D6.4

Secure and privacy preserving data exchange among operators (v2)

DOCUMENT	D6.4	**WORKPACKAGE**	WP6
DELIVERABLE STATE	V2 FINAL	**PROGRAMME IDENTIFIER**	H2020-SU-DS-2020
REVISION	V2.0	**GRANT AGREEMENT ID**	101020560
DELIVERY DATE	18/04/2024	**PROJECT START DATE**	01/10/2021
DISSEMINATION LEVEL	PU	**DURATION**	3 YEARS

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

DISCLAIMER

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 Nº 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 AL ENERGIEI ELECTRICE TRANSELECTRICA SA (TEL), CENTRUL ROMAN AL ENERGIEI (CRE), TIMELEX (TLX).
WORKPACKAGE	WP6
DELIVERABLE TYPE	R Document, report DEM Demonstrator, pilot, prototype DEC Websites, patent fillings, videos, etc. **OTHER** ETHICS Ethics requirement ORDP Open Research Data Pilot DATA data sets, microdata, etc.
DISSEMINATION LEVEL	**PU Public** CO Confidential, only for members of the consortium (including the Commission Services) EU-RES Classified Information: RESTREINT UE (Commission Decision 2005/444/EC) EU-CON Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)

	EU-SEC Classified Information: SECRET UE (Commission Decision 2005/444/EC)
DELIVERABLE STATE	V2.0 final
CONTRACTUAL DATE OF DELIVERY	18/04/2024
ACTUAL DATE OF DELIVERY	15/04/2023
DOCUMENT TITLE	Secure and privacy preserving data exchange among operators (v2)
AUTHOR(S)	Paul Lacatus (CRE), Amir Safdarian(ENERIM), Luigi Coppolino(CINI), Alfredo Petrulo(CINI), Andrej Bregar(INF), Marco Angelini(ENG), Paolo Rocetti(ENG), Andreas Papadakis(SYN), Konstantinos Lessis (WIN), Andreas Georgakopoulos(WIN).
REVIEWER(S)	Andrej Bregar (INF), Priit Anton (GT)
ABSTRACT	SEE EXECUTIVE SUMMARY
HISTORY	SEE DOCUMENT HISTORY
KEYWORDS	EPES, Cyber security, Cyber threat intelligence, CTI sharing, Electronic Data Exchange, STIX, TAXII, MISP, Results Exploitation

Document History

Version	Date	Contributor(s)	Description
V1.1	20/10/2023	CRE	Table of Content (ToC) updated for version 2
V1.2	30/01/2024	CRE	Updated sections for MISP and Federated Machine Learning models for Privacy EPES sensitive data
V1.3	01/03/2024	ENG	Filled paragraph 8.1
V1.4	25/03/2024	INF, CINI	Contribution to Chapter 8
V1.5	10/04/2024	CRE	Refining content based on deliverables in development
V1.9	10/04/2024	CRE	Version for peer review
V2.0	15/04/2024	CRE	Compiled the remarks from peer review and generated the final version V2.0

Table of Changes in Version 2

Section	Contributor(s)	Change description
All	CRE	Updated the ToC for Version 2 and document structure
6	CRE, INF	Added section 6 for MISP protocol analysing
7	CRE, ENG	Added section 7 for Federated Machine Learning models for Privacy EPES sensitive data
8	CRE, ENG, SYN, INF, CINI	Added section 8 focusing on Achievements in CYBERSEAS Project

Table of Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

AKOS	Communications Networks and Services Agency of the Republic of Slovenia
AHP	Analytical Hierarchical Process
CL	Cascading Level
CEI	Critical Energy Infrastructure
CEIS-SG	Critical Energy Infrastructure Security Stakeholders Group
CIRTS/ CERTS	Computer emergency response team
CoU	Community of Users
CSI	Cyber Security Intelligence
CTI	Cyber Threats Intelligence
ECSO	European Cybersecurity Organization
DER	Distributed Energy Resources
DP	Differential Privacy
DG ENER	Directorate-General for Energy
DSO	Distribution system operator
ECCC	European Competence Network of Cybersecurity Centres
ENISA	The European Union Agency for Cybersecurity
ENTSO-E	European Network of Transmission System Operators for Electricity
EPES	Electrical Power and Energy System
EE-ISAC	European Energy – Information Sharing & Analysis Centre
ECSCI	European Cluster for Securing Critical Infrastructure
FL	Federated learning
FedAvg	Federated Averaging
GNMax	Gaussian based noise distribution
HE	Homomorphic Encryption
IDSA	International Data Spaces Association
IED	Intelligent Electronic Device

IM	Information Management
KPI	Key performance indicator
LNMax	random Laplacian noise
ML	Machine learning
NIS	NIS Directive (Directive on security of network and information systems)
NIS2	ENISA NIS directive. "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)".
PATE	Private Aggregation of Teacher Ensembles
PES	Power and Energy System
PLC	Programmable Logic Controller
REA	Research European Agency
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SGAM	Smart Grid Architecture Model
SODO	Slovenian DSO (Sistemski Operater Distribucijskega Omrežja)
SCO	STIX Cyber-observable Object
SDO	STIX Domain Objects
SOTA	State of the art analyses
SRO	STIX relationship Object
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Intelligence Information
TNCEIP	Thematic Network on Critical Energy Infrastructure Protection
TSO	Transmission System Operator
VS	Vulnerability Score
WP	Work Package

Executive Summary

This report constitutes the deliverable D6.3 Secure and privacy preserving data exchange among operators (v1) of the CyberSEAS Project.

The deliverable D6.3 is focusing on dissemination of Cyber Security Intelligence over the EPES and Energy stakeholders involved in Critical infrastructure operation to increase the awareness to Cyber Security problems focusing specific vulnerabilities and attacks over EPES.

The deliverable is analysing the status of development of Cyber Security intelligence and how this is generated and disseminated over the involved organisations from EU.

To enhance the cybersecurity and resilience of critical infrastructure in EPES and other stakeholders of critical infrastructure, the CyberSEAS project has incorporated Machine Learning techniques. The efficiency of ML algorithms is based depends on the availability of large amounts of significant data to train and validate the ml-based models. It is crucial for all parties to share Cyber Threats Intelligence (CTI) to build better-performing models. The first is the lack of a standardized method to share data among companies, and the second is the need for data anonymization to comply with GDPR and prevent the exposure of sensitive data in the event of a cyber-attack.

The deliverable is also considering the industry standards used in CTI dissemination focusing on STIX and TAXII industry standards.

The deliverable is considering in detail the two industry standards indicated above considering as next step in T6.2 the testing of a local system inside critical infrastructure based on STIX/TAXII for CTI dissemination.

The goal of this task lies into the design and