and is linked to the wider EU CSIRT community The EU NIS Directive is followed to establish the coordination with CSIRTs Mandatory and voluntary reporting Any incident with a significant impact affecting the ability to provide essential services must be immediately reported to the national CSIRT |

| | |
|-----|---|
| | Slovenian CSIRT is also recognized as the entity that coordinates activities of vulnerability handling and vulnerability disclosure |
| ROM | CERT-RO is the main authority CERT-RO operates 24/7 and can be reached through various contact channels; coordination is required under the EU NIS Directive |
| FIN | NCSC-FI (National Cyber Security Centre Finland) is the main authority Critical infrastructure operators and service providers can voluntarily notify any security incidents in their networks and information systems to NCSC-FI to receive assistance and share information within the trusted community Mandatory reporting of security incidents is also required to the relevant supervisory authority in the sector (i.e., the National Energy Authority) |
| EST | CERT-EE (Computer Emergency Response Team Estonia) is the main coordination point for incident response and support to organizations affected by cyber threats CERT-EE cooperates with other CERTs, such as CERT-EU (European Union's Computer Emergency Response Team) and CCDCOE (NATO Cooperative Cyber Defense Centre of Excellence) to share information and best practices and to coordinate incident response efforts |

The coordination with CERTs in different EU countries is established upon common rules and procedures. Each country has a national CERT representing the single central authority under the NIS Directive. National CERTs are linked to the wider EU CSIRT community to coordinate incident response activities and share information. National CERTs are therefore recognized as the entities authorized for incident and vulnerability handling and disclosure. OESs and DSPs must immediately report to the national CERT any cyber incident with a high impact. In addition to mandatory reporting, voluntary reporting is also recommended in each country.

Hence, there are many parallels in incident reporting to national CERTs in different countries. This allows us to establish a common EU space for cyber incident response. Table 19 reviews and compares national practices in incident response procedures and rules.

Table 19 – Comparison of pilot countries according to incident response procedures and rules.

| Country | Incident response procedures and rules |
|---------|--|
| ITA | The incident response process refers to ISO 27001 and ISO 27035: (1.) preparation, (2.) detection & analysis, (3.) containment, eradication, & recovery, and (4.) post-incident activity Operators follow the rules to notify the specific entities in charge of operating on the infrastructure in the case of a cyber event |
| SLO | National Incident Handling Process: (1.) preparation, (2.) detection & analysis, (3.) containment, eradication, & recovery, and (4.) post-incident activity The National Cybersecurity Incident Response Plan (NOKI) specifies the details for reporting, such as the taxonomy for the categorization of incidents, |

| | |
|-----|--|
| | <p>definitions of severity levels, methods for determining the severity of incidents, reporting timeframes for obligatory reporting, etc.</p> <p>Internal incident response procedures, rules, and plans are defined for the EPES stakeholders</p> |
| ROM | <p>Incident response process: (1.) preparation, (2.) detection & analysis, (3.) containment, eradication & recovery, and (4.) post-incident activity</p> <p>CERT-RO has the primary responsibility for incident response, however, all organizations managing the critical infrastructure are also expected to have their incident response plans and teams</p> <p>Plans must include appropriate procedures and rules for incident notification, communication, preservation of evidence, and post-incident analysis</p> |
| FIN | <p>Incident response process: (1.) preparation, (2.) detection & analysis, (3.) containment, eradication & recovery, and (4.) post-incident activity</p> <p>NCSC-FI published a report containing general instructions for organizations to develop a more detailed incident response plan according to their technological and operational environments</p> |
| EST | <p>The Cyber Security Act defines incident response procedures and rules for vital services aligned with ISO 27035 and the NIST Cybersecurity Framework to cover all standard IR phases: (1.) preparation, (2.) detection & analysis, (3.) containment, eradication & recovery, and (4.) post-incident activity</p> <p>Organizations that operate critical infrastructure or provide vital services must have incident response plans and reporting rules defined</p> <p>The authorities can take specific measures after cyber incidents are reported</p> |

Again, we can draw common rules and procedures for the EU space. All countries implement the ISO 27035 incident response process consisting of four standard phases: (1.) preparation, (2.) detection & analysis, (3.) containment, eradication & recovery, and (4.) post-incident activity. In addition, all organizations that operate critical infrastructure or provide essential services must have internal response plans, procedures, and teams in place. CERTs as single authorities can take specific measures. They are also entitled to specify detailed rules that EPES operators should implement and follow.

Although general incident response, coordination, and reporting procedures are aligned and standardized, they may utilize various data structures, formats, and tools for reporting. Table 20 gives a comparison of the latter.

Table 20 – Comparison of pilot countries according to data structures, formats, and tools for reports.

| Country | Data structures, formats, and tools for reports |
|---------|--|
| ITA | <p>There are currently no standards for data structures, formats, and tools for reporting</p> <p>Recommended use of STIX, TAXII, and TLP</p> |

| | |
|-----|---|
| | On the CSIRT website, it is possible to compile an online format specifying the characteristics of the cyber attack one has faced |
| SLO | <p>SI-CERT follows several data feeds for systems in Slovenia that show newly discovered vulnerabilities or unusual behavior that may be the result of cybersecurity incidents</p> <p>Reports can be sent via e-mail</p> <p>Currently, information is supplied in the format determined by the reporting part</p> <p>NOKI provides templates for reporting as the suggested format</p> <p>A common platform for structured reporting might be available in the future</p> |
| ROM | <p>There are currently no standards for data structures, formats, and tools for reporting</p> <p>Three ways of reporting and processing: (1.) automatic processing of alerts sent through automated systems, (2.) manual processing of individual alerts by CERT-RO analysts, and (3.) collecting of information from various sources by CERT-RO</p> |
| FIN | <p>Online incident reporting form, which has standard input fields and provides advice on reporting</p> <p>Applied for voluntary and mandatory incident reporting</p> |
| EST | <p>The data structures and formats for incident reports are defined by the Cyber Security Act and the NIS Directive</p> <p>Organizations are required to use standard incident reporting forms and provide specific information about the incident, such as the date and time of the incident, the type of incident, the affected systems and networks, and the impact of the incident</p> <p>The Estonian Information System Authority provides the incident reporting form on its website</p> <p>Organizations can also use specific tools for incident reporting, such as the EU's CSIRT Notification Format</p> |

This aspect is currently not well standardized. There are no established international standards for data structures, formats, and tools for reporting cyber incidents. Different countries use different approaches, and there can even be a variety of formats, tools, and mechanisms supported in a single EU country. The most common approach is the incident reporting form accessible on the CERT's website. This reporting format is facilitated in many EU countries, including ROM, FIN, and EST. However, many other formats and tools are available, such as STIX, TAXII, TLP, CSIRT Notification Format, e-mail, system integrations, etc. For this reason, we propose a standard reporting format based on the NOKI reporting object and the use of the MISP CTI exchange platform. This approach is described in Section 5.3. In this way, we aim to unify and standardize incident reporting formats and tools in the EU space.

The last analyzed aspect pertains to the communication strategy and information-sharing mechanisms. We summarize the comparison of EU countries represented by the CyberSEAS pilots in Table 21.

Table 21 – Comparison of pilot countries according to the communication strategy and information-sharing mechanisms.

| Country | Communication strategy and information-sharing mechanisms |
|---------|--|
| ITA | <p>Strategic and operational communication consists of developing the coordination capacity for situational awareness</p> <p>If an incident occurs, the PA Information Security Contact Person of Benetutti involves the regional CERT, sending, through shared channels, a formal request for support in handling the incident in progress</p> <p>The request must include all the details necessary for the regional CERT to be able to carry out the analysis and provide the information needed to process the incident</p> <p>At the same time as the request for support, the security contact person submits the operational plan to the regional CERT</p> |
| SLO | <p>In communication between OESs and SI-CERT, the TLP protocol is used</p> <p>OESs (and other entities, such as government institutions) are encouraged to join the local MISP network for faster IoC sharing</p> <p>Possible specific internal strategies and mechanisms include: (1.) the response management group, (2.) the notification of business partners and individuals, and (3.) rules to implement the communication strategy between SOCs, DSOs, and the national CERT</p> |
| ROM | <p>Information exchange among teams, companies, and the CERT</p> <p>Three communication strategies: (1.) automatic processing of alerts sent through automated systems, (2.) manual processing of individual alerts by CERT-RO analysts, and (3.) collecting of information from various sources by CERT-RO</p> |
| FIN | <p>Information processing and dissemination in cooperation groups is according to the TLP protocol and the Chatham House Rule</p> <p>HAVARO service is used for detecting serious information security threats affecting Finnish companies and for issuing related alerts</p> <p>HAVARO is based on maintaining national situational awareness of cyber security and ensuring the security of supply</p> <p>NCSC-FI recommends organizations to do the following: (1.) report incidents to them to review incidents they experienced and use reviews to update their incident response plan, (2.) internally review incidents they experienced and use reviews to update their incident response plan, and (3.) share their most</p> |

| | |
|-----|--|
| | important lessons learned from the experienced incidents to help other organizations too |
| EST | CERT-EE has several communication strategies and information-sharing mechanisms to effectively coordinate incident response efforts and provide guidance and support to organizations affected by cyber threats: (1.) real-time incident response, (2.) information sharing, (3.) technical support, (4.) coordination with other CERTs (e.g., CERT-EU, CCDCOE), and (5.) public awareness |

Here, several communication strategies and information-sharing mechanisms are applied by different EU countries and even within individual countries. These strategies have many strengths and account for various situations. However, due to high diversity, it can be challenging to use all strategies consistently to adhere to the NIS 2 Directive in the common EU space. Therefore, we propose a consolidated approach dealing with the communication strategy and information-sharing mechanisms in the follow-up sections of this document. It is based on the utilization of MISP and SAPPAN tools.

5.2 Unification patterns and rules for the common EU space

In Section 5.1, we performed a direct comparison of national incident response procedures, rules, strategies, acts, and decrees based on the contributions of CyberSEAS pilots to identify the parallels between EU Member States. Here, we draw from this comparison to analyze the common obligations and the alignment with legislation and standards, particularly with the NIS 2 Directive [4], CER (Critical Entities Resilience) Directive [76], and NCC (Network Code on Cybersecurity) [77]. This allows us to verify the adherence of practices in EU Member States with European regulatory frameworks and to establish the unification patterns and rules for the common EU space.

NIS 2, CER, and NCC are of particular interest to the entities in the EPES system. They entered into force recently and will significantly shape the future of cybersecurity efforts in the EU. The NIS 2 Directive (Directive on measures for a high common level of cybersecurity across the Union) [4] prescribes cybersecurity risk-management measures, reporting obligations, the use of European cybersecurity certification schemes, governance, and standardization. For D6.8, reporting obligations are of key relevance. NIS 2 sets the following requirements for Member States:

- Each Member State must ensure that essential entities notify, without undue delay, its CSIRT or, where applicable, its competent authority of any incident with a significant impact on the provision of their services.
- In the case of a cross-border or cross-sectoral significant incident, Member States must ensure that their single points of contact are provided in due time with relevant information.
- Member States must ensure that essential entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients can take in response to the threat.

- Reporting to the CSIRT is required in case of high-impact incidents, including an early warning in 24 hours, an incident notification in 72 hours, a final report in one month, and the progress report for an ongoing incident upon request.
- CSIRT is due to provide a response and a cross-border notification across the Member States. Where public awareness is necessary, CSIRT must also inform the public about a significant incident.
- CSIRT provides the competent authorities with information about significant incidents.
- The single point of contact submits to ENISA a summary report every three months.

It is to be noticed that the type of information, the format, and the notification procedure are not yet standardized. The Commission may adopt implementing acts further specifying these mechanisms and rules.

The CER Directive (Directive on the resilience of critical entities) [76] aims to enhance the resilience of critical entities, such as providers of essential services, in the internal market by laying down harmonized minimum rules and assisting them through coherent and dedicated support and supervision measures. The strategy for the resilience of critical entities must be established in each EU country, incorporating strategic objectives, priorities, measures, main authorities, relevant stakeholders, the governance framework, the policy framework, and the process to identify and support critical entities. The CER Directive introduces, among others, the following requirements for Member States:

- Establishment of one or more competent authorities and a single point of contact
- Establishment of risk assessment procedures carried out by critical entities accounting for all relevant natural and man-made risks, which could lead to an incident
- Establishment of resilience measures to prevent incidents from occurring, respond to them, recover from them, mitigate their consequences, and raise awareness
- Incident notification, cooperation, and reporting, such that critical entities notify the competent authority, without undue delay, of incidents that have the potential to disrupt the provision of essential services significantly

The Network Code on Cybersecurity (NCC) [77], introduced by the ENTSO-E network, aims to set a European standard for the cybersecurity of cross-border electricity flows. It addresses cyber risk assessment, common minimum requirements, crisis management, cybersecurity certification of products and services, monitoring, and reporting. Several security measures are proposed for critical service providers. They should:

- Implement processes for secure design, development, and production
- Implement vulnerability management, including monitoring, prioritizing, mitigating, and reporting vulnerabilities to CSIRTs
- Protect access to customer assets, including background verification checks, access limitations, protection measures, and notifying customers about security incidents

Table 22 identifies the common rules and tools for EPES operators to coordinate with CERTs and provide them with reports on cyber incidents. These rules and tools are inferred from the national practices of Member States reported by the five CyberSEAS pilots. They also consider the requirements of the most relevant European legislative frameworks described above, i.e., NIS 2, CER, and NCC.

Table 22 – Common rules and tools for operators' coordination and reporting.

| Aspect | Implementation |
|---|--|
| Underlying regulations | Based on the NIS Directive, ISO 27001/27035, GDPR, and specific national decrees |
| Required coordination with CERTs | Operators of essential services and digital service providers are obliged to forward notifications of cyber incidents with a significant impact to national CSIRTs |
| Procedures and rules for incident response | Based either on the ISO 27001/27035 IT governance or the NIST IR process consisting of preparation, detection & analysis, containment, eradication & recovery, reporting, and post-incident activities |
| Data structures, formats, and tools for reports | Standardized IR forms, automated processing of alerts from integrated systems, specific tools for incident reporting (such as the EU's CSIRT Notification Format), STIX/TAXII, and TLP |
| Communication strategy and information-sharing mechanisms | Real-time incident response, information sharing, technical support, cross-border cooperation and coordination with other CERTs, public and situational awareness |

As presented in the above table, we could identify and propose several unified standards, rules, procedures, and tools for coordination and reporting in the common EU space. We will introduce and present some of these mechanisms in detail in the follow-up sections of the document. However, these mechanisms must be consistent with the European legislation related to critical infrastructures and essential services. For this reason, we analyze their alignment with the NIS 2 Directive, the CER Directive, and the NCC Code in Table 23.

Table 23 – Alignment with legislative frameworks.

| Analyzed aspect | Alignment with NIS and NIS 2 | Alignment with CER | Alignment with NCC |
|----------------------------------|--|--|---|
| Underlying regulations | The implementation follows NIS and is prepared for NIS 2. | The implementation covers all aspects of CRR. | The implementation covers most aspects of NCC. |
| Required coordination with CERTs | Reporting obligations are fully addressed. Obligatory and voluntary reporting are supported. National CSIRT is a single point of contact and the national authority. | Expected obligations regarding reporting, notification, and coordination are fully addressed. National CSIRT is a single point of contact and the national authority. | Reporting obligations are addressed. Notification rules must be specified as a part of broader incident response procedures and rules. |

| | | | |
|---|--|--|---|
| | Response times and coordination in two ways (from operators to CERTs, and vice-versa) must be specified with the established incident response procedures and rules. | Response times and coordination in two ways (from operators to CERTs, and vice-versa) must be specified with the established incident response procedures and rules. | |
| Procedures and rules for incident response | Management of cybersecurity risks and standardization. | Establishment of procedures and measures to respond to incidents, recover from them, mitigate their consequences, and raise awareness. | Risk assessment, monitoring, and notifications about significant incidents. |
| Data structures, formats, and tools for reports | Not yet prescribed by NIS 2 – the proposed practices exceed NIS 2 requirements. | Not yet prescribed by CER – the proposed practices exceed CER requirements. | Not yet prescribed by NCC – the proposed practices exceed NCC requirements. |
| Communication strategy and information-sharing mechanisms | Single point of contact, cross-border cooperation, and two-way coordination. | Single point of contact, notification mechanisms, two-way cooperation, and CTI exchange on risk assessment and resilience measures. | Coordination and the implementation of vulnerability and crisis management. |

There are several parallels between NIS 2, CER, and NCC. The unified procedures, rules, and tools meet most of the requirements set by these three legislative frameworks. However, we can observe some aspects where our work presented in the D6.8 deliverable advances the current state of regulations. In particular, we propose uniform data structures, formats, and tools for reporting, which are not yet prescribed by any of the three frameworks, NIS 2 being the only of the three to indicate that the Commission may adopt implementing acts further specifying the mechanisms and rules to standardize the type of information, the format, and the notification procedure. This means that D6.8 may provide valuable recommendations and practices for the EU to enhance incident response, coordination, and reporting to CERTs.

The NIS 2 Directive underscores the importance of standardized cyber incident reporting and CTI sharing among European Member States. In adherence to these regulatory requirements, the EU expects organizations to follow standardized reporting mechanisms. These mechanisms can be integrated with playbooks to standardize and, where feasible, automate the associated incident response processes. Additionally, compliance necessitates the establishment of a formal, machine-readable playbook format and a multi-level process framework. This framework should encompass the integration of various abstraction levels, the use of unstructured formats for the capture of knowledge and

metadata, the application of graphical modeling notations, and the translation into executable versions with appropriate mapping schemes. We introduce this approach in Section 5.4.

5.3 Recommendations for standardized reporting and coordination with CERTs

There is a lack of a common standardized reporting format within the EU. Therefore, we will suggest an alternative approach to reporting that could partially be adopted by other EU countries. We focus on the reporting rules in Slovenia, where reporting is currently done by email with an attached NOKI form Microsoft Word document that the entities have to fill out. In the current state of practice, all the work has to be done manually, which is time-consuming. An alternative recommendation for standardized reporting would be to use the MISP object describing the incident in a standardized reporting format. The NOKI form, which is translated into the MISP object, provides all of the necessary reporting fields including the recommended values of specific fields. The object can be attached to a specific MISP event that describes the incident type and its CTI. Together with the MISP features, such as event report, timeline, and relations between the provided CTI data, the reporter can provide the relevant incident reporting body with all the information regarding the incident. In this way, all the information can be included in the event combining everything needed for a better understanding of the incident and automation, such as situational awareness and other automated data processing. The structure of the NOKI object with its fields can be seen in Figure 34. It shows the definition of the NOKI object in the JSON notation.

```
{
  "attributes": {
    "reference-number": {
      "description": "Referenčna številka incidenta (Določi odzivni center)",
      "disable_correlation": true,
      "misp-attribute": "text",
      "multiple": false,
      "ui-priority": 0
    },
    "subject": {
      "description": "Zadeva",
      "disable_correlation": true,
      "misp-attribute": "text",
      "multiple": false,
      "ui-priority": 0
    },
    "report-voluntary": {
      "description": "Prostovoljna prijava incidenta",
      "disable_correlation": true,
      "misp-attribute": "text",
      "multiple": false,
      "ui-priority": 0,
      "values_list": [
        "Prostovoljna prijava incidenta",
        "Prvo poročilo o incidentu zavezanca",
        "Vmesno poročilo o incidentu zavezanca",
        "Končno poročilo o incidentu zavezanca"
      ]
    },
    "reporter-organization": {
      "description": "Naziv subjekta, ki poroča",
      "disable_correlation": true,
      "misp-attribute": "text",
      "multiple": false,
      "ui-priority": 0
    }
  }
}
```

Figure 34 – JSON definition of the MISP NOKI object.

The reporting entity can include the NOKI object in the event describing the incident by selecting the appropriate option from the Add Object dropdown menu and filling out the relevant information about the incident. Figure 35 demonstrates the selection of the NOKI object in MISP, while Figure 36 depicts an MISP event with the NOKI object filled out.

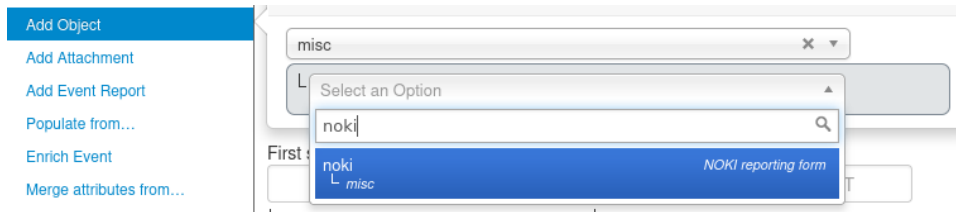


Figure 35 – Selection of the MISP NOKI object.

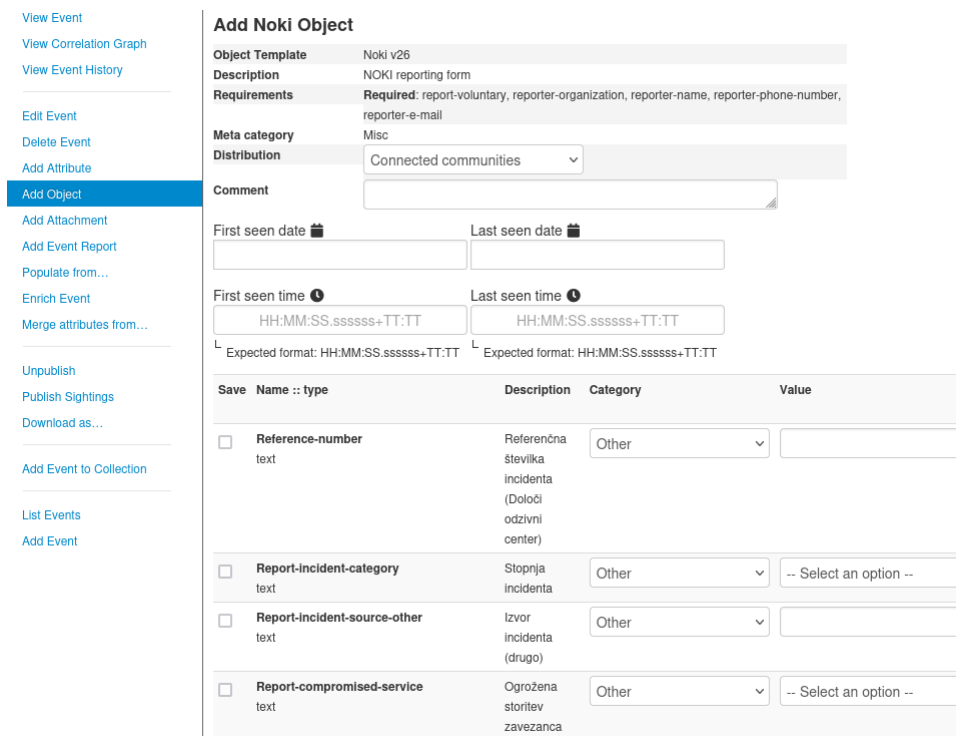


Figure 36 – MISP NOKI object.

The resulting event can be shared with all communities with the MISP feature that enables the restriction of the specific parts related to the NOKI form, event report, and timeline. This can be done by selecting a more limited distribution option limiting the distribution to the current MISP instance or connected communities, depending on the setup. In this way, the NOKI report is only available to the users with access to the MISP instance resulting in adequate restriction to the relevant incident reporting body with access to the entity's MISP instance.

With the described approach, we introduced and proposed:

1. A standardized data structure and format for reports, which is based on the definition of the NOKI object
2. A standardized reporting technology, which utilizes the MISP platform and integration of MISP instances of different cooperating EPES stakeholders in the community

The utilization of the NOKI object allows for (1.) MISP reporting, (2.) sharing of IoCs, and (3.) CTI exchange. MISP and NOKI can hence be regarded as the primary information-sharing mechanism. They consequently shape the communication strategy in full alignment with the requirements of NIS 2, CER, and NCC.

5.4 Standardized response and playbook management for the common EU space

In this section, we standardize playbook management and sharing. We specify conceptual requirements and propose a framework for the incident handling flow. Hence, this section outlines the structured approach to playbook utilization in cybersecurity, focusing on the incorporation of playbook-assisted incident handling and the automation that it entails. Our efforts are directed towards establishing a conceptual framework for the generation and management of machine-readable playbooks, which are necessary for orchestrating a standardized response across the common EU space.

In the domain of incident handling, playbooks serve as an essential component, managing a series of phases including decision-making, reporting, collaboration, and incident response. The complexity of these phases demands a robust integration of multiple components, each offering complementary functionalities that are essential for effective cybersecurity response procedures. These functionalities are categorized into several distinct groups:

- **Playbook Management:** This functionality involves the organization and maintenance of the playbooks, ensuring they are up-to-date and accessible.
- **Selection of Playbooks:** This functionality allows users to choose appropriate playbooks from a repository, tailored to specific incident types.
- **Playbook Execution:** It involves the operational aspect of playbooks, where the steps and procedures are followed to address incidents.
- **Security Information and Event Management Integration and Analysis:** It allows for the correlation and analysis of security events for the development of incident response strategies.
- **Sharing Platform Integration and Cyber Threat Intelligence Exchange:** This is essential for the exchange of CTI across different platforms, enhancing incident handling via collective efforts.
- **Collaboration and work coordination facilities:** The toolset should facilitate collaboration and coordination among different teams and actors involved in incident handling.
- **Reporting Facilities:** This allows for the generation of comprehensive reports detailing the incident, its handling process, and outcomes for CERTs.

5.4.1 Conceptual requirements on the incident handling flow

Our use case involves interfacing with external systems, such as SIEM and CTI sharing platforms. The principal entities engaging with this system are Security Operations Centers

(SOCs), Computer Emergency Response Teams (CERTs)/Computer Incident Response Teams (CIRTs), national CERTs, and other organizations that stand to benefit from a shared playbook repository.

The conceptual requirements have been formulated through intensive discussion sessions and collaboration with relevant stakeholders and experts from SOCs and CERTs. These discussions were further enriched by the collaboration with four European national CERTs that are in alignment with the project's pilot initiatives. Additionally, extensive discussions with security professionals have yielded invaluable insights, aiding in the identification of a comprehensive set of requirements and the refinement of the conceptual framework.

We will now proceed to introduce the conceptual requirements of the system, which have been carefully crafted through the synthesis of expert opinion and practical engagement with the cybersecurity landscape. The requirements are specified in Table 24.

Table 24 – Conceptual requirements on playbook utilization and playbook-assisted incident handling in cybersecurity.

| ID | Conceptual requirement | Description |
|------|---|--|
| CR.1 | Adherence to technological standards | Support standard modeling notations, execution languages, and automation formats (e.g., BPMN, CACAO, JSON). |
| CR.2 | Adherence to legislative frameworks | Legislative frameworks and requirements are strictly followed (e.g., NIS2). |
| CR.3 | Reusability | Parts of playbooks, legislative rules, reporting rules, code snippets, and standard modeling constructs are easily and efficiently reused. |
| CR.4 | Readability | The playbooks should be machine-readable for automation reasons and human-readable to help users follow the process. |
| CR.5 | Coverage of multiple abstraction levels | Playbooks are presented on different abstraction levels, from descriptive to technical. |
| CR.6 | Multipurpose suitability | Playbooks on different abstraction levels are suitable for heterogeneous purposes and staff (administrative staff, technical staff, legislative bodies, etc.). |
| CR.7 | Adaptability/modifiability | Playbooks can be easily and efficiently modified, adapted, enhanced, and tailor-suited by different stakeholders, enabling this over their entire life cycle. |
| CR.8 | Consistency | The framework and the design and development process guarantee that playbooks |

| | | |
|-------|---|---|
| | | remain consistent after consecutive iterations of modifications. |
| CR.9 | Design and development life-cycle | A multi-stage life cycle is established and coherently followed from conceptual to executable playbooks, with suitable mappings between various model levels and incorporating human interaction. |
| CR.10 | Functional integrability | Developed playbooks can directly facilitate IR and investigation tasks. |
| CR.11 | System integrability | Developed playbooks allow for high connectivity with external systems and platforms. |
| CR.12 | Shareability | Playbooks, definitions, and rules can be shared between different stakeholders/organizational levels. |
| CR.13 | Collaboration ability and empowerment | The framework encourages vertical and horizontal collaboration between stakeholders and organizational levels, in particular between SOCs and CERTs. |
| CR.14 | Reporting ability | Standardize reporting methods to enhance Cyber Threat Intelligence (CTI) exchange and legislative compliance. |
| CR.15 | Standardisation of the playbook management flow | Provide a means to standardize incident handling on various levels, e.g., sectors, infrastructures, SOCs, and stakeholders. |
| CR.16 | Confidentiality | Provide means to restrict access to playbooks, or confidential data contained within. |

5.4.2 Conceptual framework for the incident handling flow

We introduce a conceptual framework consisting of the flow and relations between the incident handling components. The incident handling flow includes the journey from log correlation in SIEM systems to a series of steps facilitated by playbooks within the SOC. This track is combined with response actions by CERT/CIRT, facilitating incident reporting to national CERTs and sharing knowledge with other organizations. The process includes feedback from SOC, CERT/CIRT, and national CERTs to improve the response procedure for upcoming incidents.

Figure 37 illustrates the structured framework that outlines this flow. A conceptual framework shows the progression of incident handling, tracing the path from log correlation within SIEM systems to a series of steps facilitated by playbooks within the SOC. This track is integrated with response measures launched by CERT/CIRT, facilitating incident reporting to national CERTs and the dissemination of insights with affiliated organizations.

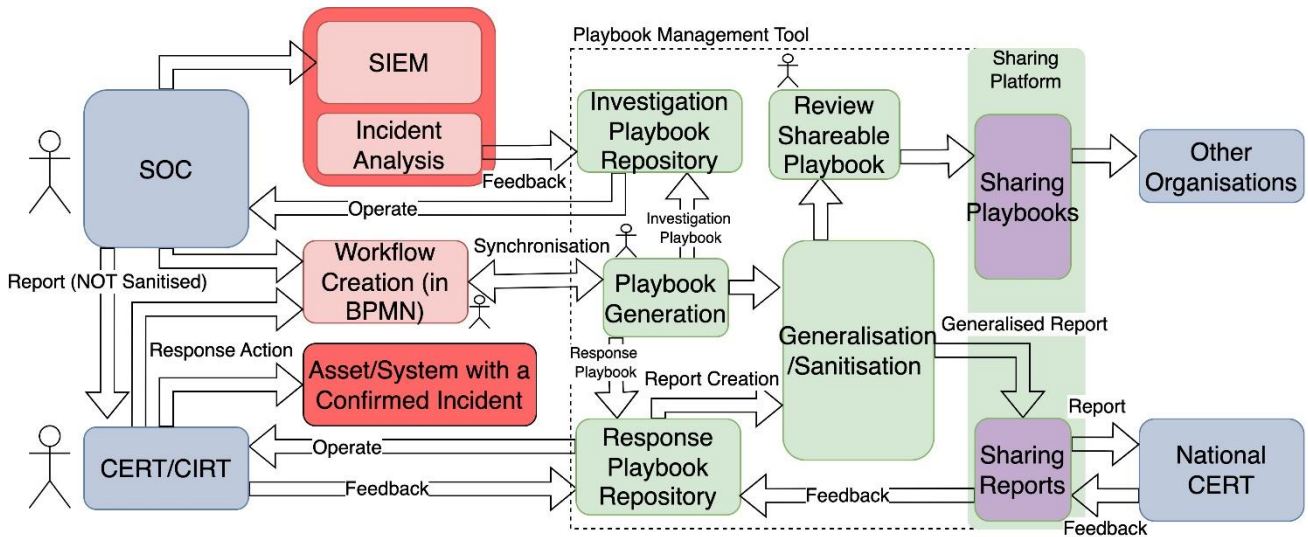


Figure 37 – Conceptual framework for the incident handling flow.

Within this framework, a Continuous Integration/Continuous Delivery (CI/CD) process initiates with log correlation in Security Information and Event Management (SIEM) systems, leading to a series of steps activated by an alarm in a Security Operations Center (SOC). This sequence commences with the definition of use cases and progresses to SOC analysis through investigative playbooks, ending with response measures executed by CERTs/CIRTs. An efficient SOC should possess a comprehensive set of rules and guidelines to address various scenarios while minimizing false alerts. Such complexity often drives companies to opt for outsourcing their SOC functions. CI/CD requires direct input from analysts to refine generic incident use cases into more precise iterations. Therefore, supplying them with modifiable investigative playbooks and records of their application is necessary to improve feedback for security engineers, who can then optimize the security use cases.

Upon verification of a SOC alarm as a security incident, the processed investigative playbooks and identified Indicators of Compromise (IoCs) can be disseminated to the response team to enrich response strategies. Here, the transition from human-readable formats to machine-readable playbooks presents a challenge. Initially, it involves translating information from existing documentation into a structured flowchart and then aligning it with machine-readable standards through a playbook management tool. Subsequently, additional elements such as metadata or detailed instructions and automation capabilities are integrated into the playbook. These playbooks are utilized by SOC and CERT personnel for incident detection and response, taking action on confirmed assets and systems. Therefore, continuous revision and improvement of the playbooks based on operational feedback are required. Moreover, reports to national CERTs can be generated automatically and in a standardized manner to simplify communication and gather feedback from authorities.

Since playbooks are tailored to specific organizations and may contain sensitive information, a generalization and sanitization process before community sharing is necessary. After ensuring privacy and confidentiality protection, the revised playbooks can be shared with other organizations to enhance their response capabilities or to foster collaborative incident response and automation.

The evolution of the cybersecurity landscape requires the adoption of standardized, machine-readable playbooks to enhance an organization's defenses against cyber threats. This move towards machine-readable playbooks constitutes a vital development in the domain of cybersecurity incident response, enhancing automation and ensuring conformity with EU directives such as NIS2. Conforming to NIS2, the proposed conceptual framework along with its proof-of-concept implementation, which adheres to the CACAO standard, offers an accessible platform for managing incidents with playbook support and enables integration with platforms like TheHive and Cortex. Nevertheless, employing a systematic Business Process Management (BPM) life cycle is essential to thoroughly document incident response activities and meet a range of requirements.

The framework components and processes address a variety of identified conceptual requirements. CR.1 (Adherence to Technological Standards), CR.3 (Reusability), and CR.4 (Readability) are fulfilled by the playbook management component, which accommodates standard modeling notation and playbook formats, and provides both machine-readable (e.g., CACAO) and human-readable representations of playbooks. Additionally, CR.16 (Confidentiality) is met by employing the Traffic Light Protocol and processes for generalization/sanitization before sharing. CR.7 (Adaptability/modifiability) is supported by the playbook management tool's capabilities for straightforward modifications and versioning. CR.9 (Design and development life-cycle) is maintained through robust version control and feedback mechanisms.

CR.2 (Adherence to Legislative Frameworks) and CR.14 (Reporting ability) are addressed by the report creation flow, which ensures compliance with legislative mandates through sharing with the National CERT. CR.5 (Coverage of multiple abstraction levels) is covered by the components that enable workflow and playbook creation, ranging from high-level BPMN to executable tasks. CR.6 (Multipurpose suitability) is guaranteed by the framework's flows, the playbook management tool, and various playbook repositories that span from investigation to response. CR.8 (Consistency) is upheld by synchronizing playbook generation processes.

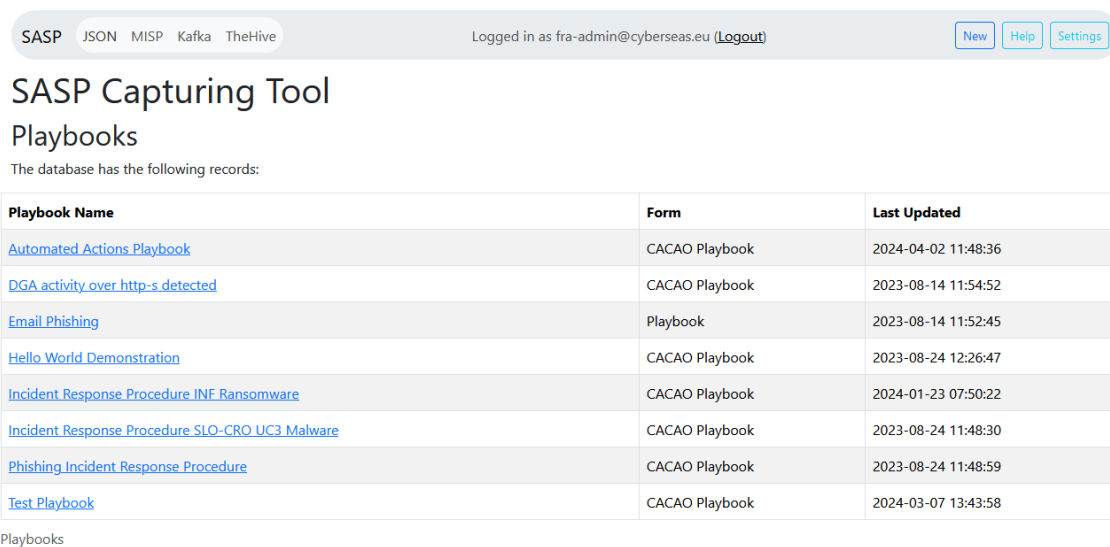
CR.10 (Functional integrability) is supported by integrations with SOC and CERT/CIRT operations, including SIEM connections. CR.11 (System integrability) is achieved by utilizing sharing platforms. CR.12 (Shareability) and CR.13 (Collaboration ability and empowerment) are advanced through sharing platforms and the framework's conceptual components, fostering collaboration between SOCs and CERTs. Lastly, CR.15 (Standardisation of the playbook management flow) is met by adopting standard processes and widely recognized tools across the framework.

To enhance cyber incident reporting and CTI exchange with CERTs, a structured approach to playbook development is essential. The initial step (Step 0) involves identifying attack scenarios that require reporting and exchanging CTI with CERTs. Subsequently (Step 1), general playbooks tailored for these scenarios are prepared, encompassing all critical phases: Preparation, Detection & Analysis, Response & Recovery, and Report & Post-incident, all while ensuring compliance with national CERT requirements. The next phase (Step 2)

entails the modeling of playbook steps into BPMN diagrams, with tools such as draw.io (<https://www.drawio.com/>). In the project, examples are provided from the SLO&CRO, EST, and FIN pilots. Moving forward (Step 3), a first draft of the playbooks is created using the SAPPAN tool, in compliance with the CACAO format, and practitioners are encouraged to familiarize themselves with the CACAO specification as the utilization of standards is emphasized by directives and regulations. At this stage, several examples (Malware, Ransomware, etc.) based on SLO&CRO models in CACAO format are offered as references. An intermediate step (Step 4) involves analyzing playbooks for similar attack types to consolidate them into a unified playbook; this step can also take place before Step 3 or even Step 2. The process ends (Step 5) with the completion of the final playbook version in the CACAO format.

5.4.3 Overview of contributed SAPPAN playbooks from pilots

All playbooks are available in the SAPPAN tool as shown in Figure 38. SAPPAN playbooks are stored in the backend of Semantic MediaWiki. They can also be accessed via the MSP platform when they are shared.



The screenshot shows the SAPPAN tool interface. At the top, there are navigation tabs for SASP, JSON, MISP, Kafka, and TheHive. The user is logged in as fra-admin@cyberseas.eu. There are buttons for New, Help, and Settings. The main heading is "SASP Capturing Tool" with a sub-heading "Playbooks". Below this, it says "The database has the following records:". A table lists the playbooks with columns for Playbook Name, Form, and Last Updated.

| Playbook Name | Form | Last Updated |
|---|----------------|---------------------|
| Automated Actions Playbook | CACAO Playbook | 2024-04-02 11:48:36 |
| DGA activity over http-s detected | CACAO Playbook | 2023-08-14 11:54:52 |
| Email Phishing | Playbook | 2023-08-14 11:52:45 |
| Hello World Demonstration | CACAO Playbook | 2023-08-24 12:26:47 |
| Incident Response Procedure INF Ransomware | CACAO Playbook | 2024-01-23 07:50:22 |
| Incident Response Procedure SLO-CRO UC3 Malware | CACAO Playbook | 2023-08-24 11:48:30 |
| Phishing Incident Response Procedure | CACAO Playbook | 2023-08-24 11:48:59 |
| Test Playbook | CACAO Playbook | 2024-03-07 13:43:58 |

Figure 38 – Common playbook repository in the SAPPAN playbook management tool.

This way, SAPPAN is used as a common repository of standard playbooks. Playbooks from the repository can be adopted, modeled, shared, and executed by all EPES stakeholders in the common EU space. D6.8 therefore provides the initial set of standardized playbooks for the uniform European EPES ecosystem. These playbooks are the result of the efforts of CyberSEAS beneficiaries, which means that SAPPAN playbooks were contributed by SLO&CRO, EST, and FIN pilots. Most of the standardized playbooks provided by D6.8 were defined by INF and PET, which are involved in the SLO&CRO pilot. They are presented in Section 4 of this document. Three examples addressing malware, ransomware, and phishing are offered as references in the CACAO format.

In addition, the EST and FIN pilots contributed standardized playbooks for the EPES system. Figure 39 shows the metering service data breach playbook of the FIN pilot and Figure 40 the substation defense playbook of the EST pilot.

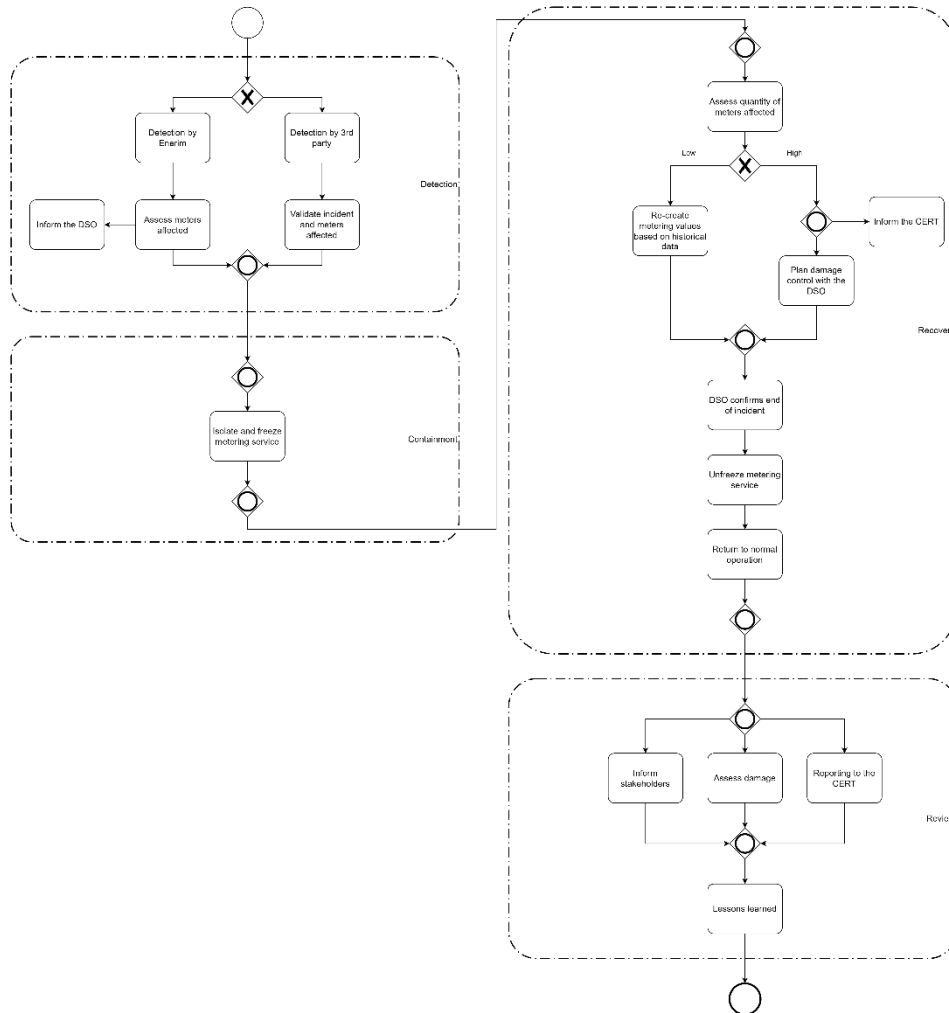


Figure 39 – Metering service data breach playbook.

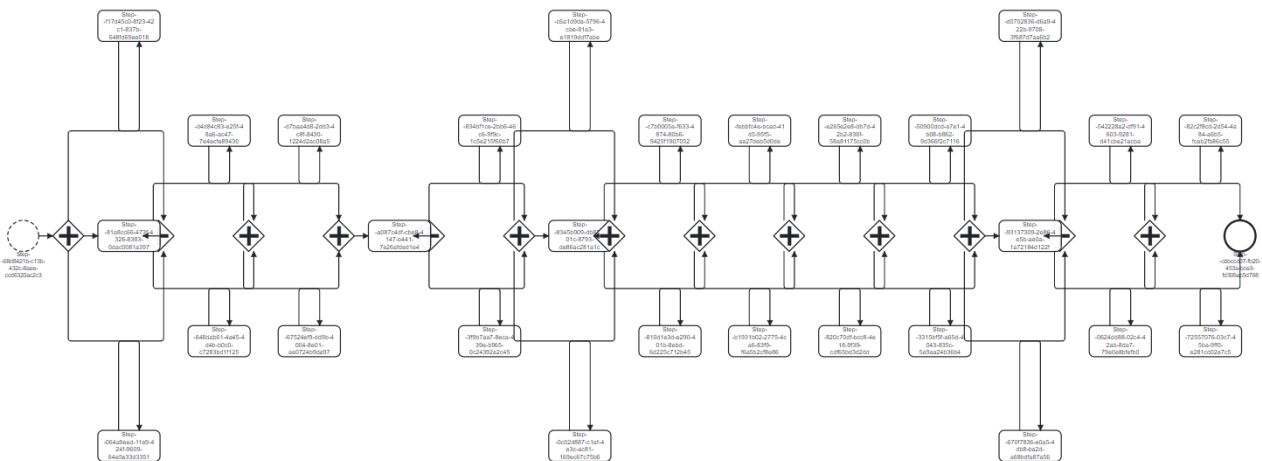


Figure 40 – Substation defense playbook.

All standardized playbooks, which are modeled as a result of D6.8, are listed in Table 25. These playbooks are shared in the common SAPPAN repository. As an integral part of incident response procedures, they cover the coordination with CERTs and rules for reporting in case of incidents. These rules are utilized through playbook activities. They determine when, how, and under which conditions incidents are notified to CERTs. This is aligned with NIS 2, CER, and NCC. The rules also consider the specifics of national legislation and authorities (CERTs). All playbooks can exchange the NOKI object representing the reporting data format.

Table 25 – List of shared standardized incident response playbooks.

| Contributor | Incident response playbook |
|-------------|---|
| INF | Malware |
| INF | Ransomware |
| INF | Phishing |
| OPR | Disgruntled employee |
| PET | Information system damage, abuse, infection, or intrusion |
| PET | Information system operation prevention |
| PET | Violations of legislation |
| PET | Disregard of security policies |
| PET | Data loss, destruction, or abuse |
| HOPS | Data poisoning of weather station data |
| ENERIM | Metering service data breach |
| ELV | Substation defense |

6 Toolset design and implementation

This section presents the design and implementation of a toolset for incident response, the coordination of EPES operators, and reporting to CERTs. We provide a prototype solution and several design artifacts.

6.1 Specification of functional and non-functional requirements

Figure 41 presents the general use case. It is complex and covers a sequence of phases that constitute the process of decision-making, reporting, collaboration, and incident response. We can observe that several modules of the toolset are integrated and that complementary groups of functionalities must be supported. We will describe the modules in Section 6.2 and specify functional and non-functional requirements below.

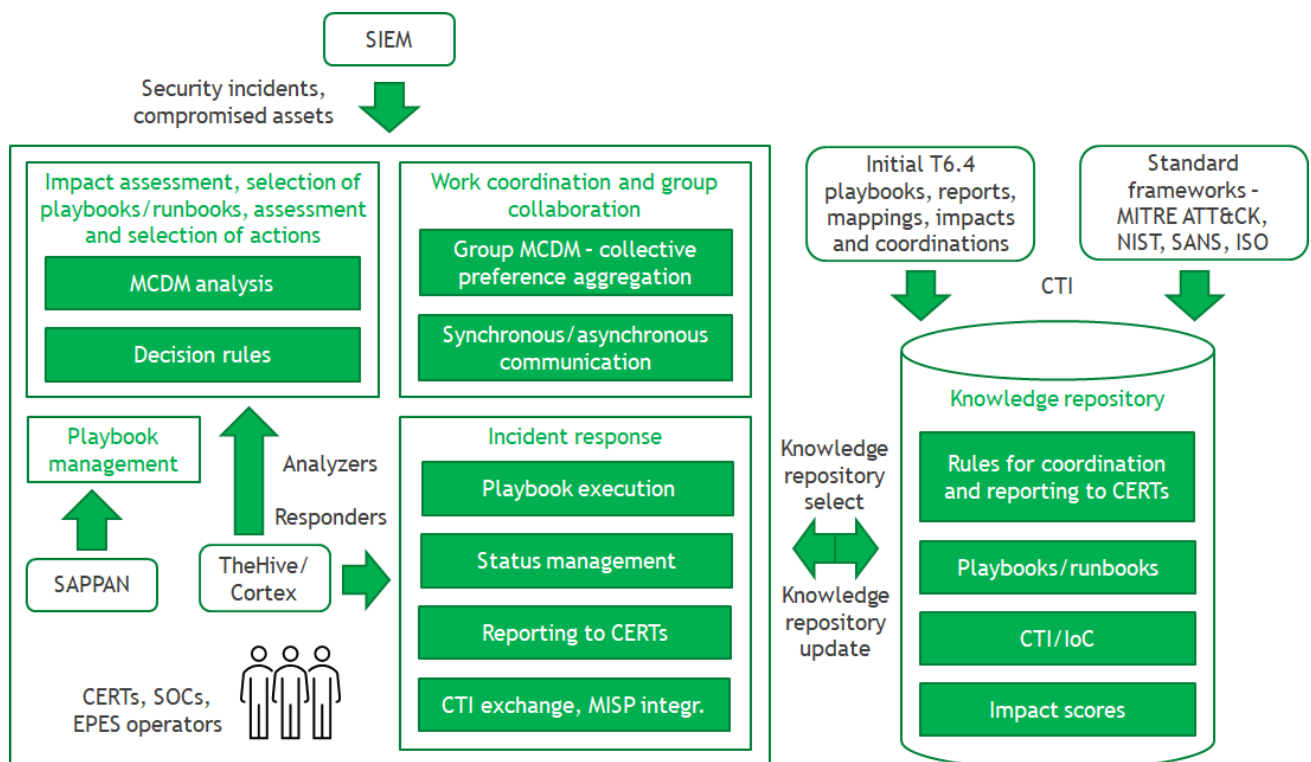


Figure 41 – General use case.

We divide the functionalities into eight groups:

- playbook management (Table 26),
- playbook selection from the SAPPAN repository (Table 27),
- playbook execution (Table 28),
- SIEM integration and analysis (Table 29),
- MISP integration and CTI exchange (Table 30),
- reporting facilities (Table 31, partially overlapping with playbook execution and MISP integration),

- incident impact assessment (Table 32), and
- collaboration and work coordination facilities (Table 33 and Table 34).

The use case relies on integrations with external systems, such as SIEM, MISP, and standard vulnerability frameworks and databases. The key actors that participate in the use case are SOC, CERT, and the EPES operator. The latter comprises the roles of CISO, security analyst, and decision-maker. The use case is (partially) demonstrated with the prototype.

Below, the system's functional requirements are categorized into groups of different main functionalities for the cybersecurity response procedures. They are followed by Table 35, which specifies non-functional requirements.

Table 26 – Functional requirements on Playbook management (SAPPAN).

| ID | Functional requirement | Description |
|--------|--|--|
| FR.1.1 | Storing playbooks in the knowledge base | The playbook management tool should support the creation of new cybersecurity playbooks and their storage in the knowledge base. |
| FR.1.2 | Managing playbooks – add | The playbook management tool should support adding new cybersecurity playbooks based on the organization's needs. |
| FR.1.3 | Managing playbooks – modify | The playbook management tool should support modifying the existing playbooks and their resources. |
| FR.1.4 | Managing playbooks – delete | The playbook management tool should support removing an existing playbook or its resources. |
| FR.1.5 | Managing playbooks – exchange | The playbook management tool should support exchanging playbooks between different departments and/or operational levels. |
| FR.1.6 | Managing playbooks – export (JSON) | The playbook management tool should support export functionality to a widely used and standardized format. |
| FR.1.7 | Managing playbooks – import (JSON) | The playbook management tool should support import functionality via a widely used and standardized format. |
| FR.1.8 | Graph representation of the playbook (BPMN) | The playbook management tool should support graph representation of the playbooks to increase readability. |
| FR.1.9 | Translation of a playbook in different formats | The playbook management tool should support playbook translation to different standards and widely used formats. |

| | | |
|---------|--------------------------|--|
| FR.1.10 | Enable Sharing playbooks | The playbook management tool should support sharing playbooks between organizations and/or different departments considering confidentiality and privacy requirements. |
|---------|--------------------------|--|

Table 27 – Functional requirements on Playbook selection (from the SAPPAN repository).

| ID | Functional requirement | Description |
|--------|--|--|
| FR.2.1 | Support searching option | Support searching and navigation in playbooks in the SAPPAN knowledge-capturing tool with the consideration of user privileges. |
| FR.2.2 | Searching from available playbooks on MISP | Support searching for shared playbooks in MISP. |
| FR.2.3 | Receive incident scores from another tool | The tool should support receiving incident scores from other tools. |
| FR.2.4 | Support knowledge representation to aid playbook selection | Show the options and support knowledge representation to aid operators in selecting a proper playbook based on the values for selection metrics. |

Table 28 – Functional requirements on Playbook execution.

| ID | Functional requirement | Description |
|--------|--|---|
| FR.3.1 | Support monitoring of steps | Introduce resources to show the progress of the steps, the result or takeaways of a step, etc. |
| FR.3.2 | Exchanging info with automation/execution tools (Cortex/TheHive) | Connect to the execution engines and run an executable task. |
| FR.3.3 | Receiving execution results from automation/execution tools (Cortex/TheHive) | Receive the result of the executed task and proceed further in the workflow based on the output of the executed/automated task. |

Table 29 – Functional requirements on SIEM integration and analysis.

| ID | Functional requirement | Description |
|--------|--|---|
| FR.4.1 | Receiving detection info triggered by incident detection | The tool should support connection to the SIEM system for triggering by incident detection. |
| FR.4.2 | On-boarding of the needed log files received by different log collectors | Log files from the affected systems should be provided to the SIEM. |

| | | |
|--------|---|--|
| FR.4.3 | Dashboard definitions | The tool should allow to define what information is important to be shown on the dashboard and what correlations are needed. |
| FR.4.4 | Alarm definitions with the corresponding case template and Correlation/Alarm search | What needs to be detected? Which event(s)? The tool should be able to detect two or more correlated events, e.g., event (a) followed by event (b), amount (x) of events (y) in time (z), etc. |
| FR.4.5 | Connection to the EPES Stakeholder for the real-time severity calculation | The tool should allow to have a matching to the asset and its stored information (e.g., IP + Name + Description or unique ID) |

Table 30 – Functional requirements on MISP integration and CTI exchange.

| ID | Functional requirement | Description |
|--------|--|---|
| FR.5.1 | Receiving detection info triggered by incident detection | The capturing tool should support connection to a CTI sharing tool to receive incident detection information. |
| FR.5.2 | Cortex Analyzer/Responder | The capturing tool should support connection to the analyzer/responder tool (Cortex). |
| FR.5.3 | Standard Cortex Analyzers and Responders per Level | |

Table 31 – Functional requirements on Reporting facilities.

| ID | Functional requirement | Description |
|--------|---|--|
| FR.6.1 | Search and preview of reporting rules | Reporting rules (based on national legislation) are retrieved from the knowledge repository and presented to the user. |
| FR.6.2 | Definition and update of reporting rules | The user may add new reporting rules or modify existing reporting rules. |
| FR.6.3 | Search and preview of reporting structures and formats | Reporting data structures and formats (based on national legislation) are retrieved from the knowledge repository and presented to the user. |
| FR.6.4 | Definition and update of reporting structures and formats | The user may define new reporting data structures and formats or modify existing ones. |
| FR.6.5 | Mapping of reporting rules to playbook actions | The user maps defined reporting rules into specific reporting actions in incident response playbooks. |

| | | |
|--------|--|--|
| FR.6.6 | Mapping of reporting structures and formats to playbook actions | The user maps defined reporting data structures and formats to specific reporting actions in incident response playbooks. |
| FR.6.7 | Generate a report from IR data based on the established rules, structures, and formats | The user (manually) or system (automatically) generates a report according to the report definition from the real case incident response data. |
| FR.6.8 | Report submission to CERTs (MISP integration) | A MISP API operation is invoked to submit the report to CERT. |
| FR.6.9 | Reporting feedback from CERTs (MISP integration) | A MISP API response is obtained from CERT and synchronously/asynchronously presented to the user. |

Table 32 – Functional requirements on Incident impact assessment.

| ID | Functional requirement | Description |
|--------|--|--|
| FR.7.1 | SIEM information visualization | SIEM information on recent cybersecurity-related events is presented in a structured way to be used for the incident impact assessment. |
| FR.7.2 | Identification of alternatives – incidents | Identification of cybersecurity-related incidents is facilitated based on SIEM information. These incidents are regarded as decision-making alternatives to be assessed by the MCDM model. |
| FR.7.3 | Identification of compromised assets | Identification of compromised assets and their dependencies is facilitated based on SIEM information and the asset repository. A set of compromised assets determines the severity of exploited attacks. |
| FR.7.4 | Restructuring of criteria | A standard set of decision-making criteria is provided to assess the impact of detected incidents, including the functional and informational impact criteria. These criteria can be restructured, additional criteria can be added. |
| FR.7.5 | Criteria weighting | Standard weights of incident impact assessment criteria are initially provided. Decision-makers (security analysts, CISOs, etc.) can modify these weights according to national or infrastructural requirements. |

| | | |
|---------|--|---|
| FR.7.6 | Presentation of the impact assessment matrix | The impact assessment matrix is provided to the decision-maker based on the identified incidents (alternatives) and the set of criteria. |
| FR.7.7 | (Pre)calculation of impact scores | For several impact assessment criteria, scores are (pre)calculated (e.g., based on the SIEM calculated severity/magnitudes, or CVSS scores of compromised assets) and provided to the decision-maker. Iterative recalculation is possible over time as more detailed SIEM information becomes available. |
| FR.7.8 | Specification of impact scores (impact assessment) | The decision-maker inputs impact scores or modifies precalculated impact scores for all criteria. The format/scale of impact scores is predefined (qualitative scale, [0 ... 10] numerical scale, etc.). |
| FR.7.9 | Aggregation of impact scores | Criteria-wise impact scores are aggregated. Total scores are presented to the decision-maker. |
| FR.7.10 | Mapping to the national impact levels | The mapping of the generic calculated impact scores to nationally prescribed impact levels is performed and presented. E.g., in Slovenia national levels are C1 (critical incident) to C6 (security event, not a relevant incident). These impact levels trigger different rules/playbooks for the coordination with CERTs. |
| FR.7.11 | Sensitivity analysis on impact scores | Several sensitivity analysis techniques are provided, such as robust weighting intervals (maximal deviations of criteria weights that do not result in a change of impact levels). |
| FR.7.12 | Storage of MCDM model and impact scores | The MCDM model (including criteria and criteria weights) and calculated impact scores are stored in the knowledge repository for future reference and decision-making. |
| FR.7.13 | Export and exchange of impact scores | Calculated impact scores are exported in a standard format (e.g., JSON) to be imported by the playbook management system (SAPPAN) and used for playbook selection. |

Table 33 – Functional requirements on Collaboration and work coordination facilities (for decision-making).

| ID | Functional requirement | Description |
|----|------------------------|-------------|
|----|------------------------|-------------|

| | | |
|--------|---|--|
| FR.8.1 | Initiation of the collaboration and group decision-making process | One of the cooperating EPES stakeholders initiates the group collaboration/decision-making process. This stakeholder invites other stakeholders. |
| FR.8.2 | Joining the collaboration and group decision-making process | The invited EPES stakeholder accepts the invitation and joins the group collaboration/decision-making process aimed at the collective assessment of incident impacts. |
| FR.8.3 | Calculation of group statistics on incident impacts | Delphi statistics on individually assessed incident impacts (assessments provided by different EPES stakeholders) are calculated. Statistical data include at least: min, max, mean/median. Aggregated group total impact scores may also be calculated. |
| FR.8.4 | Visualization of group statistics on incident impacts | Group statistics on incident impacts are presented to all EPES stakeholders (decision-makers). Delphi indicators are visualized graphically or presented in a table. |
| FR.8.5 | Adjustment and submission of individual assessments | Based on group statistics, each EPES stakeholder can adjust individual impact scores in its MCDM impact assessment matrix. The stakeholder then submits adjusted impact scores for the next group coordination iteration. |
| FR.8.6 | Acceptance of group impact assessment | The EPES stakeholder that takes part in the group coordination process may accept the current collective incident impact scores based on Delphi indicators. When all EPES stakeholders confirm their acceptance, the group coordination/decision-making process is closed. |
| FR.8.7 | Group criteria structuring | Based on individual sets and structures of criteria, the collective set and structure of common impact assessment criteria may be formulated. Visualization and graphical management of the common criteria set are provided. |
| FR.8.8 | Group chat – reading and searching messages | Group coordination and collaboration are supported by means of the group chat facility. All messages are presented to the stakeholder/participant. Search functionality is also available. |
| FR.8.9 | Group chat – writing and submitting messages | Group coordination and collaboration are supported by means of the group chat facility. |

| | | |
|---------|--|--|
| | | The participant/stakeholder can write and submit a message. |
| FR.8.10 | Visualization of stakeholders' compromised assets and incidents | A visualization/presentation facility is provided that allows each stakeholder to have an overview of all compromised assets and incidents that are identified by other stakeholders. This enables stakeholders to collectively discuss impacts, reporting rules and incident response procedures. |
| FR.8.11 | Blocking of assets and incidents for presentation | The stakeholder can block some of its assets and/or identified incidents to be shared with other stakeholders/participants in case information on these assets and/or incidents is considered confidential. |
| FR.8.12 | Presentation of incident response procedures | Incident response procedures from the repository (SAPPAN) are presented to collaborative stakeholders to facilitate the discussion about selecting the collectively appropriate procedure(s)/playbook(s) |
| FR.8.13 | Collective selection of appropriate incident response procedures | Each stakeholder can indicate which playbooks are appropriate to be executed for reporting and coordinating with CERTs. The collective selection is indicated. The stakeholder can accept or reject the collective selection. |

Table 34 – Functional requirements on Collaboration and work coordination facilities (for incident handling).

| ID | Functional requirement | Description |
|--------|-----------------------------------|--|
| FR.9.1 | Baseline definition | Define averages of the system/network load, e.g., CPU utilization or running processes. |
| FR.9.2 | Dashboard definition | Define the most important values and how they can be aggregated to provide useful information. |
| FR.9.3 | Alerting definition | Define anomalies and alarm rules. |
| FR.9.4 | Agent installation to the systems | The tool should allow to actively send information. |
| FR.9.5 | Defining/selecting SNMP trees | The tool should allow for the gathering of network and system information via a simple network protocol. |

Table 35 – Non-functional requirements.

| ID | Non-functional requirement | Description |
|---------|---|---|
| NFR.1.1 | Standardized machine-readable vocabulary | The playbooks should be machine-readable for automation reasons. |
| NFR.1.2 | Human-readability of playbooks | The playbooks should be human-readable to help them to follow the process. |
| NFR.1.3 | Privacy/confidentiality issues of playbooks and their steps | Playbooks contain sensitive information that should not be shared publicly. Also, personal information should be removed from playbooks before sharing them between different departments or organizations. |
| NFR.1.4 | Usability of the playbooks | Increasing the level of abstraction of the playbooks may lower the response effectiveness and hamper workflow automation usage. It is challenging to enable consumers of the playbook to map abstract identifiers onto their organization-specific identifiers. |
| NFR.1.5 | DNS Server Root or intermediate CA Mailservers | The tool should provide support for infrastructure components. |

6.2 Components, modules, and tools

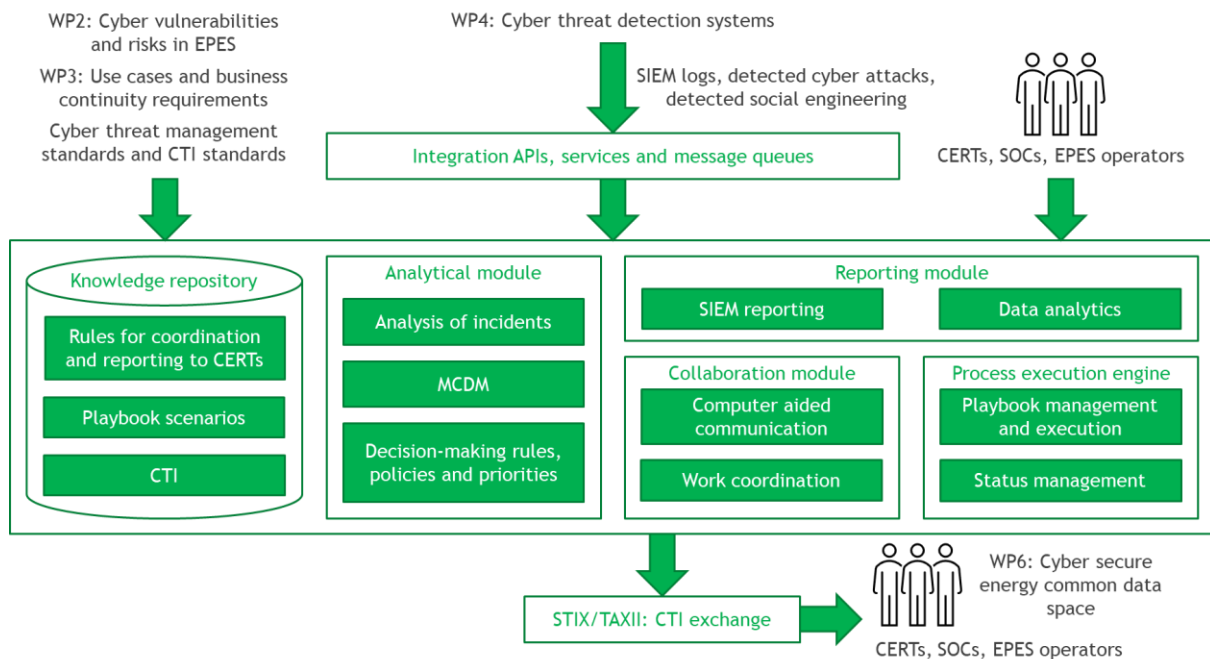


Figure 42 – Components and modules of the toolset.

Figure 42 gives a high-level overview of components and modules. We describe them in this section. They are aligned with the general use case from Section 6.1. They are also partly reused with the decision support system (DSS) we are developing in the T4.4 task. The overlap can be seen in Figure 43. In particular, the knowledge repository, analytical/MCDM module, and collaboration module are shared. We will present the analytical component of the DSS solution in Section 6.6.

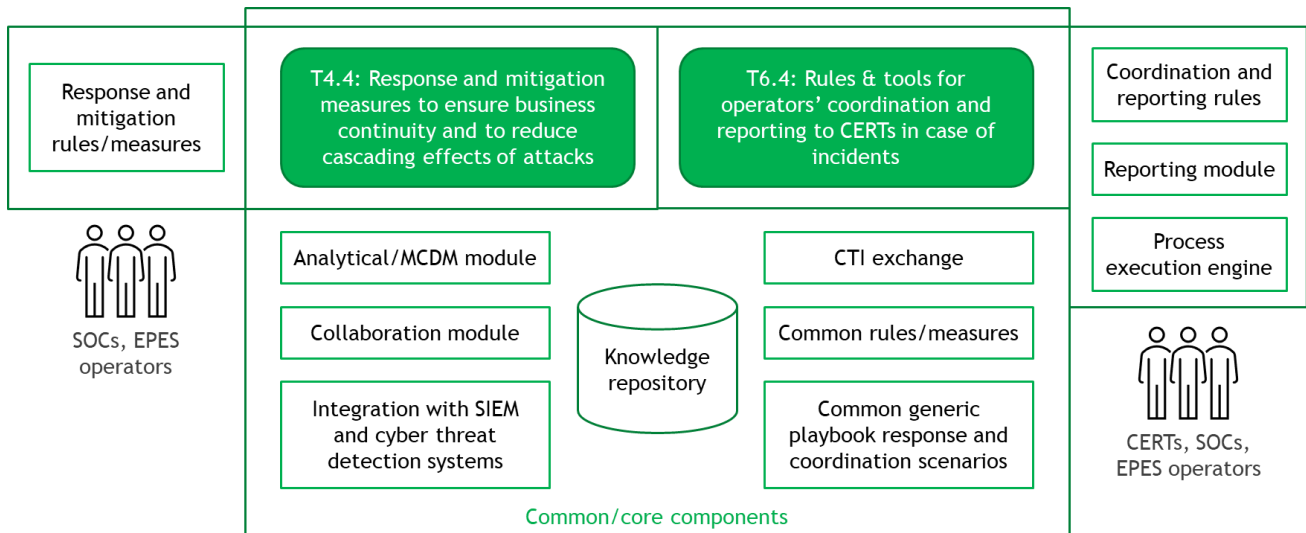


Figure 43 – T4.4 and T6.4 toolset integration.

6.2.1 Analytical module

The role of the analytical module is two-fold. On one side, it provides multi-criteria decision-making (MCDM) capabilities. On the other, it has to facilitate the analysis of cyber incidents and the integration with SIEM and other external cyber threat detection systems.

SIEM uses the collected log files from various systems, such as the firewall and EDR (Endpoint Detection and Response), to aggregate different events. In case of a triggered alarm rule, the information is pushed to TheHive. In case the alarm has no log source (e.g., a log file provided by the AV-System or IDS-System could contain a severity of that specific event), the use case owner can specify the severity of a specific event (high, medium, or low), a TLP (Traffic Light Protocol) rating to classify the sensitivity of the processed information), or a PAP (Permissible Actions Protocol) rating [78] to indicate how the received information can be used.

The MCDM component of the analytical module implements the MCDM models defined in Section 3.4. It covers the incident impact assessment process. It implements value functions, the scoring system, preference aggregation operators, and supporting mechanisms, such as the estimation of scores based on LIRI or according to historical statistical data. The analytical module must be flexible enough to support criteria structuring and weighting. It also has to implement sensitivity and robustness analysis techniques, which include “what-if” analysis, stability intervals and regions, and multi-dimensional robustness analysis. Moreover, the analytical module must provide the implementation of several MCDM methods that give the

decision-maker the ability to use the most subjectively convenient approach to decision analysis. These methods include the additive value model and the qualitative model based on the DEXi method.

Based on the above functionalities, the DSS will provide a numerical or qualitative value of the impact an asset might have and an overall CVSS score. This information can be obtained from the risk matrix provided by the EPES stakeholders. The correlation between the alarm rule or event in SIEM and DSS can be established by the IP (if unique) of the asset or a unique ID, such as CPE (Common Platform Enumeration).

This information will help the analyst to decide the relevance of a new alarm. In the case of many alarms, it can also be used for triage. The first-level analyst will be provided with all known CVEs of an asset and will decide upon the information provided by the SIEM if one of these CVEs could be associated with the provided information. He will also eliminate all non-matching CVEs.

6.2.2 Reporting and collaboration module

There are several aspects to this module. Primarily, it implements the collaborative and group decision-making functionalities described in Section 2.5. It has to cover two types of group cooperation. Firstly, the group decision-making facility implements the Delphi process or the selected group consensus-seeking preference aggregation mechanism to provide different EPES stakeholders with a means to come to the collective assessments of incident impacts. This facility is tightly aligned with MCDM methods implemented by the analytical module because it takes the individual numerical or qualitative preferences of cooperating decision-makers and computes appropriate group measures.

Secondly, this module implements the mechanisms for computer-mediated communication (CMC). These mechanisms are two-fold. They are integrated with the Delphi asynchronous communication procedure and can provide independent communication channels, such as web conferencing and chatting.

On the other hand, MISP (Malware Information Sharing Platform) can also provide the tools to achieve the collaboration among stakeholders. This tool has already proven its value in other projects like SeCollA [79], where a collaborative SOC for manufacturing was demonstrated. Threat intelligence can be shared with other SOCs or trusted parties.

Connecting the MISP instances of multiple SOCs enables threat sharing and therefore the collaborative approach of the whole setup. This can be done using the MISP web interface of the instances that shall be connected. When the configuration is done correctly, an analyst can choose to share information concerning a possible threat using MISP. The counterpart will see the shared information that was received via their MISP instance as an alert, which allows another analyst to investigate the alert and import it as a case if desired.

Information sharing can be done by using the "Communities" on MISP. Such communities can be of different natures:

- CIRCL (Computer Incident and Response Center Luxembourg): a community with more than 1100 member organizations.
- Trusted groups: communities working in a partially connected mode.

- Financial sector group includes banks, payment processing organizations, and others.
- Military and international organizations.
- Security vendors.
- Topical communities (e.g., Covid-19 MISP).

According to the technical documentation, “MISP has several organization “pools”, one for local and one for known external organizations”. The analyst is also able to add external organizations to such a pool and then connect the organization to the pool by means of an authentication key.

To exchange indicators with other instances, MISP uses its “Core” format. It includes an overall structure along with semantics associated with each respective key and is JSON-based.

6.2.3 Process execution engine

The Cortex is the processing unit that interacts with the Hive, the SIEM, and the MISP. It contains analyzers for information enrichment during the incident analysis phase and responders used during the response phase.

Analyzers and responders are called via REST API. Cortex comes with a predefined set of analyzers and responders, but new ones can be added easily. As mentioned, analyzers [80] are used to enrich an alarm or a case with information gathered from the external Threat Intelligence, such as abuse providers, MISP, Staxx, etc., or to perform external analysis on artifacts like files or hashes (e.g., ClamAV checks or starts an external malware analysis in a Cuckoo sandbox). They can also be used to interact with the SIEM, e.g., if the analyst needs to perform an additional SIEM correlation search. Responders [81], on the other hand, are used to perform action on an artifact or IoC. Response actions can be adding a new proxy or firewall rule.

6.2.4 Playbook management system

In today's complex and dynamic threat landscape, developing cybersecurity playbooks and storing and managing them in a knowledge repository is crucial for efficient incident response and management.

This project reuses the SAPPAN capturing tool as the playbook management system. The SAPPAN playbook management tool is based on Semantic MediaWiki (SMW). It features semantic web technologies on a MediaWiki knowledge base, which contains a MediaWiki-based web interface, an API, and RDF/SPARQL backends for advanced data queries. The core component is containerized for easy deployment.

The SAPPAN tool contains a more appealing Python-based web interface for capturing playbooks and their steps without the necessity of dealing with the wiki interface. The GUI can be connected to wiki instances running remotely or locally, allowing for creating new playbooks, editing existing ones, and converting playbook files.

The tool includes a playbook sanitizer component that automates the process of public or shareable playbook extraction from a confidential response and recovery workflow, where the playbook format supports this (e.g. SAPPAN). It removes or masks confidential information

from the playbook and creates a shareable version for the public or specific organizations, departments, or security operational level.

Moreover, the tool includes a playbook converter component designed to import SAPPAN/CACAO formatted playbooks directly onto the playbook management system and export playbooks from the wiki to SAPPAN vocabulary or CACAO format. Also, the playbook subscriber component allows searching and importing SAPPAN and CACAO playbooks from the MISP platform, as well as sharing them via MISP.

Additionally, the playbook steps are modeled and stored in a structured way in the playbook management system and represented in the BPMN diagrams, which can be interactively navigated.

The architectural view of the tool adopted from the paper [82] is shown in Figure 44.

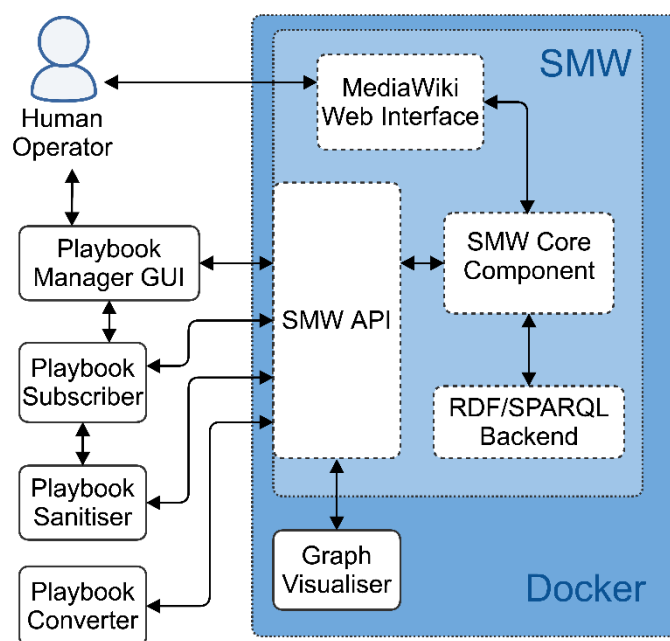


Figure 44 – Architectural view of the playbook management system.

6.2.5 Integration components

Integration components are defined in Section 6.4 about the architecture. API specifications are also provided.

6.3 Data structures

Within the scope of follow-up work, we will present a detailed definition of data structures. It will include datatypes of events (SIEM), data structures of reports, the taxonomy for CTI exchange (MISP/TheHive), data structures of MCDM models for impact assessment, and other data structures. Of particular importance are data structures for the integration of systems and tools, e.g., based on JSON.

6.3.1 Data structures for the integration of SAPPAN and Cortex Analyzers/Responders

As part of the integration effort, we plan to create an extension of the CACAO standard that defines a cortex-command data type, which should include all necessary information directly in the playbook to run a CortexAnalyzer/Responder. Because different organizations often have very different requirements for executing response actions, we expect this will provide a much more "out-of-the-box" solution by relying on the Cortex for execution, which is already a widely disseminated security tool.

Further, we envision a custom CortexAnalyzer/Responder that is capable of communicating with the SAPPAN tool via API, fetching playbooks that use cortex commands and automatically executing them. This would allow organizations to define more complex responses to security incidents (e.g., more intensive analysis of malware once hash comparisons indicate maliciousness). Further, it would enable organizations to dynamically change their responses across different incident types simply by editing the playbook in the SAPPAN tool.

6.4 Architecture

The architecture is presented in Figure 45 with a flowchart, which describes the information flow in a top-down manner. The following subsections define individual steps, phases, and components.

6.4.1 Pre-processing with SIEM and dashboards

In the beginning, the SIEM provides the correlated events, which have triggered a specific alert. To do the correlation of specific events, the log files of the systems or components that could indicate specific incidents need to be onboarded to the SIEM. These logs can be provided for example directly from the endpoints or the firewall. A log collector then forwards all the information to the SIEM where it is processed.

After the data normalization, correlation, and enrichment, an alarm query triggers an alert. The specific detection rule thereby is provided by the Use Case Factory (UCF). Figure 46 shows the specification of detection and correlation rules.

The second input is used to monitor the infrastructure. It provides information about the utilization and workload of monitored servers or network components. In addition, the dashboards give the analysts an overview of what is happening in the system.

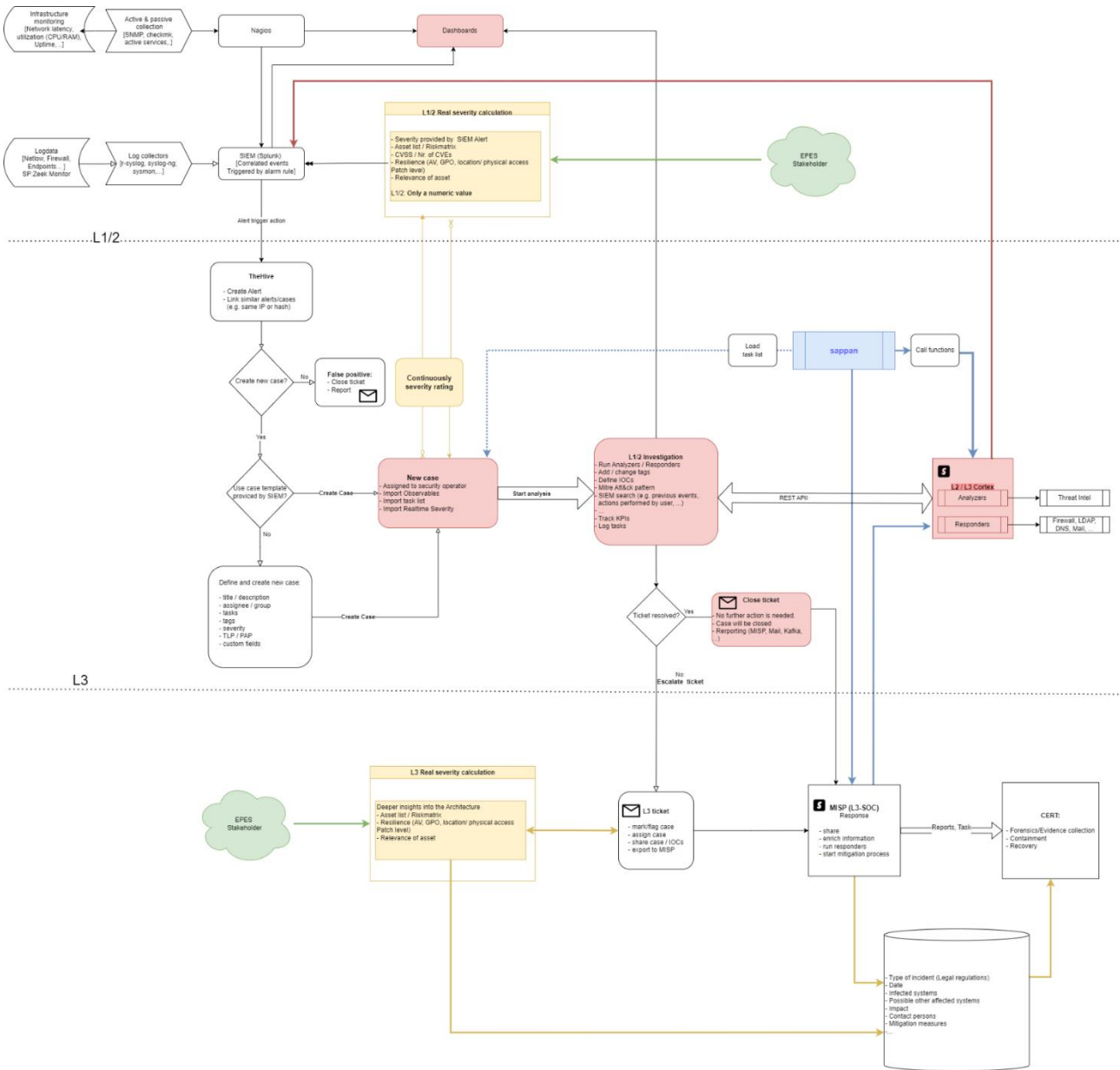


Figure 45 – Flowchart of the system.

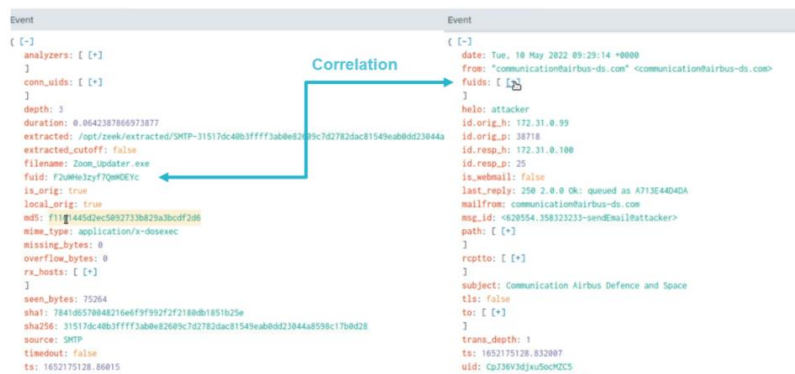


Figure 46 – Definition of event correlations.

6.4.2 SIEM alerting

The SIEM Alert triggers an action to export the correlated events with all data tables to the ticketing system (TheHive). Therefore, the Datatype (field name in the SIEM) needs to be mapped to the corresponding data type in TheHive so that they can be interpreted properly.

The case template which is provided to each alarm can bind to a new case when the alarm is imported by the L1 Analyst. TheHive attaches the predefined set of tasks (either investigation or response runbooks) to be performed when this specific event occurs. The task list that is defined in TheHive should be provided by the UCF. If there is no case template available for an alarm or the analyst decides to create a case without the suggested template, he/she might define a blank task list as well as suitable tags, additional custom fields, and a description. This is also done during the threat-hunting phase on L2 when the analyst is collecting traces from the SIEM.

TheHive matches similar events to each alert and case if the same value of a specific artifact is already a part of a previous alert or case and links it to a new alert/case. The analyst can also attach the new alarm to an existing case.

An example in TheHive can be seen in Figure 47. It showcases artifacts with their data types and IoCs.

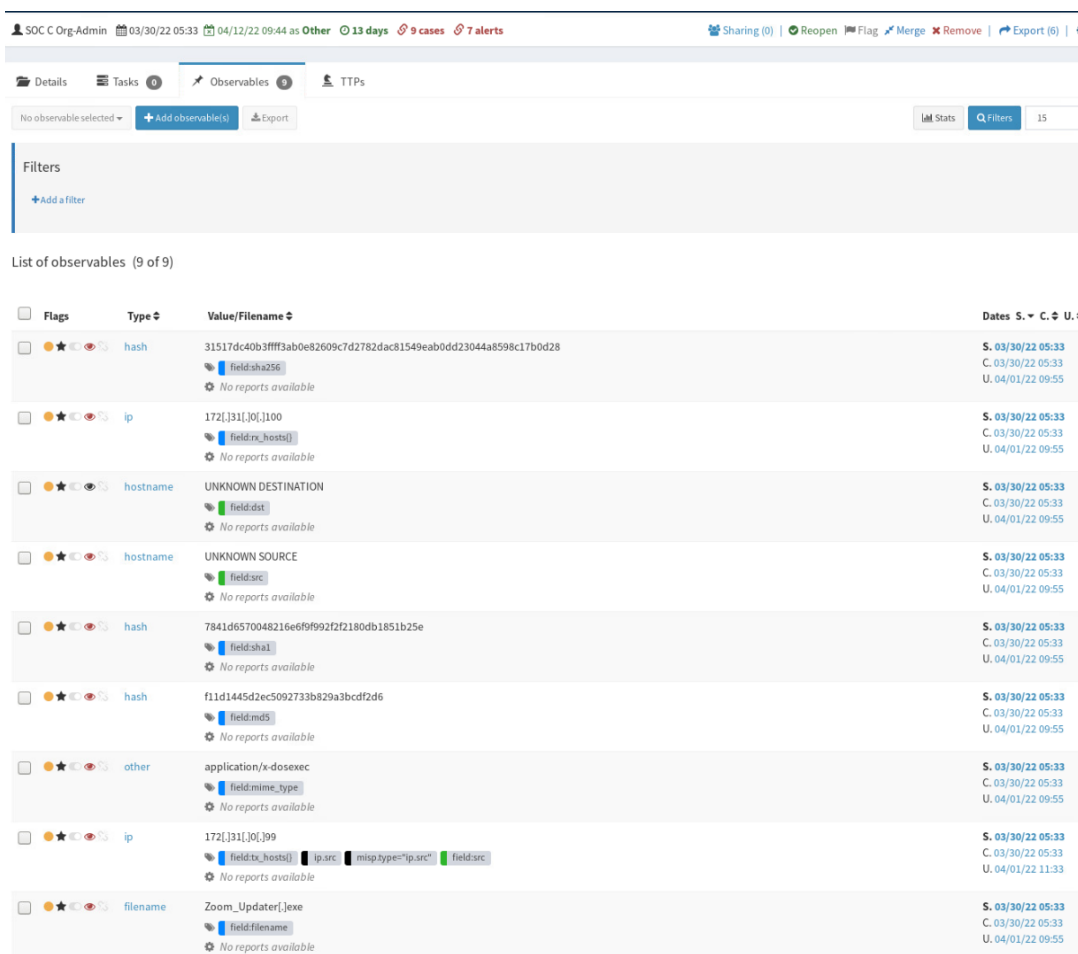


Figure 47 – Artifacts, data types, and IoCs in TheHive.

6.4.3 Possible integration of SAPPAN to perform analysis for auto-enrichment of the case

In a future release, it might be possible to provide the tasks list to TheHive, which is based on a SAPPAN playbook. The task list contains a list of tasks the L1 Analyst must perform to a specific alert and is currently defined in the UCF.

It might also be possible to run an automated analysis based on a SAPPAN playbook. In this case, the SAPPAN playbook management system would be capable of calling different cortex analyzers automatically. It would then call one or more analyzers in a row, based on the result of the current/previous analyzer and the defined decision tree of the playbook.

This could be used to automate the tasks of level 1 and 2 Analysts and would lead to a solution for a security orchestration, automation, and response (SOAR) system.

6.4.4 Continuous severity calculation

The new case has the predefined Severity (Low, Medium, or High), TLP (Traffic Light Protocol), and PAP (Permissible Actions Protocol) rating defined in the alarm rule. This rating is altered up on the continuous severity Rating.

The new rating is calculated with information like CVSS, the number of known vulnerabilities, the resilience level as well as the relevance of the affected asset(s). The resilience level might be the sum of different protection measures already applied to the specific asset and can contain:

- installed AV products,
- applied group policies,
- patch level,
- location or physical access to the asset,
- and others.

The new rating decides which playbooks are performed by SAPPAN. This value is also used in the case of triage. For example, when three events, each with a rating of 3, 4, and 8 occur at the same time, the event with the severity rating 8 will be handled first.

6.4.5 Investigation and response

Each case contains several artifacts, mapped to their data fields from the alarm rule / the correlated event provided by the SIEM. The observables can be of any type of data. This is demonstrated in Figure 48.

On each observable, either an analyzer or responder (Cortex) can be executed to enrich the case with additional information (e.g., Threat Intel). Observables can be tagged as an indicator of compromise (IoC).

Cases and alarms may contain (either provided by SIEM events or as a response of a Cortex analyzer) a MITRE technique (e.g., T1056). As shown in Figure 49, the analyst is provided with all the information related to that technique. It gives him/her insights into what an attacker could have performed. Up on this provided information, he/she then starts the investigation.

This might be checking previous events from a specific host or user, the executed commands, or involved IP addresses or domain names.

Artifacts

| # | Datatype | Value |
|----|----------|--|
| 1 | url | hxxps://attack[.]mitre[.]org/techniques/T1012 |
| 2 | url | hxxps://attack[.]mitre[.]org/techniques/T1056 |
| 3 | url | hxxps://attack[.]mitre[.]org/techniques/T1056/004 |
| 4 | url | hxxps://attack[.]mitre[.]org/techniques/T1027 |
| 5 | url | hxxps://attack[.]mitre[.]org/techniques/T1027/002 |
| 6 | fqdn | v[.]beahh[.]com |
| 7 | hash | b4c6fff030479aa3b12625be67bf4914 |
| 8 | domain | Zoom_Updater[.]exe |
| 9 | domain | Trojan[.]Metasploit |
| 10 | hash | 31517dc40b3ffff3ab0e82609c7d2782dac81549eab0dd23044a8598c17b0d28 |
| 11 | hash | 7841d6570048216e6f9f992f2f2180db1851b25e |
| 12 | hash | f11d1445d2ec5092733b829a3bcdcf2d6 |

Figure 48 – List of artifacts and their corresponding datatypes.

Figure 49 – MITRE ATT&CK taxonomy provided to an alarm or a case (based on an IoC or a SIEM event).

6.4.5.1 L1 Analyst

L1 Analyst represents the first line of defense. He/she has the following responsibilities:

- Security monitoring of the dashboards (resource utilization like CPU load or network availability)

- Executes the generic playbooks imported from SAPPAN into the task list of the ticketing system
- Tracks performed tasks in a log and acknowledges each task from the task list
- Often closes known alerts as false positives and enriches the case with information gathered by external resources / Cortex analyzers

If L1 cannot find a solution or does not close the ticket as a false positive, the case will be shared with L2.

6.4.5.2 L2 Analyst

The L2 Analyst has a higher experience than the L1 Analyst. He/she performs security analysis and runs more sophisticated Analyzers (e.g. Cuckoo malware analysis), which might also be more costly than standard analyzers.

He/she is able to perform Threat Hunting (e.g., a zero-day attack or a new serious vulnerability discovered in the architecture) based on CTI information or charged by the customer or asset owner. During a threat hunt, the L2 Analyst collects traces from the SIEM (which did not trigger an alert because no rule has yet been implemented) and searches for patterns that might indicate that new vulnerability that might have been exploited. The L2 Analyst reports the incident to the customer, department, or asset owner (as far as agreed) when the case is solved or an incident confirmed. If L2 cannot find a solution nor can confirm an event as a real incident, he/she will escalate the incident to L3 by exporting the case with its artifacts and IoCs to the MISP.

6.4.5.3 L3 Analyst

In general, L3 is responsible for the incident response handling and reporting to the CERT. The L3 Analyst has the most experience, knowledge, and possibly the right to perform a response/mitigation measure by calling Cortex responders. He/she also has insights into the monitored infrastructure, which is a part of the information provided by the EPES stakeholders (e.g., the corresponding assets, their purpose, and functions). The L3 Analyst can perform mitigation measures via Cortex responders, like adding firewall rules and isolating hosts or networks, or is at least collaborating with the responsible IT department.

The L3 analyst should also be responsible for the tuning or modification of the SIEM alerting rules as he/she is also part of (or reports to) the Use Case Factory (UCF).

6.4.5.4 Handling false positives and rule tuning

In case an alarm rule is badly configured, or anything has been changed in the preprocessing (e.g., someone changed the log level), it could let the rule excessively trigger alarms. That could flood the ticketing system even with triaged events and the analyst could easily oversee a real incident. In such a case, the alarm rule needs to be modified as quickly as possible.

On a regular basis (e.g., monthly), false positives should also be analyzed as this is part of the CI/CD process of the UCF. In that context, also the provided real-time severity needs to be considered and possibly modified.

6.4.6 Authentication

Internally, TheHive uses signed session cookies and CSRF tokens [83]. Cortex supports local, LDAP, Active Directory (AD), X.509 SSO, API keys for authentication, and OAuth2.

API keys can only be used to interact with the Cortex API (for example when TheHive is interfaced with a Cortex instance, it must use an API key to authenticate to it). API keys cannot be used to authenticate to the Web UI. By default, Cortex relies on local credentials stored in Elasticsearch.

Therefore, a sync-user needs to be created for each organization or TheHive instance. The API key (bearer token) must be known to TheHive. This makes it important to use SSL/TLS encrypted connections if Cortex and TheHive are hosted on different machines.

6.4.7 MISP integration

Auth keys are used to authenticate MISP API requests. Auth keys can be set to read-only. A single user can have multiple auth keys. When a new sync user for TheHive or Cortex instance is created, it must be provided to the application.conf. Each communication partner can additionally be verified via X.509 certificates (stored in the Truststore).

Artifacts or complete cases can be shared with connected communities or connected CERTs. The following figures present basic sharing mechanisms. Figure 50 gives an example of MISP and TheHive integration. Figure 51 shows the propagation of sharing a specific IoC or artifact. Sharing with communities is presented in Figure 52.

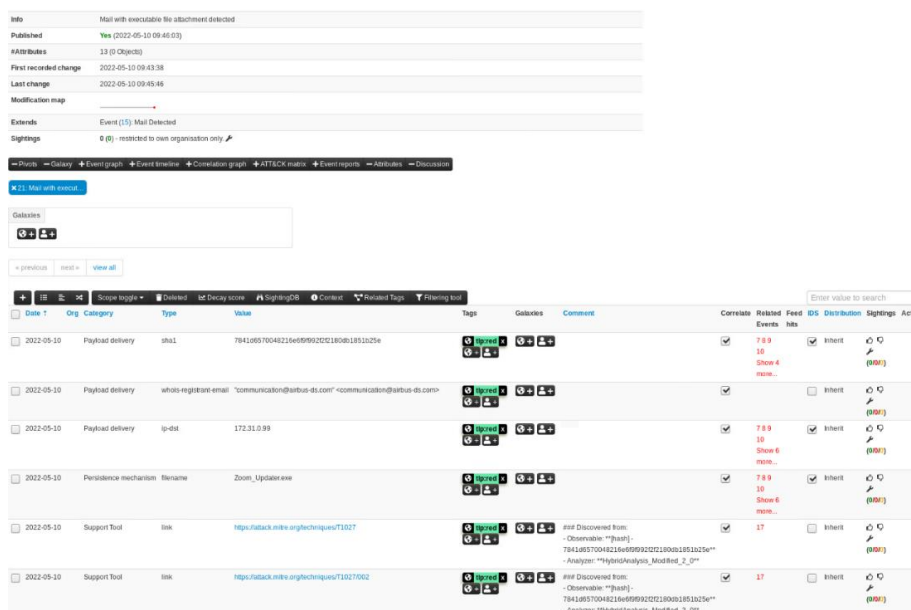


Figure 50 – Integration with MISP from TheHive.

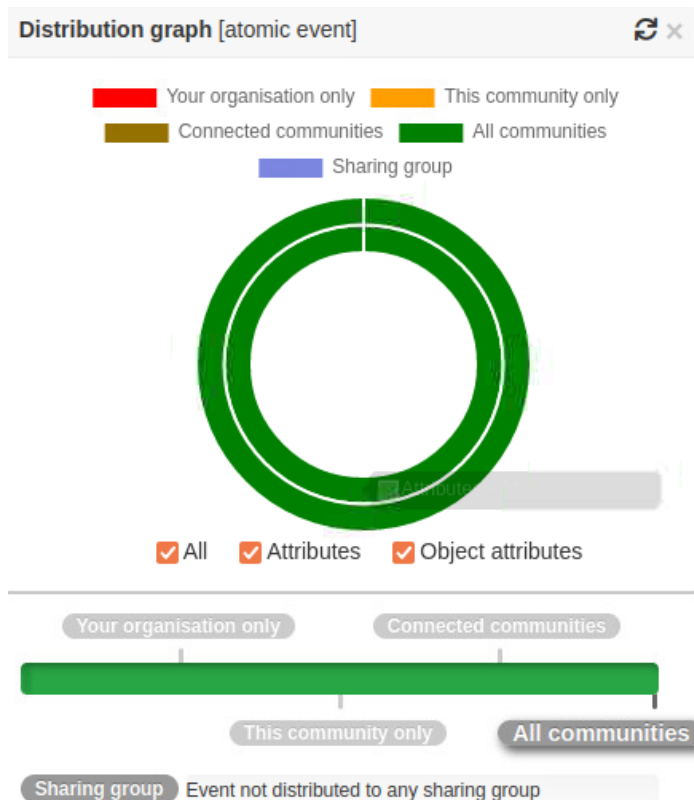


Figure 51 – Propagation of sharing a specific artifact or IoC.

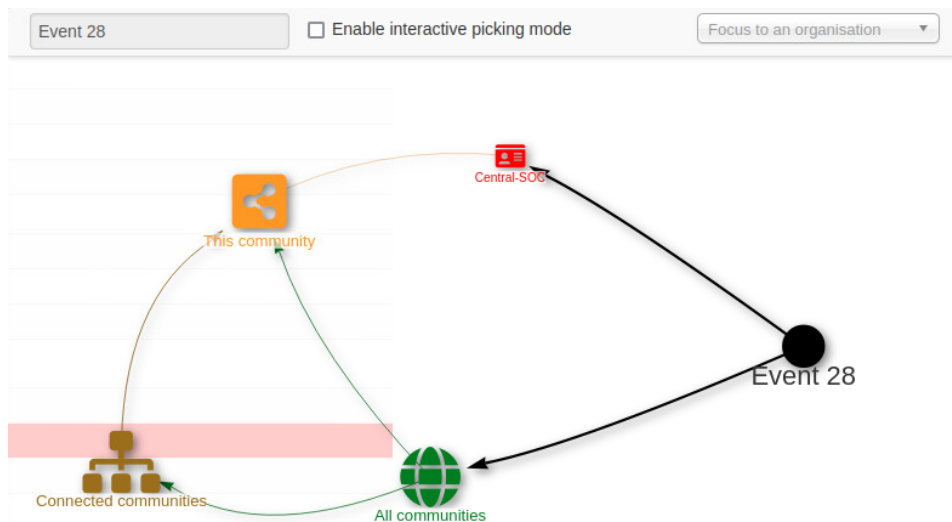


Figure 52 – Sharing of a MISP case or event with connected companies or communities.

Users can be authenticated via a PGP key. Users (and their authentication keys) are used to serve as the points of connection between instances. Events pushed to an instance are pushed to a sync user, who then creates the events on the remote instance. Events pulled are added by the sync user that is used to connect the remote instance to your instance [84]. MISP authentication is shown in Figure 53.

D6.8 Rules & Tools for Operators' Coordination and Reporting to CERTs in Case of Incidents V2

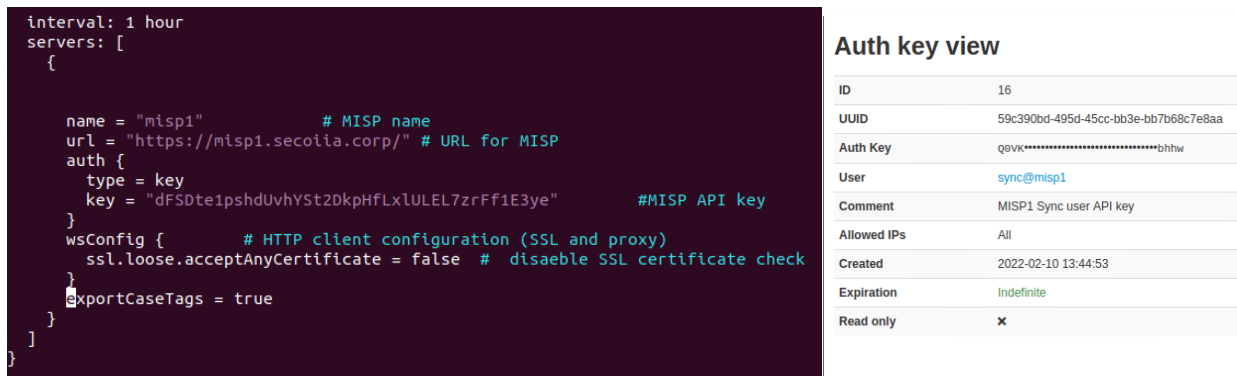


Figure 53 – MISP authentication.

It is possible to connect two MISP instances (e.g., local MISP to CERT). We create an additional sync user on either the local instance or the remote instance. The remote instance is added to the server. Therefore, the organization's UUID represented on the remote server must be known. This is depicted in Figure 54.



Figure 54 – Connection of two MISP instances.

Last, Figure 55 presents the connection to the Splunk SIEM. For the integration into Splunk, a new sync user must be created on TheHive and/or Cortex. The API key must be known to the application.

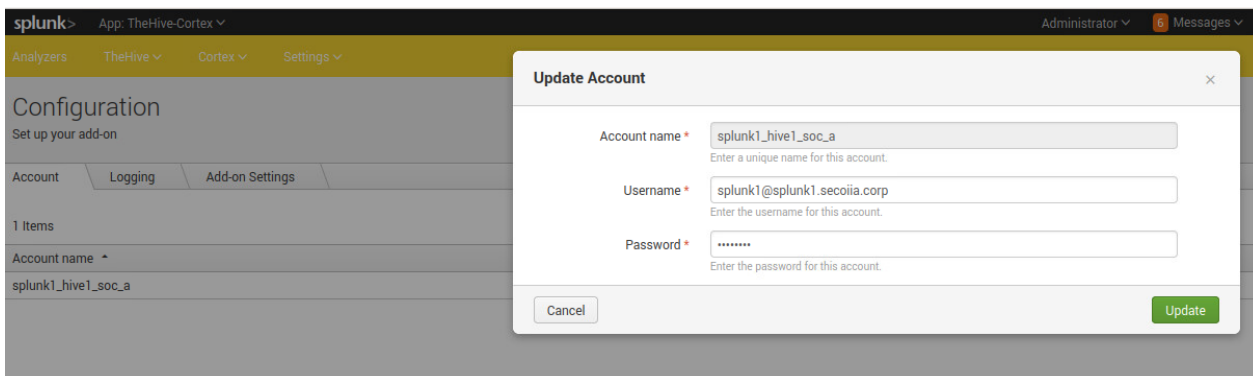


Figure 55 – Connection to SIEM.

6.4.8 Analyser and Responder integration/interaction

Responders can be executed either via the API connection from theHive, directly from the Cortex Web-UI, or from the SIEM. Each analyzer or responder needs at least one artifact type (e.g., hash, fqdn, ip, etc.) to interact with. Cortex 3 uses files. A job is stored in a folder with the following structure:

job_folder

_ input

| _ input.json <- input data, equivalent to stdin with Cortex 2.x

| |_ attachment <- optional extra file when analysis concerns a file

|_ output

_ output.json <- report of the analysis (generated by analyzer or responder)

|_ extra_file(s) <- optional extra files linked to report (generated by analyzer)

Figure 56 shows a Cortex job, Figure 57 a Cortex Responder, and Figure 58 a Cortex Analyzer report.

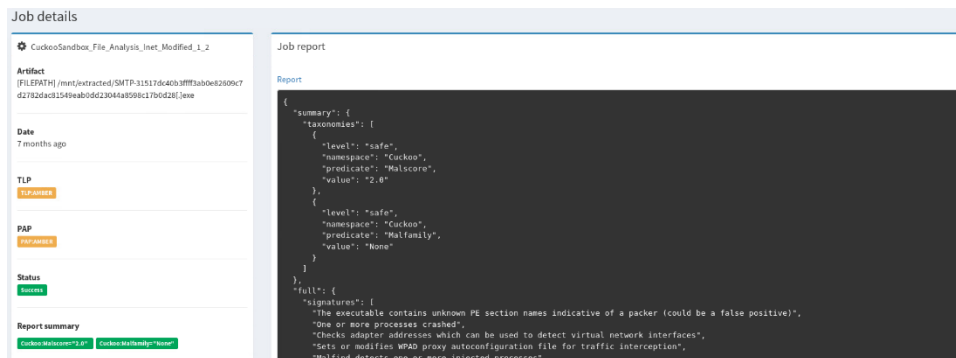


Figure 56 – Cortex job.

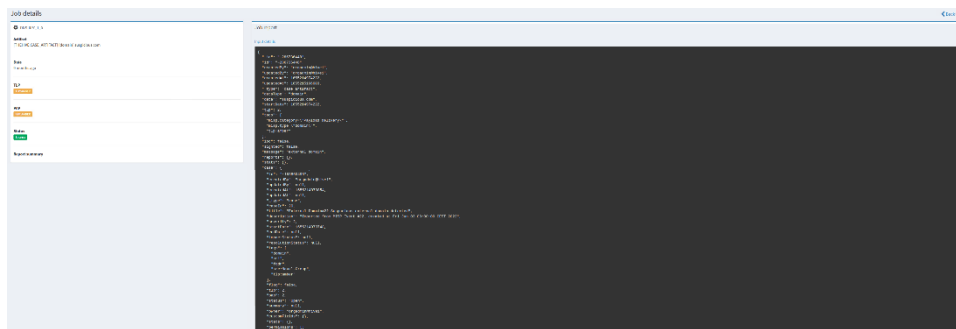


Figure 57 – Cortex Responder.

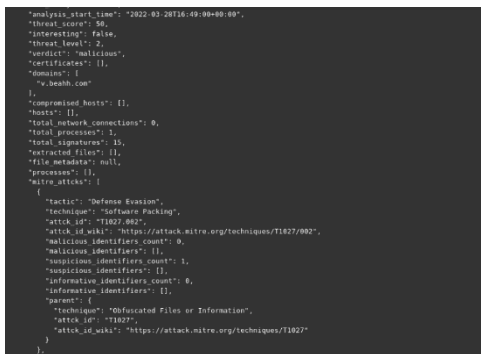


Figure 58 – Cortex Analyzer report.

TheHive and Cortex currently accept the following data types defined in the dataTypeList: domain, file, filename, fqdn, hash, ip, mail, mail_subject, other, regexp, uri_path, url, user-agent ... Their use is demonstrated in Figure 59.

```

{
  "name": "VirusTotal_GetReport",
  "version": "3.0",
  "author": "CERT-BDF",
  "url": "https://github.com/TheHive-Project/Cortex-Analyzers",
  "license": "AGPL-V3",
  "description": "Get the latest VirusTotal report for a file, hash, domain or an IP address.",
  "dataTypeList": ["file", "hash", "domain", "ip"],
  "command": "VirusTotal/virustotal.py", <== Program to run when invoking the analyzer
  "baseConfig": "VirusTotal", <== name of base config in Cortex analyzer config page
  "config": {
    "service": "get"
  },
  "configurationItems": [ <== list of configuration items the analyzer needs to operate (api key etc.)
    {
      "name": "key",
      "description": "API key for Virustotal",
      "type": "string", <== defines what kind of data type the configuration item is (string, number)
      "multi": false, <== setting multi to true allows to pass a list of items (e.g. MISP analyzer)
      "required": true
    },
    {
      "name": "polling_interval",
      "description": "Define time interval between two requests attempts for the report",
      "type": "number",
      "multi": false,
      "required": false,
      "defaultValue": 60
    }
  ]
}

```

If the analyzer **succeeds** (i.e. it runs without any error):

```

{
  "success": true,
  "artifacts": [..],
  "summary": {
    "taxonomies": [..]
  },
  "full": {..}
}

```

Figure 59 – Use of TheHive/Cortex data types.

6.5 Playbook management integration

For the playbook management system, the SAPPAN capturing tool is utilized. In SAPPAN, the domain vocabulary and knowledge were translated and modeled into SMW forms, templates, categories, and properties. Existing domain data could be imported from different sources using the converter component.

Users can create, modify, delete, convert, search, share, and view playbooks and their resources in the capturing tool. The Create action includes adding steps, properties, associated wiki pages, and other resource values connected to a playbook or its steps. While the modify and delete actions mean editing and removing the existing playbooks or their resources. The GUI allows the creation of playbooks via a form after a successful login to the system. The playbook author should connect steps via two properties, "Next step" and "Previous step", and define the confidentiality level of a playbook through Traffic Light Protocol (TLP).

A playbook includes several steps; each contains different details. In The GUI of the SAPPAN capturing tool, an operator can navigate through the steps and modify their detailed

information. Figure 60 presents an example of a step creation and its details. The playbooks can be viewed on the knowledge base, exported to JSON format, or shared via the MSP platform. The connection to the STIX platform is also considered, but it still has not been developed.

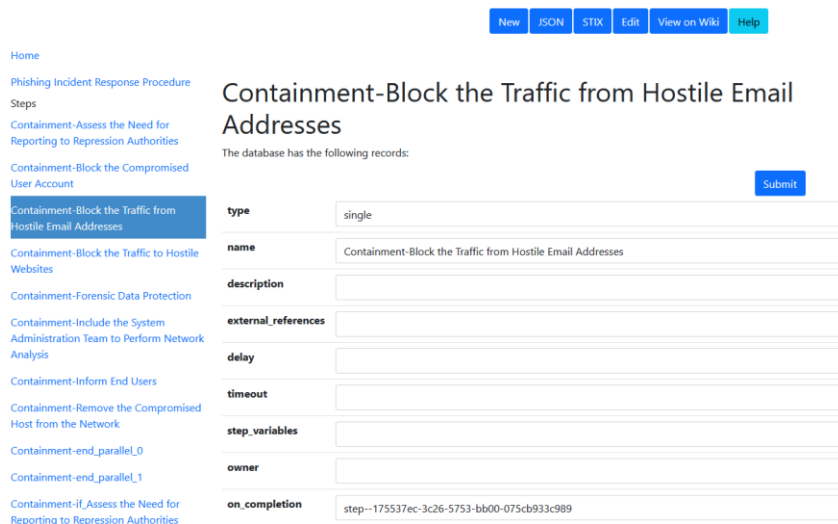


Figure 60 – Creating a playbook step in the SAPPAN capturing tool.

Moreover, Figure 61 depicts the view of the detailed created step, which uses the CACAO format. Dynamically created links and a list of pages referring to this step allow for easy navigation. If a mistake was noted or the playbook changed, the edit functionality immediately returns you to the editing page enabling quick modifications.

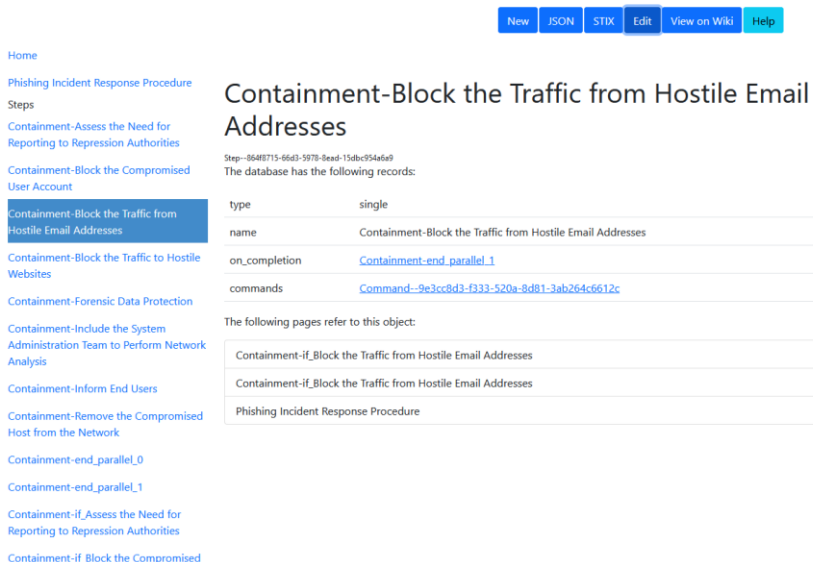
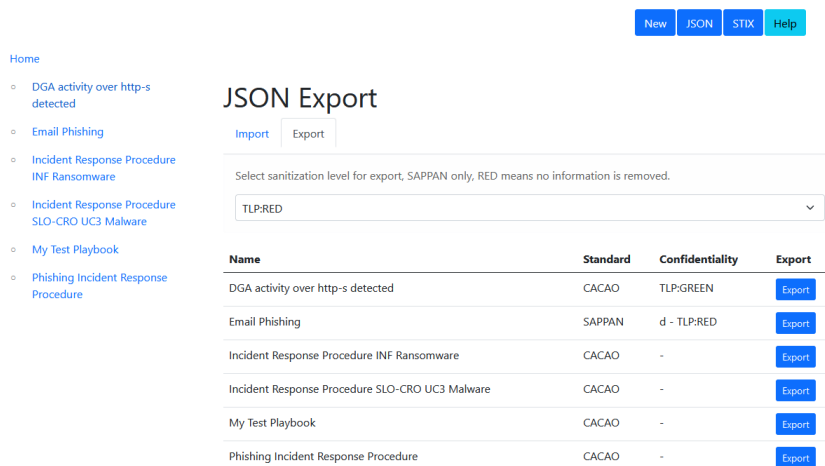


Figure 61 – Information/editing view of a created playbook step in the SAPPAN capturing tool.

The created playbooks can be exported as JSON files. On the export page, all the available playbooks are shown. The intended playbook can be selected, and the confidentiality level for the export can be determined. After that, the output would be sanitized based on the confidentiality level. Figure 62 shows the user interface for exporting playbooks.

Additionally, a converter from the CACAO specification to the Directed Acyclic Graph (DAG) format of Apache Airflow is developed as part of the efforts to create automation workflows. It allows quick sharing of automation tasks between teams, organizations, and applications [85].



Home

- DGA activity over http-s detected
- Email Phishing
- Incident Response Procedure INF Ransomware
- Incident Response Procedure SLO-CRO UC3 Malware
- My Test Playbook
- Phishing Incident Response Procedure

JSON Export

Import Export

Select sanitization level for export, SAPPAN only, RED means no information is removed.

TLP:RED

| Name | Standard | Confidentiality | Export |
|---|----------|-----------------|--------|
| DGA activity over http-s detected | CACAO | TLP:GREEN | Export |
| Email Phishing | SAPPAN | d - TLP:RED | Export |
| Incident Response Procedure INF Ransomware | CACAO | - | Export |
| Incident Response Procedure SLO-CRO UC3 Malware | CACAO | - | Export |
| My Test Playbook | CACAO | - | Export |
| Phishing Incident Response Procedure | CACAO | - | Export |

Figure 62 – Selecting and defining the confidentiality level of a playbook for exporting into JSON in the SAPPAN capturing tool.

Figure 63 and Figure 64 illustrate a simple example of machine-readable JSON export of a CACAO playbook and details of its steps, respectively.

```
{
  "type": "playbook",
  "spec_version": "1.1",
  "id": "playbook--8bf32013-452e-5555-8d42-12001e0ecd60",
  "name": "Phishing Incident Response Procedure",
  "playbook_types": [
    "remediation",
    "detection",
    "mitigation",
    "investigation"
  ],
  "created_by": "identity--0a7d4546-8846-5577-9c89-1240a0ea2c4e",
  "created": "2023-02-23T14:58:08Z",
  "modified": "2023-02-23T15:20:08Z",
  "workflow_start": "Step--9935d2ca-5f1a-5bc0-aa51-1c0758b9b5f1",
  "workflow": {...}
}
```

Figure 63 – High-level JSON export of a CACAO playbook in the SAPPAN capturing tool.

```
{
  "step--4a474164-0910-5160-a693-8540e6056198": {
    "type": "if-condition",
    "name": "Eradication and Recovery-if_Check that no more Anomalous Network Traffic can be Detected",
    "on_true": [
      "step--a97558b4-1d90-573e-9903-43f16efab3a9"
    ],
    "on_false": [
      "step--6dbf645a-cd7e-5105-b79b-25e942fe6d10"
    ]
  },
  "step--6aecc9c7-0754-58fc-8d21-a52e092d5da9": {
    "type": "single",
    "name": "Identification-User Reports Phishing and-or Extortion",
    "on_completion": "step--ab5e8873-f8cd-53c7-8370-e0f4d57751f1",
    "commands": [
      {
        "type": "manual",
        "command": "User Reports Phishing and-or Extortion"
      }
    ]
  }
}
```

Figure 64 – Details of JSON export of a CACAO playbook steps in the SAPPAN capturing tool.

While there are several models available for graph representations of playbooks, we chose BPMN for its popularity and ease of use. BPMN is widely utilized as a process visualization approach in different fields, including security response and recovery. Figure 65 is an example BPMN graph for representing a CACAO playbook for phishing. This playbook is modeled into BPMN in the CyberSEAS project and then created via the SAPPAN capturing tool. In SAPPAN, playbook steps can be interactively viewed in detail or edited by clicking on them.

Phishing Incident Response Procedure

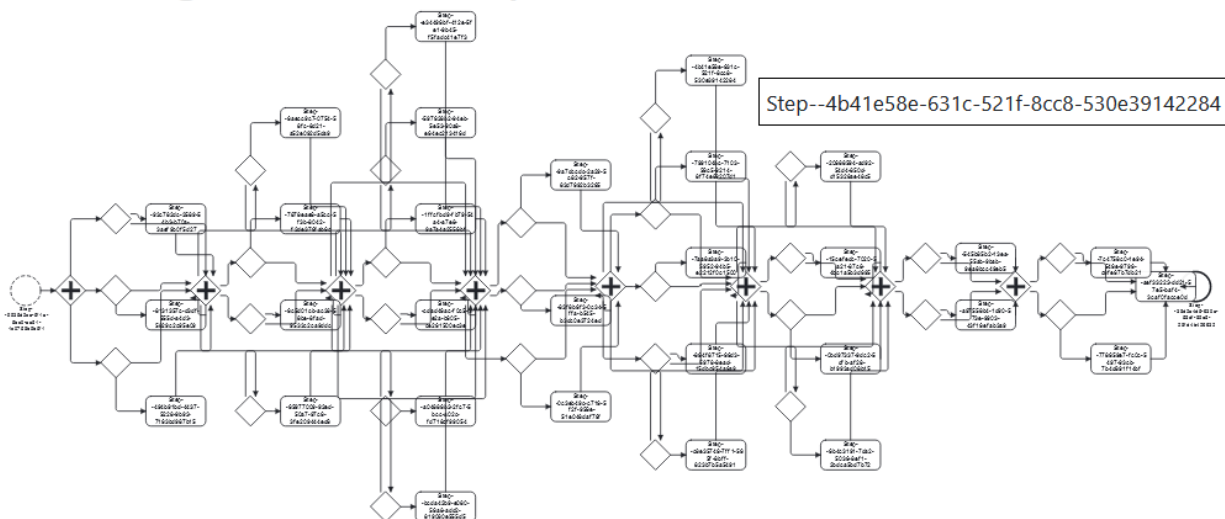


Figure 65 – BPMN representation of a sample CACAO playbook in the SAPPAN capturing tool.

Each playbook has one Initial step, which is represented by a circle. Similarly, each playbook has the Final step, which is illustrated by a thick outline circle. Intermediate steps and optional steps are displayed with boxes, while exclusive choice steps are shown with a diamond shape for decisions.

Confidentiality is clearly displayed when deriving a shareable version of a playbook, if available. For supported formats (SAPPAN), confidential information can be automatically

removed preserving the playbook structure and replacing the names of confidential steps with aliases.

In summary, the SAPPAN playbook management system is designed to be both efficient and secure. Utilizing BPMN graphs and carefully labeling each step ensures that the playbooks are easy to understand and follow. Additionally, its commitment to confidentiality means that sensitive information is always protected or sanitized before sharing.

The main functionality of the tool as a playbook management system is available as it is described in this section; however, additional functionalities such as triggering the playbooks via an IDS, selecting a proper playbook from a list of related playbooks in the knowledge repository based on the incident type and characteristics, automatic executing cortex analyzers and responders, monitoring and logging the current state of the playbook execution, as well as connection to the STIX sharing platform are considered to be potential developments for the next release.

6.6 Decision support tool

We implemented a decision support system (DSS) that facilitates the assessment of the impacts of detected cyber incidents. These impact levels determine the extent of required reporting to CERTs and the coordination between EPES operators and CERTs. DSS covers the decision-making process described in Section 3.4. It is shared and reused between tasks T4.4 and T6.4. In T6.4, DSS covers only the impact assessment phase, while in T4.4, it also facilitates the follow-up mitigation selection phase. In this section, we present the functionalities that are part of the T6.4 toolset.

DSS is implemented in VBA (Visual Basic for Applications). Its runtime environment is MS Excel. In D6.8, we also developed a web-based application integrated with the SIEM system. DSS provides several additional functionalities, particularly for group decision-making, criteria structuring and weighting, and qualitative preference modeling.

The process starts by importing information about cybersecurity-related events from SIEM. An import from a CSV (Comma-Separated Values) file is available. An example of CSV content is as follows:

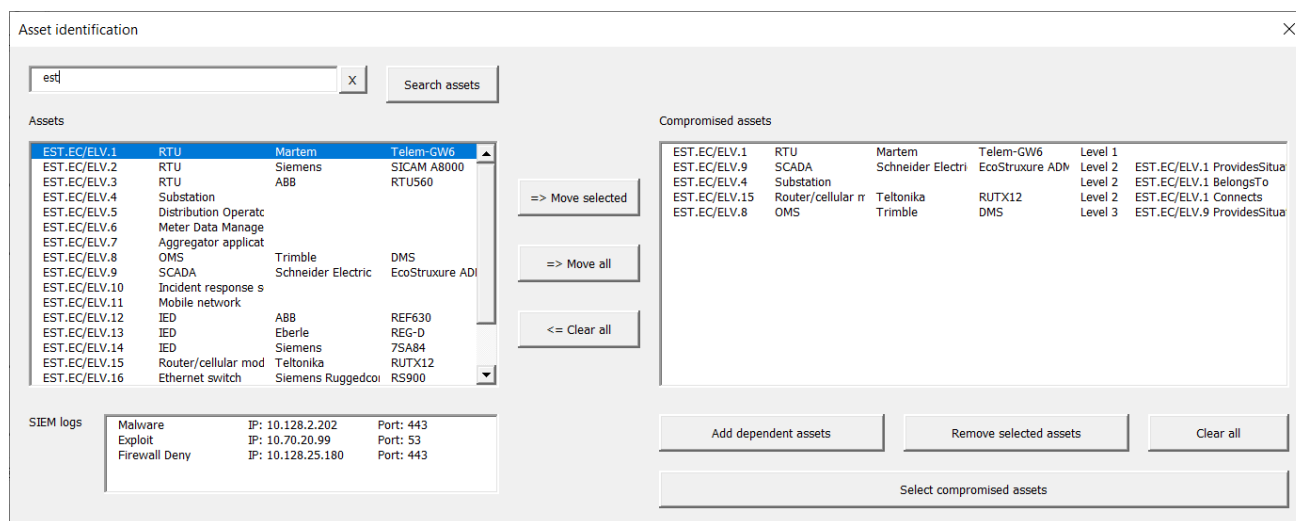
```
Malware; 28/02/2023 12:35; 28/02/2023 12:35; 33.222.30.404; 53536; 10.128.2.202; 443; 244; 1; TCP IP; System; Malware or Virus; 6; 2; 8
```

```
Exploit; 28/02/2023 15:26; 28/02/2023 15:27; 115.45.1.999; 52422; 10.70.20.99; 53; 1250; 12; TCP IP; System; Exploit or Intrusion Detection; 5; 8; 9
```

```
Firewall Deny; 01/03/2023 11:11; 02/03/2023 11:22; 2.45.99.123; 49940; 10.128.25.180; 443; 437; 3; TCP IP; System; Firewall Deny or Drop; 8; 5; 3
```

The attributes include source and target IPs, ports, network traffic data, triggered correlation rules, types of detected incidents (if possible to detect), and incident magnitude scores (if possible to estimate and if supported by a specific SIEM tool). These are not direct event logs from assets that are monitored by SIEM, but rather diagnostic reports. SIEM logs and reports are helpful in the process of analysis and decision-making but are not required. The entire decision-making process may be performed without any information from SIEM.

The first mandatory step is the identification of compromised assets. The decision-maker (for simplification, the terms “decision-maker” and “security expert” are used interchangeably in this section, although various actions could be split between these two roles) opens a user form that facilitates the asset identification activity. This form is depicted in Figure 66.



| Assets | Compromised assets |
|---|---|
| EST.EC/ELV.1 RTU Martem Telem-GW6 | EST.EC/ELV.1 RTU Martem Telem-GW6 Level 1 |
| EST.EC/ELV.2 RTU Siemens SICAM A8000 | EST.EC/ELV.2 SCADA Schneider Electri EcoStruxure ADI Level 2 EST.EC/ELV.1 ProvidesSitua |
| EST.EC/ELV.3 RTU ABB RTU560 | EST.EC/ELV.4 Substation Level 2 EST.EC/ELV.1 BelongsTo |
| EST.EC/ELV.4 Substation | EST.EC/ELV.15 Router/cellular r Teltonika RUTX12 Level 2 EST.EC/ELV.1 Connects |
| EST.EC/ELV.5 Distribution Operatc | EST.EC/ELV.8 OMS Trimble DMS Level 3 EST.EC/ELV.9 ProvidesSitua |
| EST.EC/ELV.6 Meter Data Manage | |
| EST.EC/ELV.7 Aggregator applicat | |
| EST.EC/ELV.8 OMS | |
| EST.EC/ELV.9 SCADA | |
| EST.EC/ELV.10 Incident response s | |
| EST.EC/ELV.11 Mobile network | |
| EST.EC/ELV.12 IED ABB REF630 | |
| EST.EC/ELV.13 IED Eberle REG-D | |
| EST.EC/ELV.14 IED Siemens 7SA84 | |
| EST.EC/ELV.15 Router/cellular mod Teltonika RUTX12 | |
| EST.EC/ELV.16 Ethernet switch Siemens Ruggedcoi RS900 | |

| SIEM logs | IP | Port |
|---------------|---------------|------|
| Malware | 10.128.2.202 | 443 |
| Exploit | 10.70.20.99 | 53 |
| Firewall Deny | 10.128.25.180 | 443 |

Figure 66 – Asset identification form.

A number of functionalities are supported:

- Key information that is imported from SIEM is presented to help identify compromised assets. In particular, destination IPs and ports might indicate attacked assets.
- The user can search for assets in the knowledge repository. DSS supports search on substrings, as well as on several attributes, including the asset ID, type, vendor, and product name.
- The user moves identified assets to the “Compromised assets” list box. Each moved asset is considered to be directly attacked. It is hence a level 1 compromised asset.
- The decision-maker can trigger the automatic search for dependent compromised assets. A recursive algorithm is executed that goes through all asset dependencies in the knowledge repository. It finds dependent connected assets on lower levels that might also be compromised due to cascading effects. Duplicates are prevented, which means that a dependent asset is not added to the list if it is already included, since an asset might be affected through several connection paths.
- The decision-maker is able to exclude any dependent asset from the “Compromised assets” list if it is determined that it should not be considered as compromised.
- Finally, the decision-maker confirms the identified and selected assets. An assessment matrix is then automatically generated on the “Incident impact assessment” sheet.

The decision-maker then proceeds with the identification of incidents and common attack techniques. A user form supports this identification activity. It is shown in Figure 67.

Several functionalities are available:

- SIEM information is again presented to help the decision-maker in the identification of incidents and vulnerabilities. The magnitude of an incident is also shown if available (e.g., IBM Security QRadar SIEM has this capability). This magnitude (incorporating the

D6.8 Rules & Tools for Operators' Coordination and Reporting to CERTs in Case of Incidents V2

severity, relevance, and credibility) is considered as one of the attributes to assess the impact of an incident.

- The decision-maker analyses a number of correlations. They are obtained from the mappings stored in the knowledge repository.
- All compromised assets that were identified in the previous step are presented in the first listbox. The decision-maker goes through each asset and analyses it.
- When an asset is chosen for the analysis, all relevant CVEs and attack techniques are obtained from the knowledge repository based on MITRE ATT&CK mappings.
- DSS calculates the average CVSS score for the chosen CVEs. It is important that the decision-maker has the ability to select only some CVEs from the repository because not all mapped CVEs are always relevant for a CPE. It depends on the update/patch of an asset.
- In a similar way, the decision-maker selects only the relevant attack techniques and connects them with a detected incident or threat. This incident may come directly from the imported SIEM information or may be defined manually if it is not included in SIEM information or if SIEM imports are not available.
- The decision-maker adds each relevant combination of an asset, incident, and a set of exploited attack techniques to the "Identified incidents" listbox.
- After all incidents are identified, the decision-maker confirms the selection by clicking the "Select identified incidents" button. All information is added to the assessment matrix on the "Incident impact assessment" sheet.

The screenshot shows a web-based interface for identifying incidents and attack techniques. It features several data tables and interactive elements:

- Compromised assets:** A table listing assets with columns for ID, name, manufacturer, model, and level. One asset, EST.EC/ELV.15, is selected.
- CVEs for selected asset:** A table showing CVEs associated with the selected asset, including CVE-2017-8116, CVE-2022-1012, and CVE-2022-37434.
- SIEM logs:** A table displaying log entries with columns for event type, IP address, port, and magnitude.
- Attack techniques for selected asset:** A table listing attack techniques such as T1105, T1190, and T0814.
- Identified incidents:** A table showing the final identified incidents, including EST.EC/ELV.1 and EST.EC/ELV.9, with associated attack techniques and scores.

Figure 67 – Incident identification form.

The decision-maker can now proceed to the assessment of the impacts of incidents. For this purpose, the assessment matrix is generated by DSS. It is shown in Figure 68.



| | A | B | C | D | E | F | G |
|----|--|------|---------------|--------------------------------|------------------------|-----------------------|--------------------------------|
| 1 | Asset ID | | EST.EC/ELV.1 | EST.EC/ELV.9 | EST.EC/ELV.4 | EST.EC/ELV.15 | EST.EC/ELV.8 |
| 2 | Asset type | | RTU | SCADA | Substation | Router/cellular modem | OMS |
| 3 | Asset vendor | | Martem | Schneider Electric | | Teltonika | Trimble |
| 4 | Asset product | | Telem-GW6 | EcoStruxure ADMS | | RUTX12 | DMS |
| 5 | Asset level | | Level 1 | Level 2 | Level 2 | Level 2 | Level 3 |
| 6 | Dependency | | | EST.EC/ELV.1 ProvidesSituation | EST.EC/ELV.1 BelongsTo | EST.EC/ELV.1 Connects | EST.EC/ELV.9 ProvidesSituation |
| 7 | Incident type | | Firewall Deny | Firewall Deny | Firewall Deny | Exploit | Exploit |
| 8 | Attack techniques | | | T0886, T0888 | T0814 | T1105, T1190, T0814 | T1210 |
| 9 | SIEM magnitude | 0,10 | 5,33 | 5,33 | 5,33 | 7,33 | 7,33 |
| 10 | CVSS V2.0 | 0,10 | 7,50 | 8,75 | | 9,33 | 10,00 |
| 11 | System scale | 0,05 | 7,00 | | | | |
| 12 | Public safety concern | 0,05 | 6,00 | | | | |
| 13 | Workforce safety concern | 0,05 | 5,00 | | | | |
| 14 | Ecological concern | 0,05 | 4,00 | | | | |
| 15 | Financial impact on utility | 0,05 | 8,00 | | | | |
| 16 | Restoration costs | 0,05 | 8,00 | | | | |
| 17 | Negative impact on generation capacity | 0,05 | 10,00 | | | | |
| 18 | Negative impact on energy market | 0,05 | 9,00 | | | | |
| 19 | Negative impact on transmission system | 0,05 | 9,00 | | | | |
| 20 | Negative impact on customer service | 0,05 | 7,00 | | | | |
| 21 | Destroys goodwill toward utility | 0,05 | 3,00 | | | | |
| 22 | Immediate economic damage | 0,05 | 8,00 | | | | |
| 23 | Long term economic damage | 0,05 | 7,00 | | | | |
| 24 | Privacy loss of stakeholders | 0,05 | 10,00 | | | | |
| 25 | Resilience of asset | 0,05 | 6,00 | | | | |
| 26 | Relevance of asset | 0,05 | 9,00 | | | | |
| 27 | Impact score | 1,00 | 7,08 | 1,41 | 0,53 | 1,67 | 1,73 |
| 28 | | | | | | | |
| 29 | | | | | | | |

Figure 68 – Partially filled in incident impact assessment matrix.

Initially, this matrix is prefilled only with SIEM magnitudes and CVSS scores that were obtained during the incident identification activity. Scores with regard to other criteria are provided by the decision-maker. In accordance with the introduced scoring system, only scores from 0 to 10 may be chosen from the list in each cell or typed in manually. The aggregated impact scores are categorized/colored.

Several criteria are considered in the assessment. Most of them come from the NESCOR model as explained in Section 3.4. Criteria are weighted, so the weighted sum is used as the aggregated score.

| | A | B | C | D | E | F | G |
|----|--|------|---------------|--------------------------------|------------------------|-----------------------|--------------------------------|
| 1 | Asset ID | | EST.EC/ELV.1 | EST.EC/ELV.9 | EST.EC/ELV.4 | EST.EC/ELV.15 | EST.EC/ELV.8 |
| 2 | Asset type | | RTU | SCADA | Substation | Router/cellular modem | OMS |
| 3 | Asset vendor | | Martem | Schneider Electric | | Teltonika | Trimble |
| 4 | Asset product | | Telem-GW6 | EcoStruxure ADMS | | RUTX12 | DMS |
| 5 | Asset level | | Level 1 | Level 2 | Level 2 | Level 2 | Level 3 |
| 6 | Dependency | | | EST.EC/ELV.1 ProvidesSituation | EST.EC/ELV.1 BelongsTo | EST.EC/ELV.1 Connects | EST.EC/ELV.9 ProvidesSituation |
| 7 | Incident type | | Firewall Deny | Firewall Deny | Firewall Deny | Exploit | Exploit |
| 8 | Attack techniques | | | T0886, T0888 | T0814 | T1105, T1190, T0814 | T1210 |
| 9 | SIEM magnitude | 0,10 | 5,33 | 5,33 | 5,33 | 7,33 | 7,33 |
| 10 | CVSS V2.0 | 0,10 | 7,50 | 8,75 | | 9,33 | 10,00 |
| 11 | System scale | 0,05 | 7,00 | 6,00 | 6,00 | 6,00 | 5,00 |
| 12 | Public safety concern | 0,05 | 6,00 | 5,00 | 5,00 | 5,00 | 4,00 |
| 13 | Workforce safety concern | 0,05 | 5,00 | 4,00 | 1,00 | 4,00 | 3,00 |
| 14 | Ecological concern | 0,05 | 4,00 | 3,00 | 3,00 | 3,00 | 2,00 |
| 15 | Financial impact on utility | 0,05 | 8,00 | 6,00 | 6,00 | 6,00 | 5,00 |
| 16 | Restoration costs | 0,05 | 8,00 | 6,00 | 1,00 | 6,00 | 5,00 |
| 17 | Negative impact on generation capacity | 0,05 | 10,00 | 8,00 | 3,00 | 8,00 | 6,00 |
| 18 | Negative impact on energy market | 0,05 | 9,00 | 7,00 | 3,00 | 7,00 | 6,00 |
| 19 | Negative impact on transmission system | 0,05 | 9,00 | 7,00 | 3,00 | 7,00 | 6,00 |
| 20 | Negative impact on customer service | 0,05 | 7,00 | 6,00 | 6,00 | 6,00 | 5,00 |
| 21 | Destroys goodwill toward utility | 0,05 | 3,00 | 2,00 | 2,00 | 2,00 | 2,00 |
| 22 | Immediate economic damage | 0,05 | 8,00 | 6,00 | 6,00 | 6,00 | 5,00 |
| 23 | Long term economic damage | 0,05 | 7,00 | 6,00 | 6,00 | 6,00 | 5,00 |
| 24 | Privacy loss of stakeholders | 0,05 | 10,00 | 8,00 | 4,00 | 8,00 | 6,00 |
| 25 | Resilience of asset | 0,05 | 6,00 | 5,00 | 5,00 | 5,00 | 4,00 |
| 26 | Relevance of asset | 0,05 | 9,00 | 7,00 | 7,00 | 7,00 | 6,00 |
| 27 | Impact score | 1,00 | 7,08 | 6,01 | 3,88 | 6,27 | 5,48 |
| 28 | | | | | | | |
| 29 | | | | | | | |

Figure 69 – Completed incident impact assessment matrix.

The decision-maker does not need to provide all scores. It suffices that the impact of security incidents on level 1 assets is assessed. The decision-maker can then go to the control panel and execute the "Estimate dependent impacts" functionality. Based on LIRI and criteria-wise scores of level 1 assets, DSS can automatically recursively calculate the impacts of incidents on all assets on lower levels. Of course, the decision-maker has to afterwards return to the matrix to verify estimations and make appropriate corrections. The completed (fully filled in) impact assessment matrix can be seen in Figure 69.

7 Implementation and verification of rules and tools (new)

This section describes the implementation of the introduced procedures, rules, and tools for operators' coordination and reporting to CERTs. Several scenarios are prepared and utilized to verify functional and non-functional requirements. These scenarios are further upgraded in D7.4 to validate tools from the CyberSEAS toolset, especially the SAPPAN tool. A local test and deployment environment is set up on the INF, SI-CERT, and FRAUNHOFER infrastructure to facilitate the implementation and verification.

7.1 Infrastructure setup

This section presents the virtual INF infrastructure, the SI-CERT CTI exchange and cooperation infrastructure, and the SAPPAN deployment environment. This infrastructure is required to implement and verify rules and tools for reporting and coordination.

7.1.1 INF Virtual Pilot Infrastructure

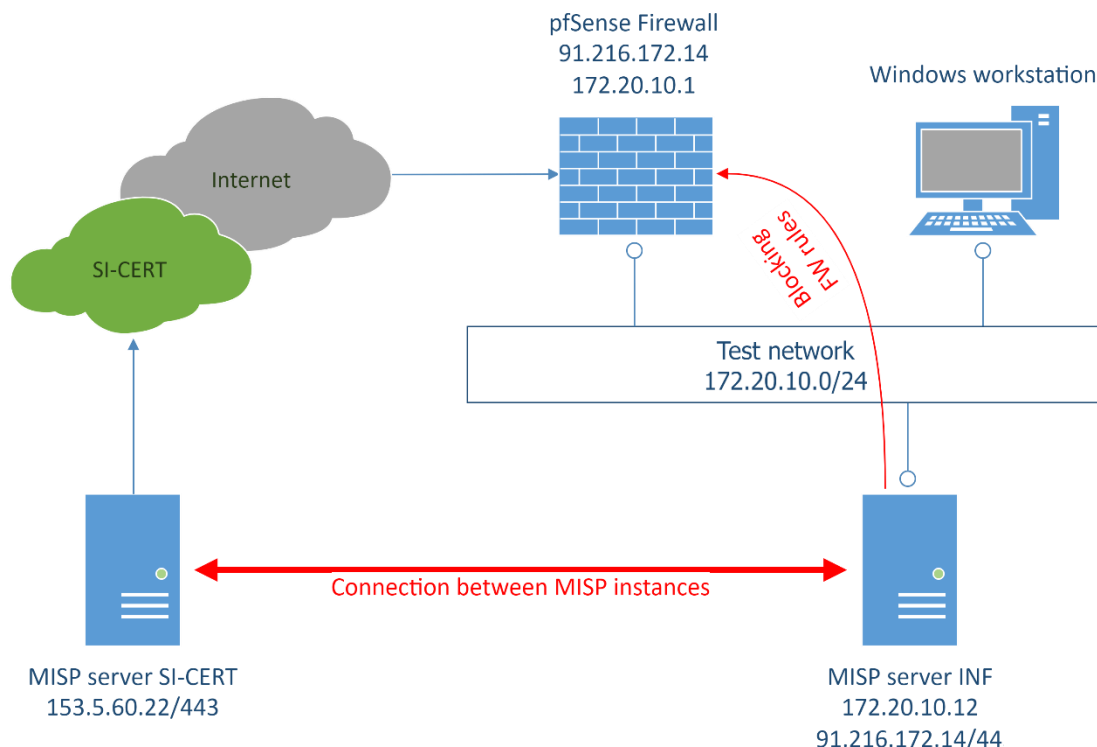


Figure 70 – INF virtual pilot infrastructure for the CTI exchange scenario.

The virtual pilot infrastructure is depicted in Figure 70. The INF test environment consists of a restricted network, which includes the following assets:

- the MISP server deployed on the 64-bit Red Hat Enterprise Linux 8 with the DNS name `cslab-misp-cs.in.si` and the static IP address `172.20.10.0`;

- two end-user workstations with dynamic IP addresses running on the Microsoft Windows 10 operating system;
- the SAPPAN workstation cslab-sappan.in.si running on the 64-bit Ubuntu Linux at the 172.20.10.11 static IP address;
- the pfSense 2.7.1 firewall configured at the 91.216.172.14 static IP address.

For CTI exchange and reporting, another MISP server is configured within the SI-CERT network. The INF MISP server is synchronized with the SI-CERT MISP server in the INF test environment.

7.1.2 SI-CERT MISP CTI Sharing Infrastructure

Based on the project's needs, a dedicated MISP infrastructure has been set up. The MISP infrastructure used for scenario testing and PoC is similar to the production MISP infrastructure but simplified to some degree. It consists of a simulated remote MISP instance, playing the role of outside MISP partners that SI-CERT is exchanging data with. It also plays the role of outside MISP partner connections providing threat info inside and outside the EU cyberspace. The instance is further connected to the SI-CERT MISP instance, which is exchanging data with EPES local partners. This infrastructure is schematically presented in Figure 71.

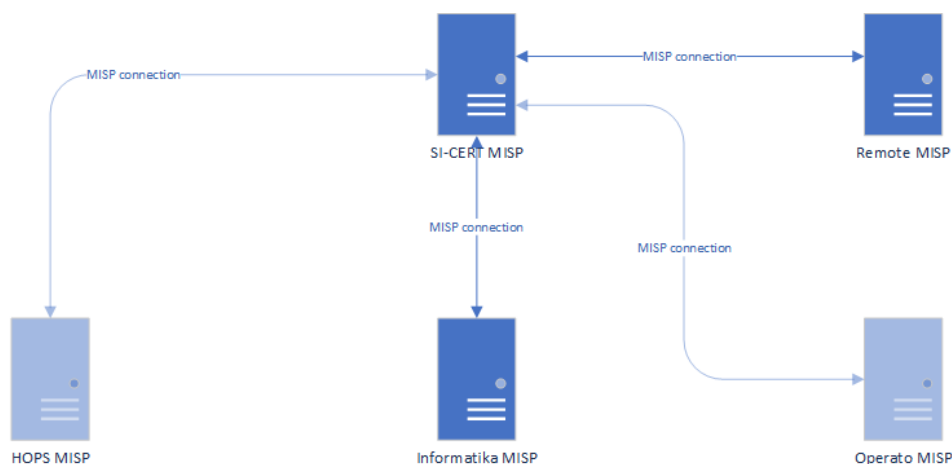


Figure 71 – SI-CERT MISP infrastructure for the CTI exchange scenario.

7.1.3 SAPPAN Deployment Environment and extended functionalities

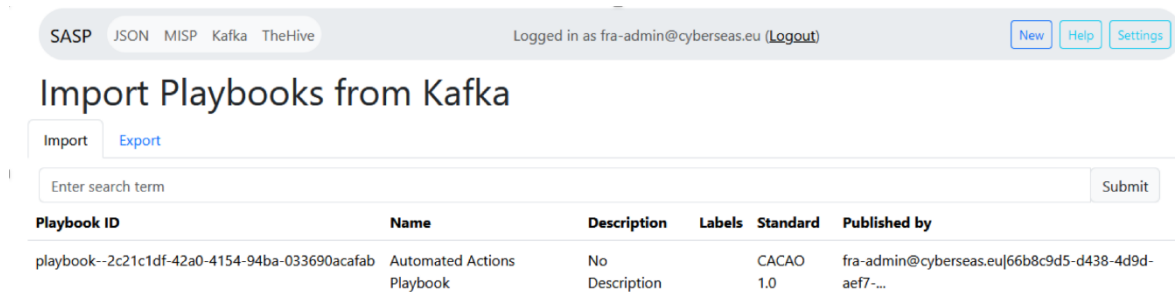
The playbook management tool is developed to produce and manage machine-readable playbooks with a user-friendly interface, in a proprietary format of a standardized CACAO format from the OASIS consortium. The CACAO standard [53] promotes automation by providing structured playbooks with machine-readable instructions, such as OpenC2 commands, and specifying targets like IP addresses for response actions. The tool features import and export functionality for playbooks, integration with the MISP CTI sharing platform for playbook distribution among teams and external organizations, and user-oriented options like playbook versioning for incremental enhancements and the automatic generation of BPMN graphs for visual representation. It also allows for playbook reuse as templates or to

invoke other playbooks as part of the workflow. The tool offers benefits like improved searchability, streamlined version control, and seamless integration with CI/CD practices. Present efforts are focused on integrating the tool with TheHive, a security incident response platform, with the objective of establishing an extensive playbook repository for a variety of organizational situations.

The tool can be deployed as a standalone application, utilising various technologies including MediaWiki, Semantic MediaWiki, Docker, PHP, Python, Django, Bootstrap, mwclient, pm4py, pymisp, and CACAO for development. It is compatible with both Windows and Unix-based systems, offering automatic installation commands or the option for manual installation as described in the tool's documentation. The tool features a web interface based on Python, which runs on the local host. It can seamlessly interact with TheHive and MISP through REST API integration. The tool functionality has been extended during the project to support integration with Kafka and Keycloak, enable seamless communication with other toolsets within the CyberSEAS framework, and align with the conceptual framework for automation and reporting. Playbooks can be stored locally or shared and stored within MISP instances.

7.1.3.1 Playbook sharing via Kafka

Kafka is an open-source distributed event streaming platform developed by the Apache Software Foundation. We provide the ability to export our playbooks as JSON and immediately publish them as an event in a connected Kafka instance while at the same time providing the ability to search Kafka for already published playbooks and import them directly into our tool. Together with raw JSON files and MISP, this provides a third way of sharing playbooks between organizations, and it includes alignment with the general CyberSEAS architecture and toolset communication. Figure 72 illustrates the playbook importing functionality of the tool through a Kafka instance.



| Playbook ID | Name | Description | Labels | Standard | Published by |
|--|----------------------------|----------------|--------|----------|---|
| playbook--2c21c1df-42a0-4154-94ba-033690acafab | Automated Actions Playbook | No Description | CACAO | 1.0 | fra-admin@cyberseas.eu[66b8c9d5-d438-4d9d-ae7f-...] |

Figure 72 – Importing playbooks from a connected Kafka instance.

7.1.3.2 Sharing and storing playbooks via MISP

Playbooks can be easily shared via a connected MISP instance and received by the relevant partners. MISP can also be used as a repository to search for relevant playbooks based on the metadata attached to them. Figure 73 illustrates an example of a shared playbook from the playbook management tool as the MISP event and the relevant metadata attached to it.

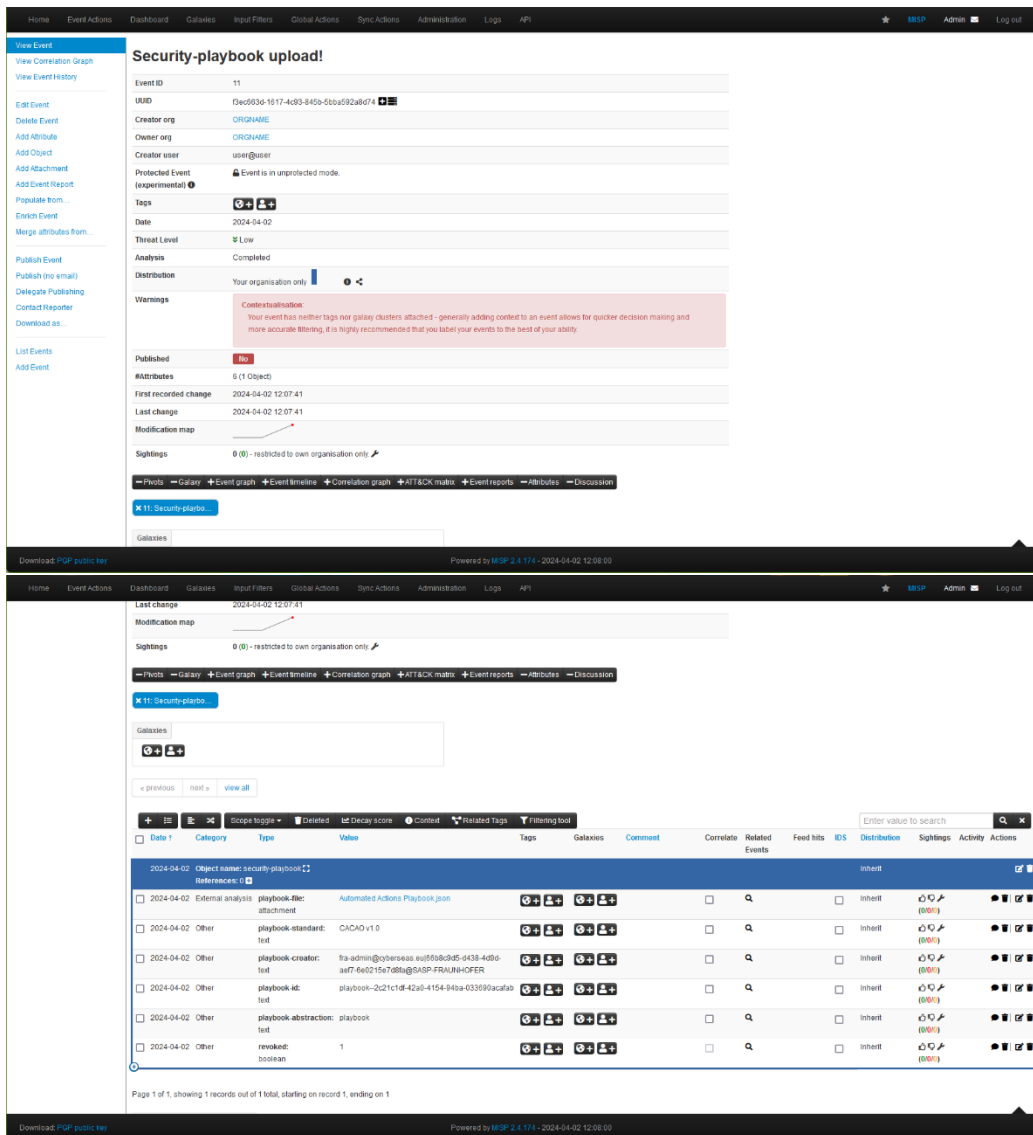


Figure 73 – Playbook sharing as an event via MISP (top), and more relevant metadata attached (bottom).

7.1.3.3 Automation component

The aim of the development is not only to facilitate the management of playbooks but also to automate their execution, saving operator time by performing routine analysis tasks before even noticing the alert or immediately reacting in case of possible security violations.

Given the extensive range of potential responses to an incident, we have integrated with the existing response platforms TheHive and Cortex. Once the playbook management tool is connected to an operational Hive instance, users are presented with an overview of open cases on Hive, and they have the capability to execute a playbook on such a case. Commands within this playbook may be manual, interrupting the workflow to prompt the user for confirmation of command execution, or they may utilize a robust syntax for invoking Cortex Responders and Analyzers. This syntax incorporates variables that grant access not only to the fields and artifacts of the active case but also to the results from previously

executed Analyzers/Responders. The use of these variables in conditional statements like while, switch, and if steps enable the creation of complex playbooks that can dynamically adapt to varying scenarios. At each stage of execution, an overview page displays a JSON-formatted report detailing the current state, active steps, and any steps that necessitate attention or confirmation. Figure 74 shows a sample of the tool functionality for showing the current state of a playbook execution, and Figure 75 depicts the visual overview of a sample playbook execution for monitoring.

Figure 74 – The overview page for an active playbook execution with the command prompt.

Figure 75 – The visual overview page to display the current stage of an active playbook execution.

7.1.4 CyberRange Incident Response Environment

The CyberRange environment enables the automation and verification of chosen CACAO-based incident response and reporting procedures for the SLO&CRO pilot. Of particular interest are INF's malware, ransomware, and phishing playbooks modeled in the executable CACAO notation. We use the CyberRange infrastructure to execute a playbook and deploy all necessary tools. CyberRange contains and utilizes:

- TheHive/Cortex for analyzers and responders;
- SAPPAN for playbook sharing and execution;
- SIEM to detect cyber incidents;
- MISP for CTI exchange and reporting; and
- DSS to assess the impact of cyber incidents and trigger the appropriate coordination and reporting mechanisms based on their severity.

The CyberRange incident response environment, which is set up for verification scenarios, is depicted in Figure 76. Additional details are provided in Section 6. Please refer to Figure 45 and its description.

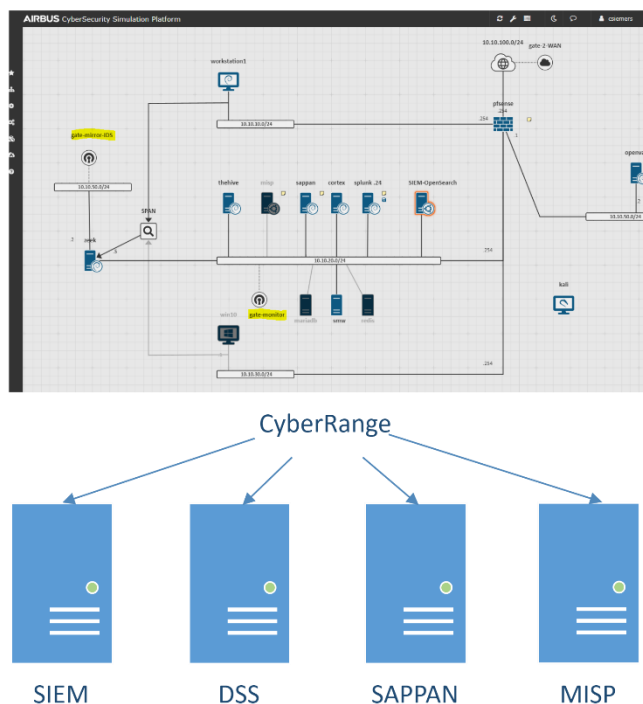


Figure 76 – CyberRange incident response environment.

7.2 MISP reporting and CTI sharing scenarios

This section describes the implementation of a standardized protocol for reporting and coordination with the national CERT for the SLO&CRO pilot based on the MISP platform.

7.2.1 Motivation

The purpose of MISP is to enable organizations and SOCs to share threat intelligence on completed cases or events, such as IoCs and other artifacts, in real time to help each other prevent cyber-attacks. Another possibility for organizations and SOCs is to use MISP to be connected with CERTs. This positions MISP as a powerful platform for the exchange of CTI between national SOCs and national CERTs in the common EU data space. Therefore, SI-CERT already follows several data feeds for systems in Slovenia that show newly discovered vulnerabilities or unusual behavior that may be the result of cybersecurity incidents. SI-CERT also encourages OESs and other entities, such as governmental institutions, to join the local MISP network for faster IoC sharing.

CTI exchange through MISP can be implemented by connecting two or more MISP instances, e.g., the SOC MISP to the CERT MISP, or vice versa. The second approach is to connect MISP with other security systems or tools to enable the exchange of cybersecurity-related data and the automation of cybersecurity operations. Two common possibilities are to integrate MISP with SIEM or firewall. This opens many possible scenarios to enhance the security of IT and OT environments in the EPES ecosystem.

Such a scenario was implemented in the SLO&CRO pilot by INF and SI-CERT. Section 7.2.2 describes it in detail to show the concept of IoC exchange and utilization based on the MISP protocol. The outline of the scenario is as follows:

1. The SOC environment is protected with the pfSense firewall.
2. SOC and CERT have their own MISP servers set up. Both MISP instances are part of the community and are synchronized. IoC exchange is automated with a script, which makes an API (Application Programming Interface) connection secured with a generated API key.
3. CERT's MISP is further connected through the community with MISP servers of several other national CERTs in the common EU data space.
4. The national CERT shares newly identified security events, such as C2 attacks, with the SOC through connected MISPs. These events are usually propagated within the community from other connected MISP instances of partner CERTs in the common EU data space.
5. SOC runs periodically a cron job script that retrieves new malicious IPs from the MISP instance, generates a list of blocked IPs, and then creates IP blocking rules on the pfSense firewall.

This procedure demonstrates the possibility of CTI exchange through MISP and direct use of information on IoCs to automatically and immediately enhance the security of the IT and OT environments. As soon as a new malicious IP is detected, it gets shared through connected MISP instances in the entire community. It is in turn propagated to all national SOCs. After receiving it, the SOC automatically protects the infrastructure of the EPES ecosystem by blocking the IP with the firewall.

In case the SOC detects a new incident, MISP can also be used for CTI sharing in the other direction, which means that the new event is propagated from the SOC to the national CERT and then further through the community to CERTs in other EU countries and, in the last stage, to all other connected energy SOCs. In addition, this approach allows for the reporting to CERTs. The MISP event published by the SOC can include a specific reporting object. In the

SLO&CRO pilot, the NOKI object is defined and implemented. It includes attributes, such as reference number, subject, reporting organization, reportername, reporter contact, incident start timestamp, incident detection timestamp, incident taxonomy, incident category, incident description, incident severity, incident impact, voluntary reporting status, etc. The JSON format is used to specify the NOKI object and import it into MISP.

7.2.2 CTI sharing scenario for EPES SOC providers

A persistent threat to organizations is the infection of workstations by opening malicious email attachments or visiting websites with injected malicious code. In the event of an ongoing malware campaign, there is a small window of time that the infection might not be detected by the installed endpoint detection agent or the infection is present in an environment not running an antimalware solution. In the case that a workstation gets infected, the malicious traffic and data loss can be limited on the border network inspection devices, e.g., the firewall of the organization, which means that the firewall is updated with the latest signatures. The CTI information can be received through MISP and extracted in real time to prevent the infection from contacting the Command and Control (C2) server. In this scenario, the SI-CERT MISP can receive the infection network IoCs from the MISP instance of a foreign partner. The IoCs that can be the result of malware analysis in a sandbox or static analysis are shared with Informatika and other EPES partners via MISP. The propagated IoCs are received by Informatika and extracted in the appropriate firewall format. In the case of an infection with malware that has already been analyzed and its IoCs extracted and added to the firewall, the consequent malicious network connections are blocked and the network administrator is notified of the infected workstation. This is shown in Figure 70 from the point of view of INF and in Figure 77 from the perspective of SI-CERT.

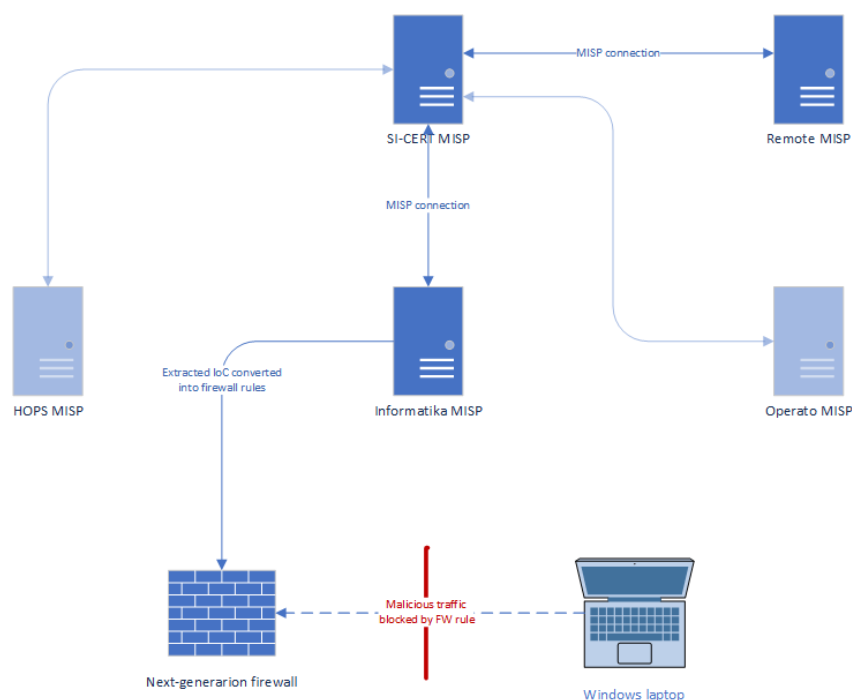


Figure 77 – Malware blocking on the firewall based on CTI exchange in the community.

Below, we provide a detailed description of the implementation utilizing the infrastructure of INF. The procedure starts as IoCs involving the Trickbot C2s are distributed via SI-CERT MSP to the MSP instance of Informatika. An event is pulled off the remote MSP instance with new IoCs regarding C2 spreading. Once gathered in INF MSP, IoCs are automatically extracted and pushed to the local Informatika's firewall to prevent communication with malicious C2 servers. The malicious communication is detected, and the SOC team is notified.

7.2.2.1 Definition of a list of blocked ID addresses

A cron job script running on the MSP server in the INF virtual test environment creates the list of blocked IP addresses. It uploads the list in text format to the local website.

The script is executed on the MSP server by an API call. It has to be authenticated with an API key. We generate the API key in the web user interface of MSP as shown in Figure 78. We securely save it for future use as it cannot be regenerated.

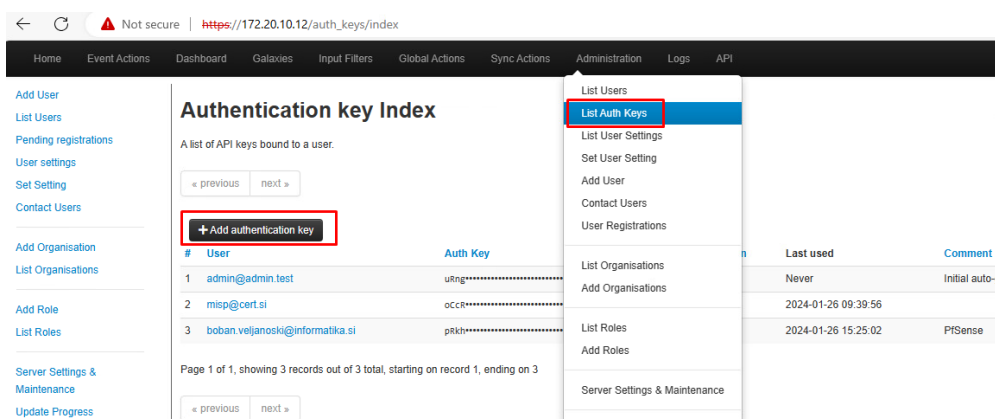


Figure 78 – Generation of the authentication key for API calls to the MSP server.

The script to generate the list of blocked IP addresses from the events published on INF's MSP instance runs once each minute from the cron system on the MSP server. The procedure to generate the list is as follows:

1. We connect to the local MSP server and run a query on MSP events with the following conditions:
 - "returnFormat":"text"
 - "type":"ip-src"
 - "category":"Network activity"
 - "last":"90d"
 - "enforceWarninglist":true
 - "to_ids":true
2. We use a regex filter to obtain IP addresses, such that there is only one IP in each line: `grep -oe '^[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}$'`.
3. We again connect to the MSP server and run a query considering the following conditions:
 - "returnFormat":"text"
 - "type":"domain | ip"
 - "category":"Network activity"

- "last":"90d"
 - "enforceWarninglist":true
 - "to_ids":true
4. We once more filter the list with a regex which returns the domain in addition to IP addresses contained in each line: `grep -oe '[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}'`.
 5. We store the results of both queries in the `blocklist.txt` file, which is stored locally at the following URL: `http://172.20.10.12/blocklist.txt`.

We run the script with the below command:

```
# cat /etc/cron.d/update-blocklist-file
* * * * * root /root/api/update-web-blocklist.sh
```

The complete script code is as follows:

```
[root@cslab-misp-cs api]# cat update-web-blocklist.sh
#!/bin/bash

/root/api/get-ipsrc-blocklist.sh | grep -oe '^([0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\})$' >
/var/www/html/blocklist.txt.tmp

/root/api/get-domainip-blocklist.sh | grep -oe '([0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\})$' >>
/var/www/html/blocklist.txt.tmp

cp /var/www/html/blocklist.txt.tmp /var/www/html/blocklist.txt

[root@cslab-misp-cs api]# cat get-domainip-blocklist.sh
#!/bin/bash

curl \
  --insecure \
  -d '{"returnFormat":"text","type":"domain|ip","category":"Network activity","last":"90d","enforceWarninglist":true,"to_ids":true}' \
  -H "Authorization: *****" \
  -H "Accept: application/json" \
  -H "Content-type: application/json" \
  -s \
  -X POST https://172.20.10.12/attributes/restSearch
[root@cslab-misp-cs api]#
[root@cslab-misp-cs api]# cat get-ipsrc-blocklist.sh
#!/bin/bash

curl \
  --insecure \
  -d '{"returnFormat":"text","type":"ip-src","category":"Network activity","last":"90d","enforceWarninglist":true,"to_ids":true}' \
  -H "Authorization: *****" \
```

```
-H "Accept: application/json" \  
-H "Content-type: application/json" \  
-s \  
-X POST https://172.20.10.12/attributes/restSearch
```

7.2.2.2 Configuration of the pfSense firewall

The pfSense firewall is configured to periodically obtain the list of blocked IP addresses from the `http://172.20.10.12/blocklist.txt` URL. It then inserts data on IPs from this file into the user-defined table `misp_blocktable` using the Aliases/URLs native function. This table is accessed by the implemented firewall filtering rule to block the traffic from the list of malicious IP addresses.

The configuration procedure is as follows:

1. We define Aliases/URLs.
2. We add the `misp_blocktable` table as shown in Figure 79, where the table type is »URL Table (IPs)« and the frequency of updates is 1 day.
3. We create the firewall rule as presented in Figure 80 and Figure 81, such that the following properties are set:
 - Action: Block
 - Address Family: IPv4
 - Protocol: Any
 - Source: Address or Alias: `misp_blocktable` (the name of the used table)
4. The preset update frequency is 1 day, so we can make a bypass to implement shorter updates (e.g., in 5 minutes) by creating the `/etc/cron.d/mips-update` with the contents: `*/5****root/usr/bin/nice-n20/etc/rc.update_urltablesnow forceupdate!`

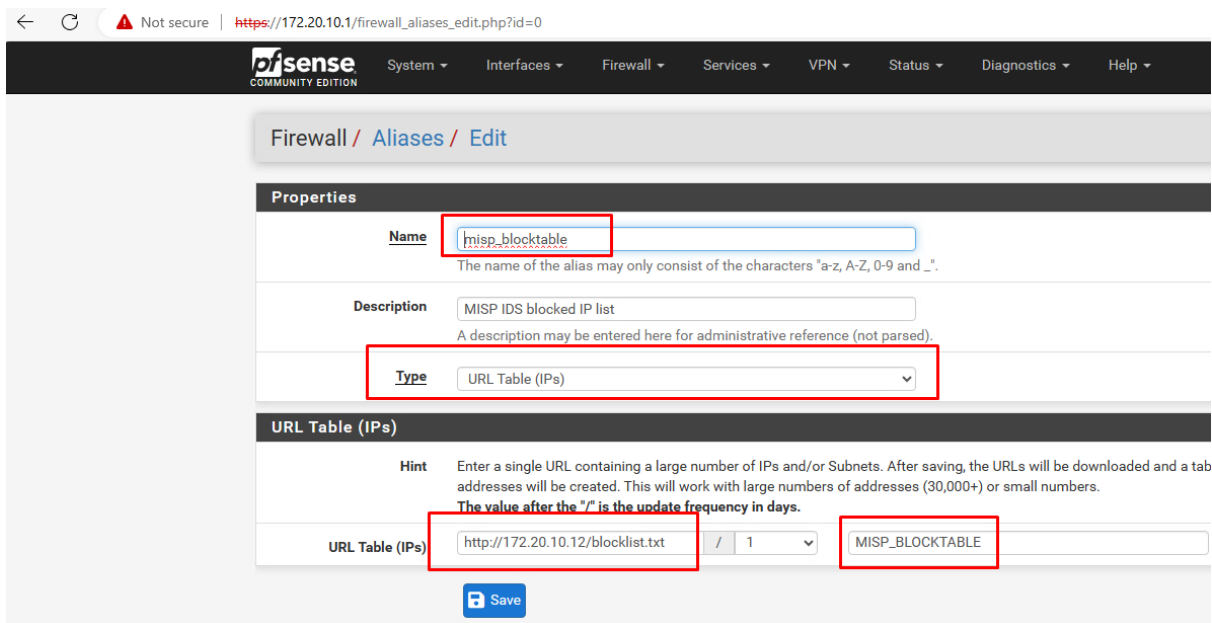


Figure 79 – Definition of the MISP block table in the pfSense firewall.

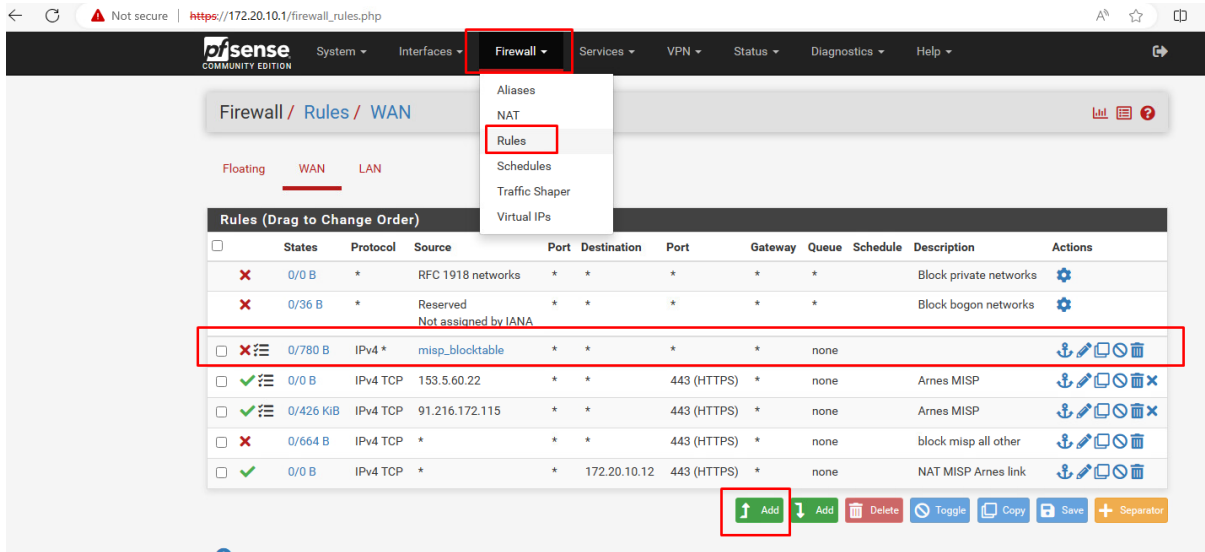


Figure 80 – Creation of the pfSense firewall blocking rule.

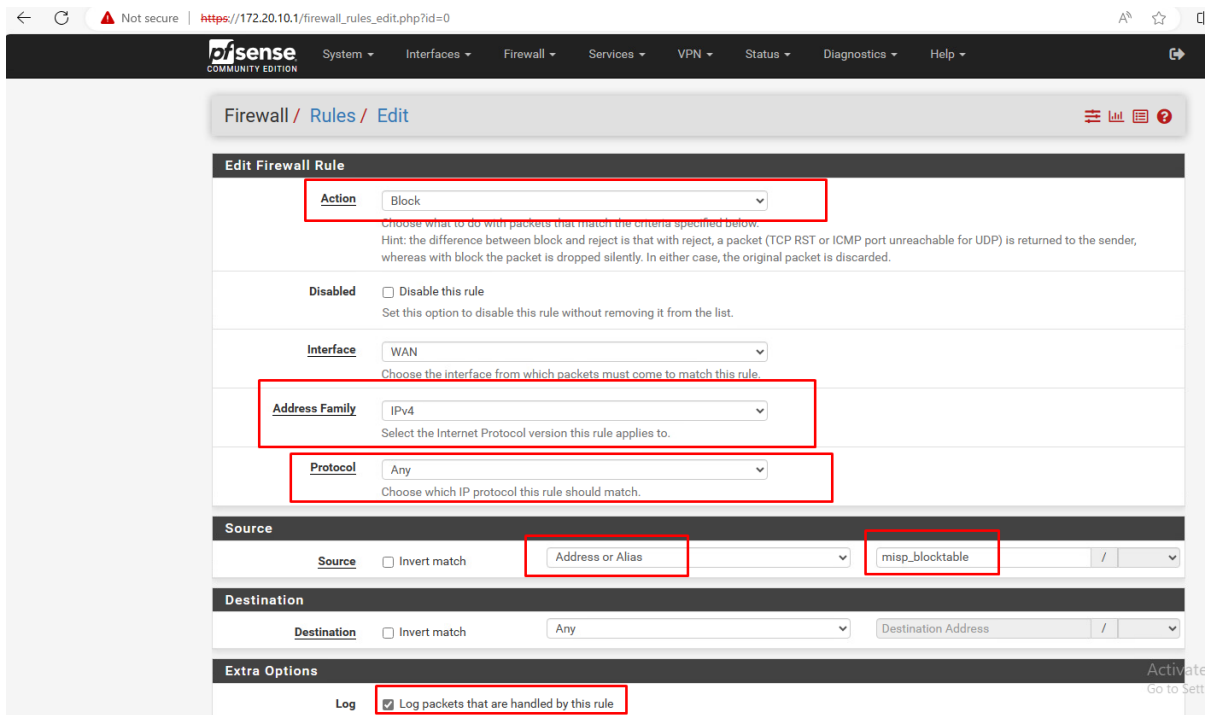


Figure 81 – Definition of the pfSense firewall blocking rule.

7.2.2.3 Scenario execution

Si-CERT MISP publishes and shares new events on malicious network activity with INF MISP. We can look up these events in INF MISP as shown in Figure 82.

D6.8 Rules & Tools for Operators' Coordination and Reporting to CERTs in Case of Incidents V2

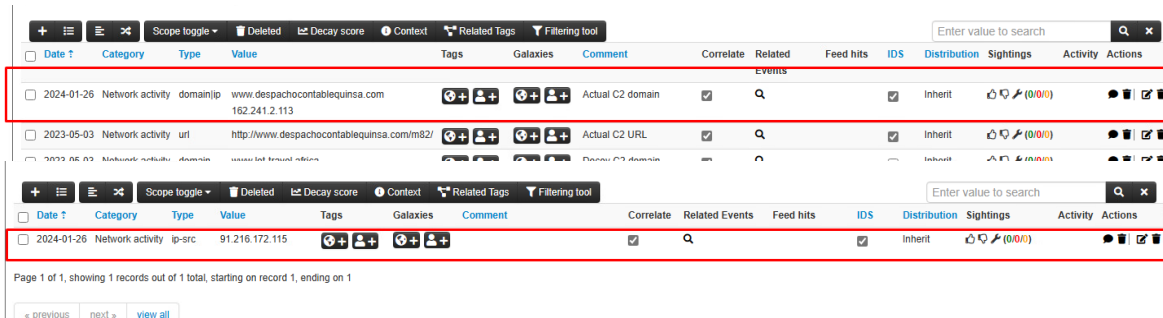


Figure 82 – Published and shared network activity events in MISP.

We check the list of blocked IP addresses at the <http://172.20.10.12/blocklist.txt> URL. It includes both published IP addresses:

```
# curl http://172.20.10.12/blocklist.txt
91.216.172.115
162.241.2.113
```

We now check the `misp_blocktable` table on the pfSense firewall. As demonstrated in Figure 83, it contains both malicious IPs.

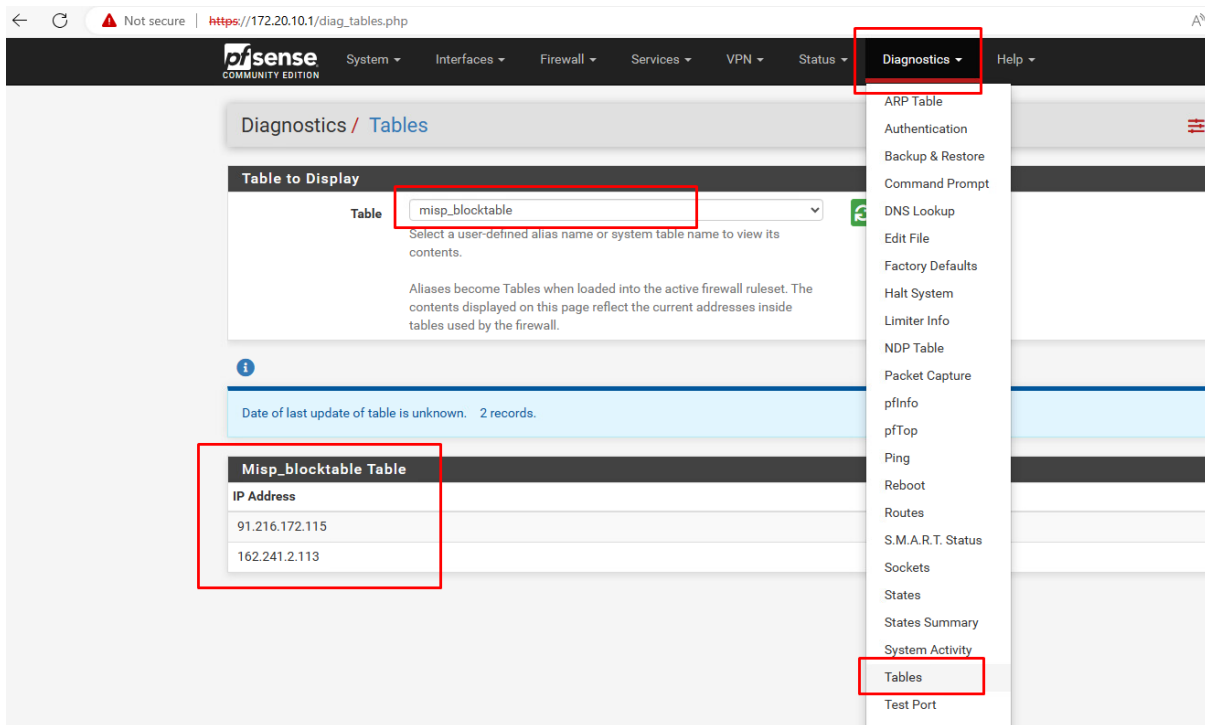


Figure 83 – Table of blocked IPs on the firewall.

We can now test traffic blocking. We try to access the published 91.216.172.115 IP address from the INF network. The firewall blocks the connection, which is hence not established. We can see this in system logs as depicted in Figure 84.

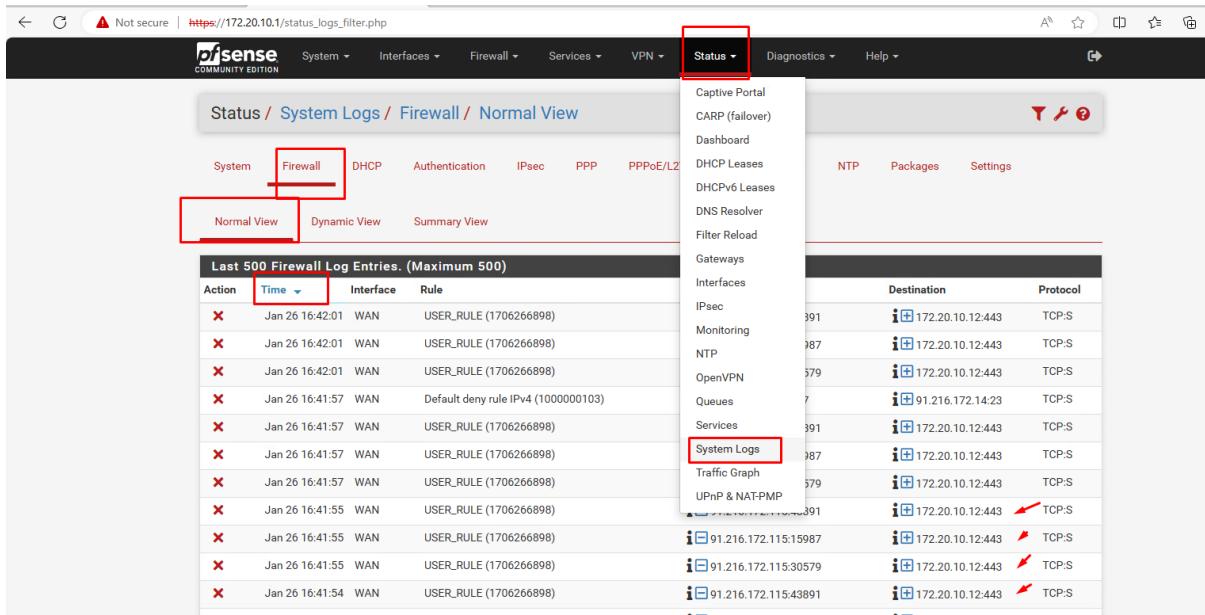


Figure 84 – System logs of firewall traffic blocking.

We can also resolve an IP address after some time if it ceases to be malicious. In this case, we uncheck the IDS parameter of the MISP event belonging to a relevant IP address (e.g., 91.216.172.115) and republish the event. This is shown in Figure 85.

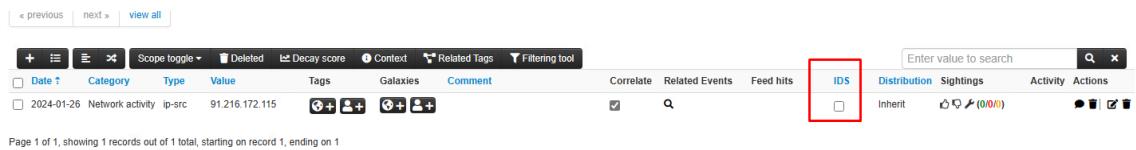


Figure 85 – Resolving an IP address in MISP.

After 5 minutes, the pfSense firewall updates the *misp_blocktable* table. It no longer contains the 91.216.172.115 IP address as evident from Figure 86 and Figure 87. This IP address can now be accessed because the firewall no longer blocks it.

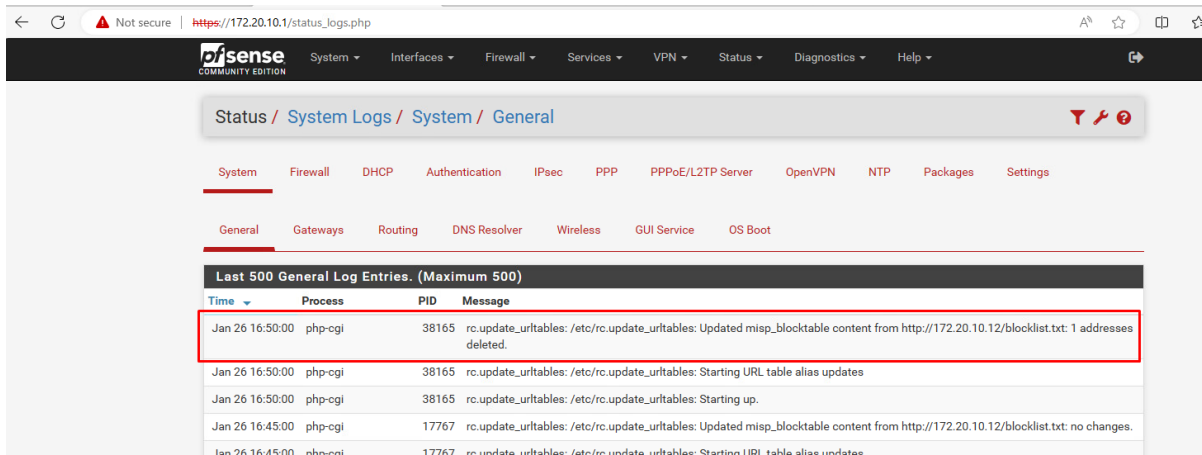


Figure 86 – Unblocking of an IP address on the firewall.

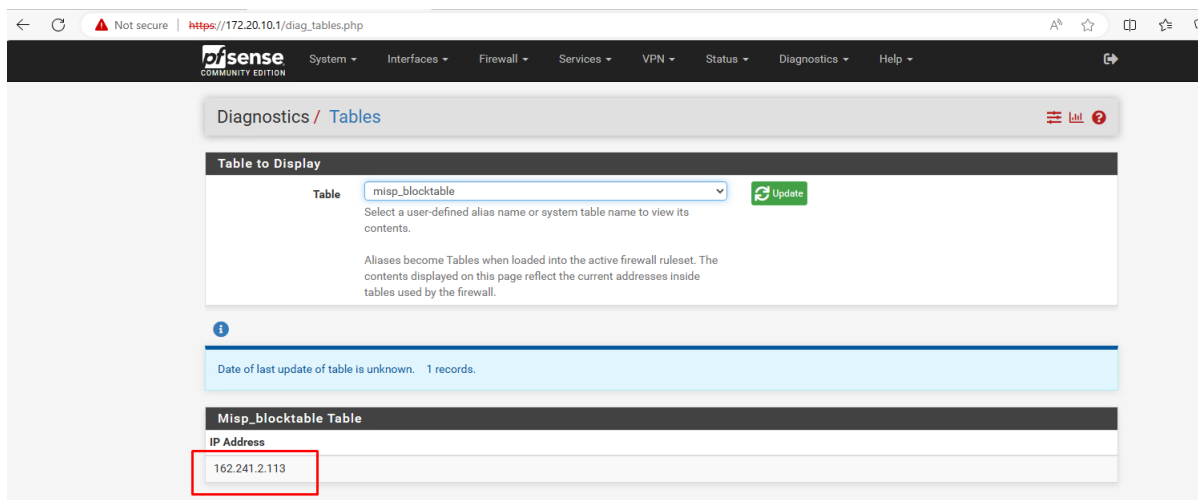


Figure 87 – Unblocked IP address on the firewall.

To implement blocking on the pfSense firewall, we followed the recommended practices of the SANS Institute [86] and the best practices to set the URL table update frequency [87]. We used the MISP automation API (<https://www.misp-project.org/openapi/>) for implementation. It should be noted that several IP addresses are referenced in this section. They pertain to the virtual pilot infrastructure and do not represent any production assets of INF or DSOs. They are consequently not required to be treated as confidential.

7.2.3 MISP-based incident reporting scenario

In this CTI exchange scenario, INF publishes phishing IoC data and reports the incident to SI-CERT through a NOKI object via MISP. This approach enables IoCs targeting the EPES sector to be detected and shared via MISP. We simulated it on the INF pilot infrastructure.

INF detects a phishing attack targeting its infrastructure and aiming at its constituency. To prevent the attacker from gaining a foothold in other institutions, INF shares the phishing IoCs with SI-CERT via MISP, through which these IoCs are further distributed to other EPES organizations. This way, CTI data regarding the attack is added to the MISP event, which is propagated through the MISP network via the MISP instance of SI-CERT.

7.2.3.1 Implemented malicious program

To simulate and validate the procedure of IoC exchange from INF SOC to SI-CERT and then further through other national CERTs to EPES SOCs within the European space, we implemented a malware dropper program *piloader.exe*. This program hides the malicious code from the security mechanisms and smuggles it into the computer OS environment. When we run *piloader.exe*, it creates the *piloader_test.txt* file. Windows Security immediately recognizes the latter as malicious code.

We implemented the malware dropper code in the C programming language. We compiled it in the MinGW-w64 runtime environment (x86_64-w64-mingw32-gcc) (<https://www.mingw-w64.org/>). The creation of the executable *piloader.exe* file is shown in Figure 88.


```

$ sha256sum piloader.exe
36dfdfceb3584da43f04592a242d3933093d6ef96e1c6ed9693d227ef3923089 *piloader.exe

lab@DESKTOP-1PP703A ~
$ ls -al
total 287
drwxr-xr-x 1 lab None           0 May 24 12:49 .
drwxrwxrwt 1 lab Administrators 0 May 21 15:11 ..
-rw----- 1 lab None          2230 May 22 14:56 .bash_history
-rwxr-xr-x 1 lab None          1494 May 21 14:56 .bash_profile
-rwxr-xr-x 1 lab None          5645 May 21 14:56 .bashrc
-rwxr-xr-x 1 lab None          1919 May 21 14:56 .inputrc
-rw----- 1 lab None           20 May 24 08:42 .lesshst
-rw-r--r-- 1 lab None           39 May 21 17:13 .minttyrc
-rwxr-xr-x 1 lab None          1236 May 21 14:56 .profile
-rw-r--r-- 1 lab None           438 May 22 14:05 piloader.c
-rwxr-xr-x 1 lab None        258823 May 24 12:49 piloader.exe

lab@DESKTOP-1PP703A ~
$ x86_64-w64-mingw32-gcc piloader.c -o piloader

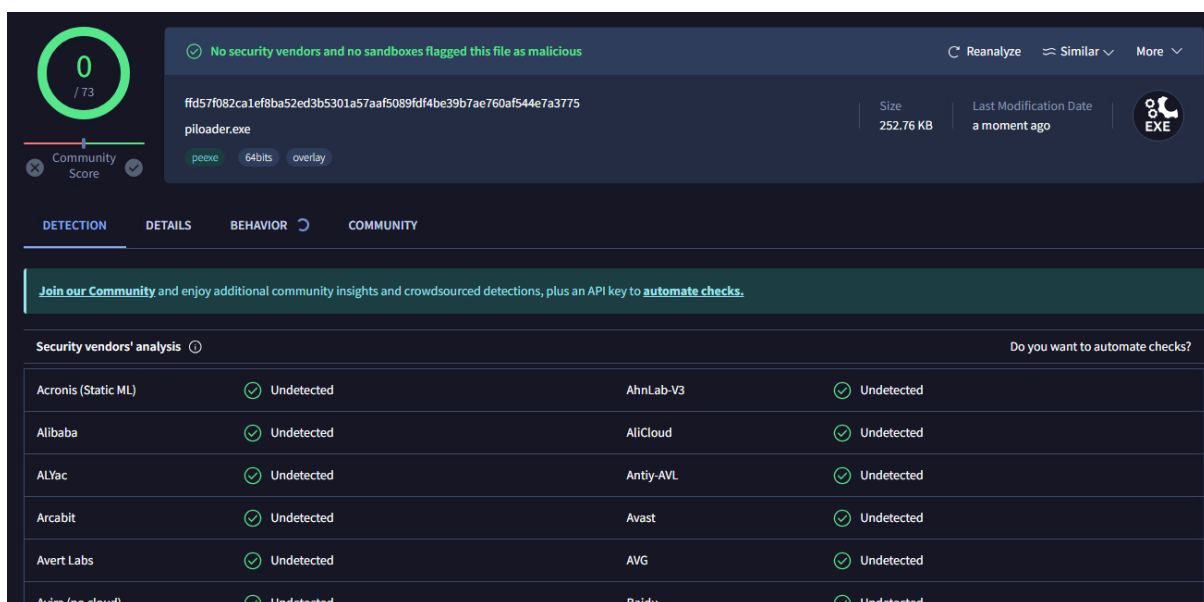
lab@DESKTOP-1PP703A ~
$ sha256sum piloader.exe
ffd57f082ca1ef8ba52ed3b5301a57aaf5089fdf4be39b7ae760af544e7a3775 *piloader.exe

```

Figure 88 – Compilation of the malware dropper program.

7.2.3.2 Scenario execution

A user downloaded the malware dropper executable *piloader.exe* from a malicious website due to a phishing attack. The malicious file was analyzed with VirusTotal (<https://www.virustotal.com/>). No security risk was detected and no warning was issued. This is indicated in Figure 89. Figure 90 shows the basic properties and hashes of the malware dropper executable.



The screenshot shows the VirusTotal interface for the file *piloader.exe*. The file is identified by the SHA-256 hash `ffd57f082ca1ef8ba52ed3b5301a57aaf5089fdf4be39b7ae760af544e7a3775. The file size is 252.76 KB and it was last modified "a moment ago". The file type is identified as EXE. The interface shows a green circle with a '0' indicating that no security vendors or sandboxes flagged this file as malicious. Below this, there is a table of security vendors' analysis results, all of which are "Undetected".`

| Security Vendor | Analysis Result |
|---------------------|-----------------|
| Acronis (Static ML) | Undetected |
| Alibaba | Undetected |
| ALYac | Undetected |
| Arcabit | Undetected |
| Avert Labs | Undetected |
| Avira (no cloud) | Undetected |
| AhnLab-V3 | Undetected |
| AliCloud | Undetected |
| Antiy-AVL | Undetected |
| Avast | Undetected |
| AVG | Undetected |
| Baidu | Undetected |

Figure 89 – Security analysis of the malware dropper executable with VirusTotal.

D6.8 Rules & Tools for Operators' Coordination and Reporting to CERTs in Case of Incidents V2

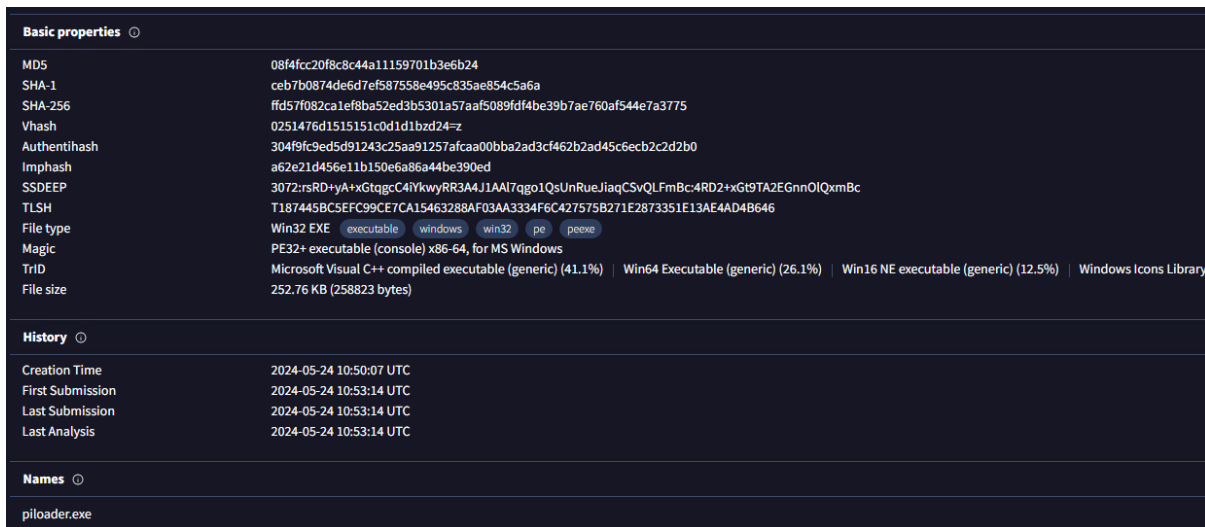


Figure 90 – Basic properties and hashes of the malware dropper executable.

The user then runs *piloader.exe* creating the *piloader_test.txt* file as depicted in Figure 91. As is presented in Figure 92, Windows Security instantly recognizes this file as malicious code. It subsequently blocks and deletes it.

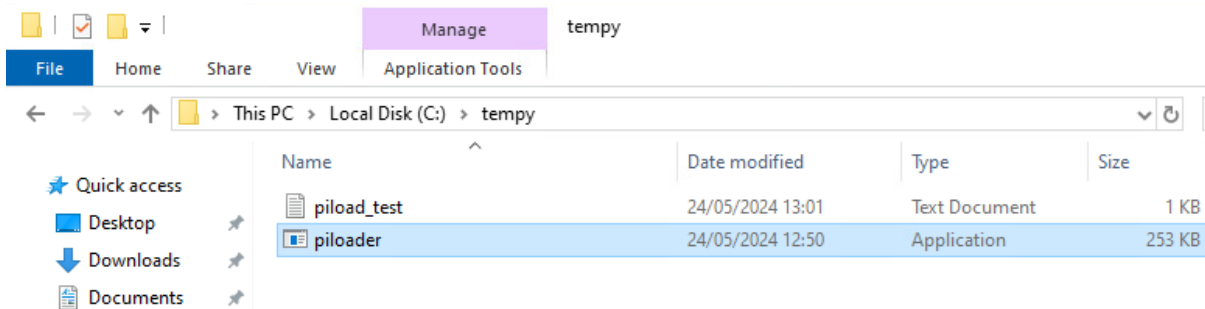


Figure 91 – Creation of a malicious file.



Figure 92 – The blocked malicious file generated by the malware dropper executable.

After INF SOC receives a notification about the malware, it publishes its IoCs as a new MISP event, which is, in turn, propagated to the SI-CERT's MISP instance. INF SOC sets all required attributes of this event, such as the file name, size in bytes, and SHA-1 and SHA-256 hashes. This is depicted in Figure 93 and Figure 94, respectively, where the first shows the general attributes, while the latter focuses on the SHA-256 hash.

| Date | Category | Type | Value | Tags | Galaxies | Comment | Correlate | Related Events |
|-------------|------------------|---------------|--|------|----------|---------|-------------------------------------|----------------|
| 2024-05-24* | Other | size-in-bytes | 258823 252.76 kB | | | | <input checked="" type="checkbox"/> | 🔍 |
| 2024-05-24* | Payload delivery | filename | piloader.exe | | | | <input checked="" type="checkbox"/> | 2125 🔍 |
| 2024-05-24* | Payload delivery | sha1 | ceb7b0874de6d7ef587558e495c835ae854c5a6a | | | | <input checked="" type="checkbox"/> | 🔍 |
| 2024-05-24* | Payload delivery | md5 | 08f4fcc20f8c8c44a11159701b3e6b24 | | | | <input checked="" type="checkbox"/> | 🔍 |

Figure 93 – A new MISP event published by the INF SOC.

| Date | Category | Type | Value | Tags | Galaxies | Comment |
|------------|------------------|--------|---|------|----------|---------|
| 2024-05-24 | Payload delivery | sha256 | ffd57f082ca1ef8ba52ed3b5301a57aaf5089fd4be39b7ae760af544e7a3775 | | | |

Figure 94 – IoC (SHA-256 hash) in the published MISP event.

In addition to the CTI exchange, the MISP event published by INF SOC also allows for the reporting to SI-CERT, because the incident is classified with a high threat level as depicted in Figure 95. The NOKI object is hence appended to the event as the means of standardized reporting. This can be seen in Figure 96.

The event created will be visible to the organisations having an account on this platform, but not synchronised to other MISP

Add Event

Date: 2024-05-24 | Distribution: Connected communities

Threat Level: High | Analysis: Ongoing

Event Info: Test dropper for project CyberSEAS

Extends Event: Event UUID or ID. Leave blank if not applicable.

Submit

Figure 95 – Definition of a new MISP event addressing the malware dropper.

| View Event History | | Make sure that the below Object reflects your expectation before submitting it. | | | | | | | |
|--------------------------|--|---|---------------|------|-------------------------------------|--------|---------|---------------------------------------|---------------|
| View Event History | | Name | noki | | | | | | |
| Edit Event | | Template version | 25 | | | | | | |
| Delete Event | | Meta-category | misc | | | | | | |
| Add Attribute | | Distribution | Inherit event | | | | | | |
| Add Object | | Comment | | | | | | | |
| Add Attachment | | First seen | 2024-05-24 | | | | | | |
| Add Event Report | | Last seen | 2024-05-24 | | | | | | |
| Populate from... | | | | | | | | | |
| Enrich Event | | Object name | Category | Type | Value | To IDS | Comment | URIID | Distribution |
| Merge attributes from... | | report-incident-category | Other | text | C4 | No | | e39da32-1a49-4ba3-9501-7333bac2b459 | Inherit event |
| Publish Event | | report-compromised-service | Other | text | Bistvena storitev ZinTV | No | | 087e926-1395-4787-99e9-9bc875ac6a01 | Inherit event |
| Publish (no email) | | report-crossborder-influence | Other | text | NE | No | | 1e7764a5-8271-4e98-9641-5555d4ef026d | Inherit event |
| Contact Reporter | | report-incident-source | Other | text | Spletno mesto | No | | 827d2c-16-9d5a-4485-95cc-38d05d0c7191 | Inherit event |
| Download as... | | report-incident-type | Other | text | Izsiljevalski virus | No | | 443bac07-cb65-4a79-be41-6b52aaea0813 | Inherit event |
| List Events | | report-voluntary | Other | text | Prvo poročilo o incidentu zavezanca | No | | b86e4579-8881-463c-a58e-633baef3792af | Inherit event |
| Add Event | | reporter-organization | Other | text | Informatika d.o.o. | No | | 39c2e56c-e792-4988-99de-b229c7be6600 | Inherit event |
| | | reporter-name | Other | text | VOC | No | | 103877ba-4734-4d2f-a23b-07369aaa4b3f | Inherit event |
| | | reporter-phone-number | Other | text | 027071158 | No | | 0d09ce65-129-40af-b7b6-e188d8703e57 | Inherit event |
| | | reporter-e-mail | Other | text | voc@informatika.si | No | | 39c98513-3281-4411-861b-8a187590096c | Inherit event |
| | | report-type | Other | text | Vmesno | No | | 7c454316-866c-4daa-9524-127c13653b25 | Inherit event |

Figure 96 – NOKI object for the standardized reporting of the malware dropper event.

7.3 Playbook sharing and reporting scenarios

In this section, we use the SAPPAN playbook management tool in addition to MISP to share and standardize incident response procedures and incorporate incident reporting into these procedures.

7.3.1 Motivation

SAPPAN's functionalities are essential for cybersecurity response procedures. They allow playbooks to be used by SOCs, CERTs/CIRTs, and national CERTs. This implies that SAPPAN playbooks and MISP are correlated in the following ways:

1. Playbooks are shared between different SOCs as they represent standardized incident response procedures that serve as common best practices and may be reused by SOCs for the same types of cyber incidents. MISP guarantees full security in playbook exchange, which is necessary because incident response actions may contain sensitive information. It also serves as a uniform repository for community members to provide and access playbooks. The JSON format is the enabler to store playbooks in MISP.
2. MISP is intended to share information on security events. Each type of security event usually has a (more or less) standard response. A playbook is therefore a standardized incident response procedure suited to a specific type of cyber-attack. It can be of significant value to append it as a JSON object to the published event in MISP as a recommendation for other SOCs on how to treat this type of cyber-attack.
3. Playbooks are, at least partially, executable. Their execution includes steps to exchange CTI information on the identified IoCs and report to CERTs as an integral part of incident response. SAPPAN playbooks should hence include some predefined steps that support MISP integration. Such a step may publish a new event to MISP. It may also append the NOKI object to this event.

The project requirements analysis revealed a significant advantage in associating playbooks with MISP incident events. This association ensures that when a MISP event is shared with other organizations, the corresponding playbook is also disseminated. To verify this scenario effectively, it is important to consider the inclusion of playbook execution components.

7.3.2 NOKI Responder

As an example of tasks that can be automated, we developed a Cortex Responder that can automatically generate a NOKI (Nacionalni Načrt Odzivanja Na Kibernetske Incidente) Report for cyber security incidents as introduced by the Slovenian government. It can fill the reports fields either directly from a Hive Case's fields (optionally mapping a case field to the corresponding report entry) or its tags, when invoked from the Hive. Even more powerfully it can be evoked from our tool as part of an automated playbook which allows filling a report with regards to the actions taken, through our syntax including Analyzer/Responder results, and attaching information about the used playbook.

Once the report is created and confirmed, it gets published to a connected MISP instance for further review and processing by the team. Figure 97 shows a command in the playbook management tool that invokes the NOKI Cortex Responder.



The screenshot shows a web interface for managing playbooks. At the top, there are navigation links for SASP, JSON, MISP, Kafka, TheHive, and View on Wiki. The user is logged in as fra-admin@cyberseas.eu. Below the navigation, the title of the command is "Command--57708385-a00e-43ff-a8ef-fe9f52da9c0b". The command is of type "openc2-json". The command content is a JSON object:

```

{
  "action": "start",
  "target": {
    "uri": "NOKI_Reporter_1_0"
  },
  "args": {
    "data": {
      "noki_report": {
        "incident-start-timestamp": "hive-case-field:createdAt",
        "report-voluntary": "Prostovoljna prigrasitev incidenta",
        "reporter-e-mail": [
          "itsame@mario.nintendo"
        ],
        "reporter-name": [
          "Mario"
        ],
        "reporter-organization": "Fraunhofer FIT",
        "reporter-phone-number": [
          "123456789"
        ]
      },
      "report-compromised-service-description": "hive-case-field:customFields.serviceName",
      "report-initiated-countermeasures": "SASP: Automated Actions Playbook"
    },
    "dataType": "SASP Playbook Data"
  }
}

```

Figure 97 – A command that invokes the NOKI Cortex Responder.

7.3.3 Playbook exchange and reuse

This approach ensures that when we share a cybersecurity event with other organizations via MISP, the corresponding playbook is also disseminated. This playbook should be sanitized before sharing and modified by the receiving organization to be adapted to its needs. Figure 98 illustrates the conceptual strategy for managing and disseminating playbooks across organizations. The SAPPAN tool is employed for the creation, editing, and management of

playbooks, to come up with complete response and recovery workflows. Before sharing, playbooks undergo a generalization and sanitization process through the SAPPAN tool's sanitizer component, which operates in accordance with the Traffic Light Protocol (TLP) tagged to each resource within the playbook. Once sanitized, the playbook can be shared through MISP by attaching it to a corresponding MISP event. Upon reception, the playbook can be retrieved, modified within the SAPPAN tool by the receiving organization, and stored in various versions using the tool's versioning system. This scenario must consider the inclusion of the component for playbook execution and step monitoring.

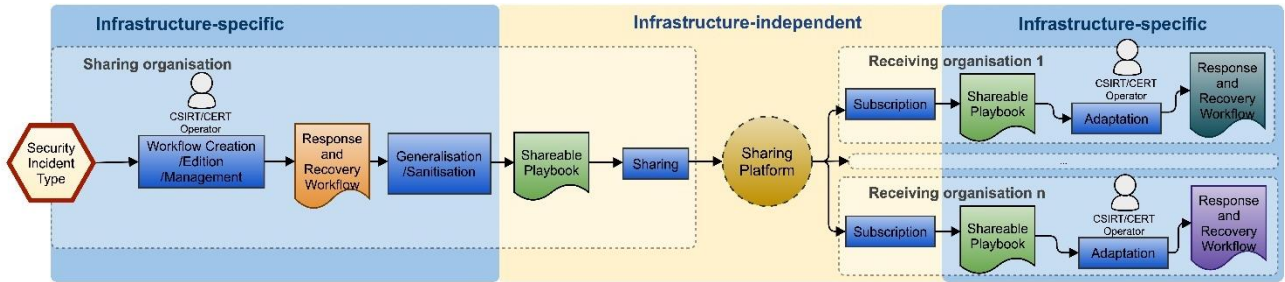


Figure 98 – Conceptual approach for cyber security playbook management and sharing.

In the implemented and verified scenario, INF shares a SAPPAN malware response playbook with SI-CERT via SAPPAN integration with MISP as shown in Figure 99. At SI-CERT, the playbook is reviewed, generalized, and sanitized. This is presented in Figure 100. The malware playbook is then further shared by SI-CERT in the community with relevant stakeholders as depicted in Figure 101. Finally, Figure 102 shows that the new generalized playbook can be obtained via MISP by any stakeholder in the community.

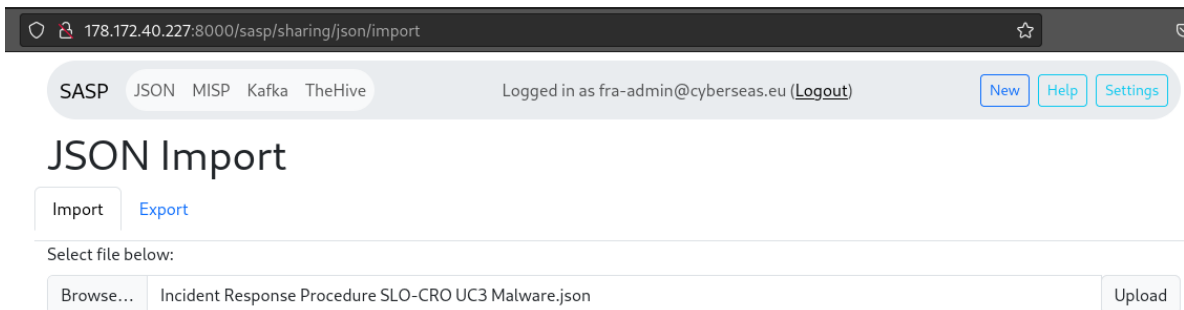


Figure 99 – Sharing the initial internal INF SOC playbook with the national CERT.

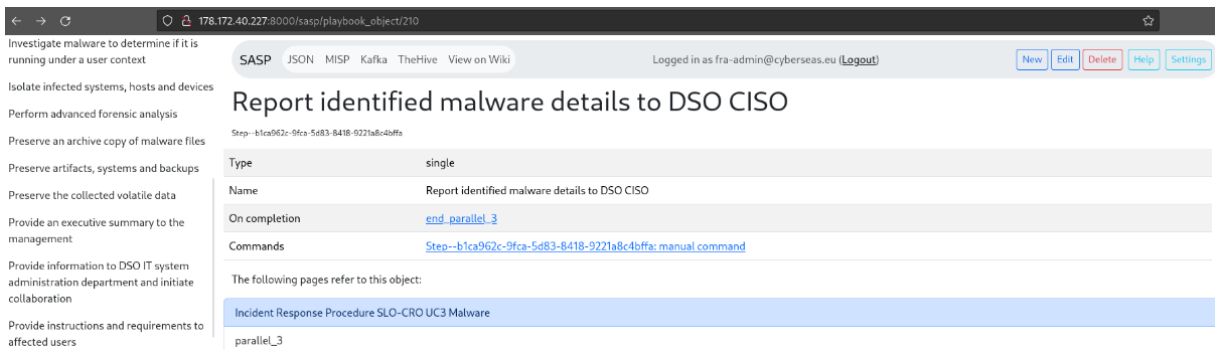


Figure 100 – Modification and generalization of the playbook by the national CERT.



Figure 101 – Resharing the generalized and sanitized playbook with the EPES community.

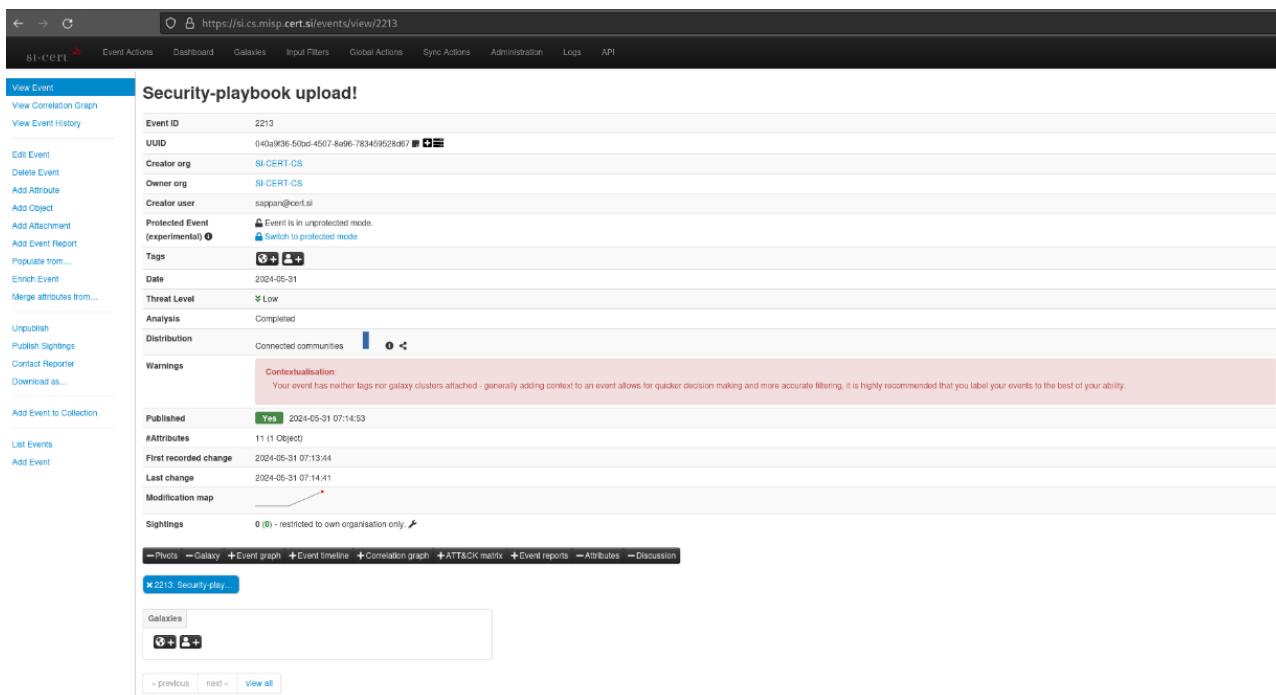


Figure 102 – Generalized playbook in the MISP repository.

7.3.4 Enrichment of shared IoC data with standardized playbooks

Through this protocol, a playbook JSON object or reference is appended to the published MISP event to provide community stakeholders (EPES SOCs) with a standardized IR procedure to address the identified type or case of cyber-attack.

In the implemented scenario, INF shares phishing IoCs including a reference to the related playbook via MISP for better understanding and resolution of the incident. The created MISP event is enriched with the information on the relevant playbook enabling a better handling of the incident by all event's receivers. The event containing IoCs and the playbook is shared with all the interested community members via SI-CERT's MISP instance. Figure 103 presents how the UUID of a phishing IoC references a common playbook for the standardized phishing incident response.

D6.8 Rules & Tools for Operators' Coordination and Reporting to CERTs in Case of Incidents V2

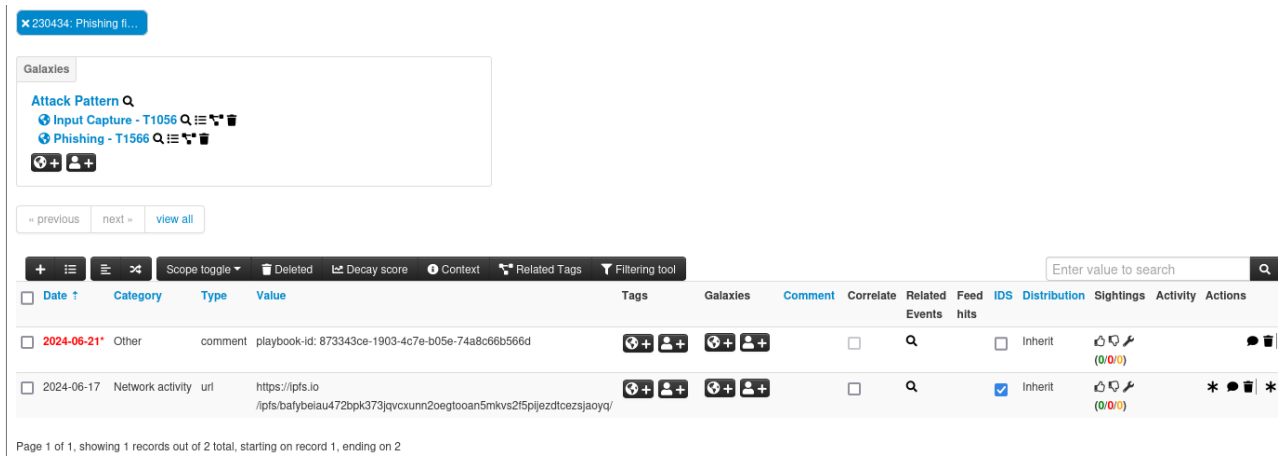


Figure 103 – UUID of a phishing IoC referencing a playbook for the standardized phishing IR.

An extension of this protocol is to include the NOKI object in the MISP event in addition to the playbook reference. In this way, we can provide all relevant information for the coordination of operators and CERTs in a single MISP event:

- IoCs to identify the incident;
- the playbook to standardize incident response and provide commonly accepted instructions to operators;
- the NOKI object to report to the CERT.

In the implemented scenario, phishing attack data detected by INF is shared via MISP to SI-CERT as demonstrated in Figure 104 and Figure 105. The NOKI object is added to the MISP event due to the severity of the incident, including the mandatory reporting information required by legislation as presented in Figure 106. The sharing level is lowered for the NOKI object to prevent further unwanted redistribution of information included in it.

| Save | Name :: type | Description | Category | Value |
|--------------------------|--------------------------------------|--|----------|------------------------|
| <input type="checkbox"/> | Reference-number text | Referenčna številka incidenta (Določil odzivni center) | Other | |
| <input type="checkbox"/> | Report-incident-category text | Stopnja incidenta | Other | -- Select an option -- |
| <input type="checkbox"/> | Report-incident-source-other text | Izvor incidenta (drugo) | Other | |
| <input type="checkbox"/> | Report-compromised-service text | Ogrožena storitev zavezanca | Other | -- Select an option -- |

Figure 104 – Adding of the NOKI object.

View Event History

- Edit Event
- Delete Event
- Add Attribute
- Add Object
- Add Attachment
- Add Event Report
- Populate from...
- Enrich Event
- Merge attributes from...
- Publish Event
- Publish (no email)
- Contact Reporter
- Download as...
- List Events
- Add Event

Make sure that the below Object reflects your expectation before submitting it.

| | | | | | | | |
|------------------|---------------|--|--|--|--|--|--|
| Name | noki | | | | | | |
| Template version | 25 | | | | | | |
| Meta-category | misc | | | | | | |
| Distribution | Inherit event | | | | | | |
| Comment | | | | | | | |
| First seen | 2024-05-24 | | | | | | |
| Last seen | 2024-05-24 | | | | | | |

| Object name | Category | Type | Value | To IDS | Comment | UUID | Distribution |
|------------------------------|----------|------|-------------------------------------|--------|---------|--------------------------------------|---------------|
| report-incident-category | Other | text | C4 | No | | e39da32-1a49-4ba3-9501-733bac9b459 | Inherit event |
| report-compromised-service | Other | text | Bishevna storitev ZinTV | No | | 0874926-1395-4787-99e9-9bc875ac6a01 | Inherit event |
| report-crossborder-influence | Other | text | NE | No | | 1e7764a5-8271-4e98-9641-5555d4ef026d | Inherit event |
| report-incident-source | Other | text | Spletno mesto | No | | 827d2-16-9d5a-4485-95cc-38d05d6c7191 | Inherit event |
| report-incident-type | Other | text | Izjavevski virus | No | | 443bdc7-cb5-4a79-b641-6b52aaea0813 | Inherit event |
| report-voluntary | Other | text | Prvo poročilo o incidentu zavezanca | No | | b86e4575-881-463c-a58e-b33ba8792af | Inherit event |
| reporter-organization | Other | text | Informatika d.o.o. | No | | 39c2e56c-4792-4989-99de-b229c7be600 | Inherit event |
| reporter-name | Other | text | VOC | No | | 103877ba-4734-4d2f-a23b-07369aaa4b3f | Inherit event |
| reporter-phone-number | Other | text | 027071158 | No | | 0d09ce65-129-40af-b7b6-e188d0703e57 | Inherit event |
| reporter-e-mail | Other | text | voc@informatika.si | No | | 39c9513-3281-4411-851b-8a18759006c | Inherit event |
| report-type | Other | text | Vmesno | No | | 7e454316-866c-46aa-9524-127c13653b25 | Inherit event |

Figure 105 – Added NOKI object (INF SOC).

Test dropper for project CyberSEAS

| Event ID | Priority | Category | Type | Source | Target | UUID | Comment | First Seen | Last Seen |
|----------|----------|----------|------|-------------|---------------|--------------------------------------|---------|------------|------------|
| 1234567 | High | Malware | File | 192.168.1.1 | 192.168.1.100 | e39da32-1a49-4ba3-9501-733bac9b459 | | 2024-05-24 | 2024-05-24 |
| 1234568 | High | Malware | File | 192.168.1.1 | 192.168.1.100 | 0874926-1395-4787-99e9-9bc875ac6a01 | | 2024-05-24 | 2024-05-24 |
| 1234569 | High | Malware | File | 192.168.1.1 | 192.168.1.100 | 1e7764a5-8271-4e98-9641-5555d4ef026d | | 2024-05-24 | 2024-05-24 |
| 1234570 | High | Malware | File | 192.168.1.1 | 192.168.1.100 | 827d2-16-9d5a-4485-95cc-38d05d6c7191 | | 2024-05-24 | 2024-05-24 |
| 1234571 | High | Malware | File | 192.168.1.1 | 192.168.1.100 | 443bdc7-cb5-4a79-b641-6b52aaea0813 | | 2024-05-24 | 2024-05-24 |
| 1234572 | High | Malware | File | 192.168.1.1 | 192.168.1.100 | b86e4575-881-463c-a58e-b33ba8792af | | 2024-05-24 | 2024-05-24 |
| 1234573 | High | Malware | File | 192.168.1.1 | 192.168.1.100 | 39c2e56c-4792-4989-99de-b229c7be600 | | 2024-05-24 | 2024-05-24 |
| 1234574 | High | Malware | File | 192.168.1.1 | 192.168.1.100 | 103877ba-4734-4d2f-a23b-07369aaa4b3f | | 2024-05-24 | 2024-05-24 |
| 1234575 | High | Malware | File | 192.168.1.1 | 192.168.1.100 | 0d09ce65-129-40af-b7b6-e188d0703e57 | | 2024-05-24 | 2024-05-24 |
| 1234576 | High | Malware | File | 192.168.1.1 | 192.168.1.100 | 39c9513-3281-4411-851b-8a18759006c | | 2024-05-24 | 2024-05-24 |
| 1234577 | High | Malware | File | 192.168.1.1 | 192.168.1.100 | 7e454316-866c-46aa-9524-127c13653b25 | | 2024-05-24 | 2024-05-24 |

Figure 106 – Received NOKI object (SI-CERT).

7.3.5 Automation of reporting to CERTs via playbooks

A playbook can include steps to automate reporting to CERTs as an integral part of incident response. Such a step may publish a new event to MISP and append the NOKI object to this event. In addition, it is beneficial to automatically or semi-automatically execute a playbook once a cyber incident is detected. This frees up human resources, increases the efficiency of incident response, and reduces the probability of errors. This represents a similar approach to SOAR (Security Orchestration, Automation, and Response). However, we do not aim to rely on proprietary technology, instead focusing on open modeling and automation standards and notations, such as BPMN and CACAO.

The playbook execution scenario is presented in Figure 107. It automates INF's malware IR and reporting procedure. A Windows workstation in INF's virtual test network is compromised

by malware, which is detected after causing damage to the workstation. The malware IR playbook is invoked through the gate monitor in the CyberRange environment. The playbook runs in TheHive/Cortex software following the steps defined and implemented in the CACAO notation. Some steps are executed automatically, while others are performed manually, such that SAPPAN provides security analysts with information about the current status of playbook execution. Several other tools are also integrated and used:

- SIEM is integrated to identify and investigate the incident;
- MISP is invoked to share IoCs about the incident and report to CERT;
- DSS allows us to assess the severity of the incident to apply appropriate reporting rules.

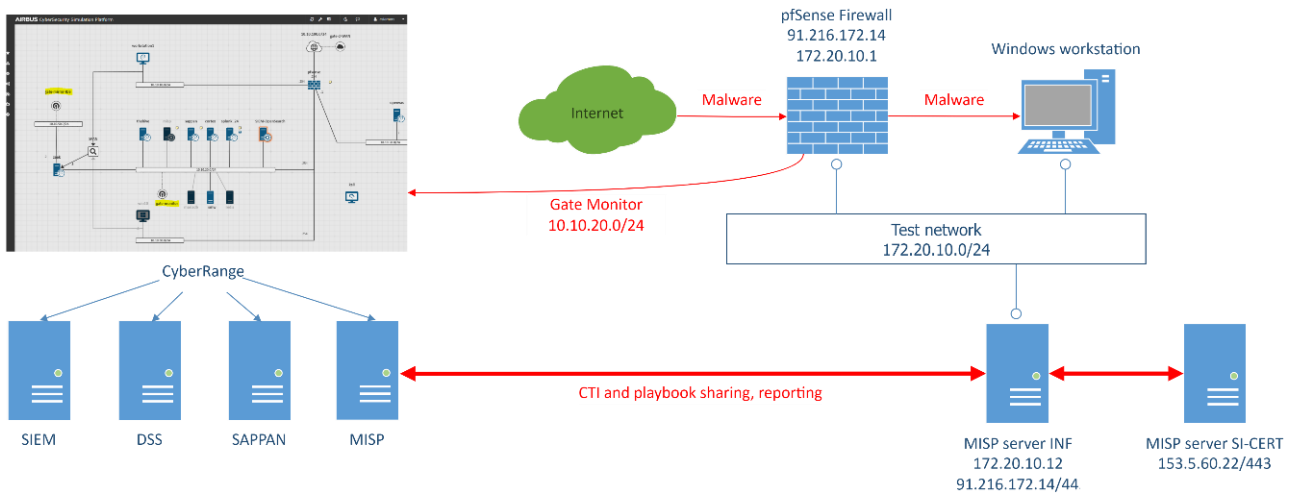


Figure 107 – Playbook execution scenario.

7.4 Summary of implemented rules and tools

Table 36 summarizes the proposed and implemented procedures, rules, and tools intended to enhance and standardize the coordination of EPES operators and reporting of incidents to CERTs.

Table 36 – Summary of proposed and implemented procedures, rules, and tools.

| Standardized procedure | Key steps, rules, and benefits | Key tools |
|-------------------------------------|---|---|
| CTI sharing for the EPES operator | The operator receives CTI information from the community to proactively block known cyber-attacks, CERT acts as an intermediary and the single point of contact in the community | MISP, security tools (such as NGFW) |
| CTI exchange from the EPES operator | The operator shares CTI information about the detected incident with the community to enhance the resilience of the EPES ecosystem, CERT acts as an intermediary and the single point of contact in the community | MISP, security tools (such as SIEM, Windows Defender, etc.) |

| | | |
|---|---|--|
| Standardized NOKI reporting to the CERT | The operator reports an incident through a standardized semi-automatic procedure by sending a standard NOKI object to the CERT | MISP, DSS, security tools (such as SIEM, Windows Defender, etc.) |
| Enrichment of IoCs with playbooks | The operator appends the reference to a standardized playbook as an addition to IoCs of the detected incident in the created MISP event to provide the community with a uniform procedure to respond efficiently to this type of cyber-attack and report to CERT in a standardized manner | MISP, SAPPAN |
| Management and sharing of playbooks | A repository of standard playbooks is available for the community of operators and CERTs increasing awareness and knowledge about incident response; operators and CERTs can share playbooks and enhance them to meet individual and legislative requirements | MISP, SAPPAN |
| Playbook automation and execution | A playbook is automatically executed to respond to the detected incident increasing the efficiency of response, recovery, reporting, and coordination | MISP, SAPPAN, DSS, TheHive, Cortex, security tools (such as SIEM) |
| Combined procedure | A standardized procedure involving the exchange of IoCs about the detected incident together with the NOKI object for reporting and the reference to an appropriate incident response playbook | MISP, SAPPAN, DSS, security tools (such as SIEM, Windows Defender, etc.) |

8 Conclusions (updated)

D6.8 delivered several outcomes. It provided and utilized the methodology to define the incident response strategy, incident response procedures, cooperation and communication strategy, information sharing mechanisms, formats of reports for CERTs, and report exchange tools. Based on the methodology, each EPES stakeholder can map assets and cybersecurity events/attacks to incident response procedures consisting of containment, eradication, recovery, reporting, and coordination activities and rules. MCDM methods and collaborative techniques allow stakeholders to collectively assess the impacts and effects of cybersecurity events to select appropriate procedures by determining the scope, severity, and extent of the damage caused by the incident. A part of the methodology is the standard notation and the common vocabulary to model incident response procedures as process diagrams. Top-down and bottom-up strategies are available to differentiate responses for specific cyber-attack types. In line with the methodology, national pilots defined incident response procedures separately to consider the specifics of legislation in different countries.

Secondly, D6.8 defined incident response procedures and rules for operators' coordination and reporting to CERTs. The CyberSEAS pilot partners (ITA, SLO&CRO, ROM, FIN, and EST) provided the specifications thoroughly and extensively on the national level based on their attack scenarios, legislation, and specific rules. The procedures consider the underlying regulations; required coordination with national CERTs; data structures, formats, and tools for reports; the communication strategy; and information-sharing mechanisms. All pilots compiled general rules for reporting and coordination with CERTs. Additionally, several pilots were able to define detailed incident response procedures based on pilot attack scenarios, i.e., specific assets and types of incidents.

We elaborated further on the national procedures, rules, and tools specified by the pilots. We compared and analyzed practices in different European countries to draw parallels and establish unified protocols, rules, tools, and recommendations for coordination between stakeholders, incident response, and reporting to national CERTs in the common European space. We aligned the mechanisms and practices with the most recent legislation coming into force and required to be followed by the providers of critical infrastructure and essential services. In particular, we analyzed the adherence to the NIS 2 Directive, CER Directive, and the Network Code on Cybersecurity.

D6.8 provided the list of tools to be used to create reports and collect information for CERTs. We linked the reporting tools with pilots. We prepared a compact tools overview which can serve as a user manual (a tools mapping document) since information on how to use the tools adds value to reading and implementing cybersecurity practices and interaction with CERTs from the perspective of EPES operators. This overview supports the scenario in which an operator from another country would want to test the tools and set them up.

D6.8 also delivered a set of tools for operators' coordination and reporting to CERTs in case cyber incidents occur. We implemented the solution for the malware and phishing incident response procedures. We utilized several tools and technologies, which include SAPPAN for playbook modeling and management, TheHive and Cortex for playbook execution, MISP for CTI exchange and fundamental collaboration with CERTs, and the decision support system for incident impact assessment. The solution facilitates L1, L2, and L3 levels of SOC operations. It addresses appropriate tools to enable reporting, decision-making, analysis of incidents,

and cooperation among different stakeholders. A part of this deliverable is the toolset design specification. It defines functional and non-functional requirements, describes the high-level toolset architecture, and outlines the modules of the toolset based on TheHive, Cortex, and SAPPAN technologies.

In addition to the playbook management, sharing, and execution modules of SAPPAN, we implemented the decision support system. It demonstrates the decision-making process and can be beneficially used in practice. It is shared and reused between tasks T4.4 and T6.4. However, it is properly and carefully targeted to the specifics of T6.4.

D6.8 sets the methodological foundations underlying the design and implementation of the toolset targeting the automation of incident response procedures. This theory also gives the legislative framework for a coherent specification of national response procedures and rules. We briefly reviewed and analyzed the most relevant and widely accepted common incident response frameworks, CTI exchange standards, reporting technologies, business process modeling notations and tools, MCDM methods, and group collaboration technologies and techniques.

By analyzing the outcomes of D6.8, it can be concluded that the goals of the T6.4 task were fulfilled. D6.8 covers and facilitates all rules and incident response procedures provided for different countries by CyberSEAS pilots. It defines and implements a set of unified rules, tools, protocols, and procedures for the common European EPES system. They are coherent with the characteristics of incident response procedures for specific types of cyber-attacks and legislative requirements, both nationally and EU-wide.

An important activity in the second phase of T6.4 was the verification of the toolset and the proposed rules and procedures for coordination and reporting. We focused primarily on MSP and SAPPAN tools. We addressed key scenarios for CTI exchange and collaboration within EPES communities, standardized reporting to CERTs using the NOKI object, the enrichment of IoCs about specific types of cyber-attacks with references to the consolidated playbooks, and playbook management, sharing, and automation. The SLO&CRO pilot first verified the solutions internally and then thoroughly validated them in the scope of the D7.4 deliverable. A testing and validation plan was prepared before the verification and validation phase.

9 References

- [1] W. Chai, K. Beaver and L. Rosencrance, "Incident response," TechTarget, 2022.
- [2] R. Brown and S. J. Roberts, Intelligence-driven incident response: Outwitting the adversary, Sebastopol: O'Reilly Media, 2017.
- [3] European Parliament, "Fighting cybercrime: new EU cybersecurity laws explained," European Parliament, 16 February 2023. [Online]. Available: <https://www.europarl.europa.eu/news/en/headlines/security/20221103STO48002/fighting-cybercrime-new-eu-cybersecurity-laws-explained>.
- [4] European Parliament, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)," 14 December 2022. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2022/2555>.
- [5] ENISA, "NIS Directive," ENISA - European Union Agency for Cybersecurity, 2023. [Online]. Available: <https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new>.
- [6] P. Cichonski, T. Millar, T. Grance and K. Scarfone, Computer Security Incident Handling Guide: NIST Special Publication 800-61 Revision 2, National Institute of Standards and Technology, 2012.
- [7] E. Salfati and M. Pease, NISTIR 8428: Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT), National Institute of Standards and Technology, 2022.
- [8] P. Kral, "Incident Handler's Handbook," SANS, 2012.
- [9] ISO/IEC, "ISO/IEC 27035-1:2023: Information technology — Information security incident management — Part 1: Principles and process," ISO/IEC, 2023.
- [10] MITRE, "MITRE ATT&CK," The MITRE Corporation, 2022.
- [11] R. Daszczyszak, D. Ellis, S. Luke and S. Whitley, "TTP-Based Hunting," The MITRE Corporation, 2020.
- [12] J. Creasey and I. Glover, "Cyber Security Incident Response Guide," CREST, 2013.
- [13] J. Creasey and I. Glover, "Cyber Security Incident Response Supplier Selection Guide," CREST, 2013.
- [14] ISACA, "COBIT 5 DSS02 Manage Service Requests and Incidents Audit Program," ISACA, 2019.

- [15] OASIS, "STIX Version 2.1," OASIS, 2021.
- [16] OASIS, "TAXII Version 2.1," OASIS, 2021.
- [17] C. Vandeplas, "Galaxies in MISP," 2023.
- [18] C. Vandeplas, "MISP Taxonomies," 2023.
- [19] StrangeBee, "TheHive Indicators & KPIs," StrangeBee, 2022.
- [20] CISA, "Cyber Threat Indicator and Defensive Measure Submission System," Cybersecurity & Infrastructure Security Agency, 2023.
- [21] SecurityScorecard, "The CISO's Guide to Reporting Cybersecurity to the Board," SecurityScorecard, 2020.
- [22] Atlassian, "Jira Software," Atlassian, [Online]. Available: <https://www.atlassian.com/software/jira>.
- [23] MISP project, "MISP - Open source threat intelligence and sharing platform," 2023. [Online]. Available: <https://www.misp-project.org/>.
- [24] Wikipedia, "JSON," 2023.
- [25] Wikipedia, "Webhook," 2023.
- [26] ASF, "Apache Kafka," Apache Software Foundation, 2023. [Online]. Available: <https://kafka.apache.org/>.
- [27] N. Bouchard, "What Is Reporting? A Definition, Common Tools, and More," Unito, 2022.
- [28] Microsoft, "Microsoft Power BI," Microsoft, 2023. [Online]. Available: <https://powerbi.microsoft.com/en-us/>.
- [29] SAP, "SAP BusinessObjects Business Intelligence suite," SAP, 2023. [Online]. Available: <https://www.sap.com/products/technology-platform/bi-platform.html>.
- [30] R. L. Keeney and H. Raiffa, *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*, New York: Cambridge University Press, 1993.
- [31] A. Bregar, "Decision support on the basis of utility models with discordance-related preferential information: investigation of risk aversion properties," *Journal of Decision Systems*, vol. 27, no. S1, pp. 236-247, 2018.
- [32] K. P. Yoon and C.-L. Hwang, *Multiple Attribute Decision Making*, Sage Publications, 1995.

- [33] R. R. Yager, "On ordered weighted averaging aggregation operators in multicriteria decision making," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 18, no. 1, pp. 183-190, 1988.
- [34] Wikipedia, "Common Vulnerability Scoring System," 2023.
- [35] D. Maldenic, N. Lavrac, M. Bohanec and S. Moyle, *Data Mining and Decision Support: Integration and Collaboration*, Springer Science & Business Media, 2003, p. 275.
- [36] T. Arh and B. Jerman Blazic, "Application of Multi-Attribute Decision Making Approach to Learning Management Systems Evaluation," 2007.
- [37] M. Bohanec, "DEXi: A Program for Multi-Attribute Decision Making, Version 5.05," 30 January 2023. [Online]. Available: <https://kt.ijs.si/MarkoBohanec/dexi.html>.
- [38] S. Chakhar and I. Saad, "Incorporating stakeholders' knowledge in group decision-making," *Journal of Decision Systems*, vol. 23, no. 1, pp. 113-126, 2014.
- [39] L. C. Dias and J. N. Climaco, "ELECTRE TRI for groups with imprecise information on parameter values," *Group Decision and Negotiation*, vol. 9, pp. 355-377, 2000.
- [40] A. Bregar, "Application of a hybrid Delphi and aggregation-disaggregation procedure for group decision-making," *EURO Journal on Decision Processes*, vol. 7, no. 1-2, pp. 3-32, 2019.
- [41] N. F. Matsatsinis, E. Grigoroudis and A. P. Samaras, "Aggregation and disaggregation of preferences for collective decision-making," *Group Decision and Negotiation*, vol. 14, no. 3, pp. 217-232, 2005.
- [42] A. Bregar, "Towards a framework for the measurement and reduction of user-perceivable complexity in group decision-making methods," *International Journal of Decision Support System Technology*, vol. 6, no. 2, pp. 21-45, 2014.
- [43] E. Herrera-Viedma, F. Herrera and F. Chiclana, "A consensus model for multiperson decision making with different preference structures," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 32, no. 3, pp. 394-402, 2002.
- [44] A. Bregar, J. Gyorkos and M. B. Juric, "Interactive aggregation/disaggregation dichotomic sorting procedure for group decision analysis based on the threshold model," *Informatica*, vol. 19, no. 2, pp. 161-190, 2008.
- [45] H. A. Linstone and M. Turoff, *The Delphi method: techniques and applications*, Newark: New Jersey Institute of Technology, 2002.
- [46] M. I. Yousuf, "Using experts' opinions through Delphi technique," *Practical Assessment, Research, and Evaluation*, vol. 12, no. 4, pp. 1-8, 2007.

- [47] D. Beiderbeck, N. Frevel, H. A. von der Gracht, S. L. Schmidt and V. M. Schweitzer, "Preparing, conducting, and analyzing Delphi surveys: Cross-disciplinary practices, new directions, and advancements," *MethodsX*, vol. 8, 2021.
- [48] Wikipedia, "Computer-mediated communication," [Online]. Available: https://en.wikipedia.org/wiki/Computer-mediated_communication.
- [49] TheHive Project, "TheHive MISP connector," 2019.
- [50] C. Vandeplass, "MISP User Guide: Attribute Categories vs. Types," MISP Threat Sharing, 2023.
- [51] R. Knott, "Synchronous vs. Asynchronous Communication: How to Use Both to Dominate Remote Work," TechSmith, [Online]. Available: <https://www.techsmith.com/blog/synchronous-vs-asynchronous-communication/>.
- [52] OMG, "Business Process Model and Notation (BPMN), Version 2.0," Object Management Group, Inc. (OMG), 2011.
- [53] Jordan, B.; Thomson, A., "CACAO Security Playbooks Version 2.0: OASIS Committee Specification Draft 01," OASIS, 2023.
- [54] "SAPPAN - Sharing and Automation for Privacy Preserving Attack Neutralization, H2020 Project," 2023.
- [55] "SAPPAN - Sharing and Automation for Privacy Preserving Attack Neutralization, H2020 Project," 2022.
- [56] NESCOR, "Analysis of Selected Electric Sector High Risk Failure Scenarios," National Electric Sector Cybersecurity Organization Resource (NESCOR), 2013.
- [57] "Information Security Act: Official Gazette of the Republic of Slovenia, No. 30/18 of 26 April 2018," Republic of Slovenia, 2018.
- [58] IBM, "IBM Security QRadar SIEM," IBM, [Online]. Available: <https://www.ibm.com/qradar>.
- [59] OWASP, "OWASP Foundation, the Open Source Foundation for Application Security," OWASP Foundation, [Online]. Available: <https://owasp.org/#>.
- [60] Government Information Security Office of Republic of Slovenia, "National Cybersecurity Incident Response Plan," Government Information Security Office of Republic of Slovenia, 2021.
- [61] SI-CERT, "Incident reporting," SI-CERT, [Online]. Available: <https://www.cert.si/en/incident-reporting/>.
- [62] "Critical Infrastructure Act: Official Gazette of the Republic of Slovenia, No. 75/17 of 22 December 2017," Republic of Slovenia, 2017.

- [63] "Rules on security documentation and security measures of providers of essential services: Official Gazette of the Republic of Slovenia, no. 32/19 of 13 May 2019," Republic of Slovenia, 2019.
- [64] "Regulation on the determination of essential services and a more detailed methodology for determining providers of essential services: Official Gazette of the Republic of Slovenia, No. 39/19," Republic of Slovenia, 2019.
- [65] "Ransomware vs. phishing vs. malware (what's the difference)," Avertium, 1 October 2020. [Online]. Available: <https://www.avertium.com/blog/ransomware-phishing-malware-difference>. [Accessed 10 February 2022].
- [66] TRAFICOM, "Cyber security and the responsibilities of boards," Finnish Transport and Communications Agency TRAFICOM, National Cyber Security Centre, 4 February 2020. [Online]. Available: <https://www.kyberturvallisuuskeskus.fi/en/publications/cyber-security-and-responsibilities-boards>.
- [67] TRAFICOM, "Instructions – Data breach," Finnish Transport and Communications Agency TRAFICOM, National Cyber Security Centre, 2022.
- [68] TRAFICOM, "HAVARO FAQ," Finnish Transport and Communications Agency TRAFICOM, 3 January 2022. [Online]. Available: <https://havaro.fi/en/faq>.
- [69] TRAFICOM, "Information exchange practices for cooperation groups," Finnish Transport and Communications Agency TRAFICOM, National Cyber Security Centre, 26 August 2022. [Online]. Available: <https://www.kyberturvallisuuskeskus.fi/en/information-exchange-practices-cooperation-groups>.
- [70] Republic of Estonia, "Cybersecurity Act," 9 May 2018. [Online]. Available: <https://www.riigiteataja.ee/en/eli/523052018003/consolide>.
- [71] European Parliament and the Council of the European Union, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," European Parliament and the Council of the European Union, 2016.
- [72] NIST, "Cybersecurity Framework V1.1," National Institute of Standards and Technology, 2018.
- [73] ENISA, "Incident Reporting," European Union Agency for Cybersecurity, 2023. [Online]. Available: <https://www.enisa.europa.eu/topics/incident-reporting>.
- [74] The European Parliament and the Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation - GDPR)," 27 April 2016. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04>.

- [75] The European Parliament and the Council of the European Union, "Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code," 11 December 2018. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2018/1972/oj>.
- [76] European Parliament, "Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive)," 14 December 2022. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>.
- [77] ENTSO-E, "Network Code for cybersecurity aspects of cross-border electricity flows," 14 January 2022. [Online]. Available: https://www.entsoe.eu/network_codes/nccs/.
- [78] MISP Project, "MISP Taxonomies / PAP," MISP Project, 2019.
- [79] Airbus CyberSecurity et al., "SeCollA - Secure Collaborative Intelligent Industrial Assets (H2020 Project)," Airbus CyberSecurity et al., 2023.
- [80] TheHive Project, "Cortex-Analyzers," TheHive Project, 2023.
- [81] TheHive Project, "Cortex-Analyzers / responders," TheHive Project, 2022.
- [82] M. A. Gurabi, A. Mandal, J. Popanda, R. Rapp and S. Decker, "SASP: a Semantic web-based Approach for management of Sharable cybersecurity Playbooks," in *The 17th International Conference on Availability, Reliability and Security (ARES 2022)*, Vienna, 2022.
- [83] Play, "Play Framework Documentation: The Application Secret," 2021.
- [84] C. Vandeplas, "MISP Glossary," 2023.
- [85] L. Nitz, M. Zadnik, M. A. Gurabi, M. Obrecht and A. Mandal, "From Collaboration to Automation: A Proof of Concept for Improved Incident Response," *ERCIM News 2022*, no. 129, 2022.
- [86] X. Mertens, "Simple Blocklisting with MISP & pfSense," SANS Technology Institute, 23 July 2023. [Online]. Available: <https://isc.sans.edu/diary/Simple+Blocklisting+with+MISP+pfSense/26380>.
- [87] Netgate, "Change pfSense URL table update frequency," [Online]. Available: <https://forum.netgate.com/topic/114364/change-url-table-update-frequency>.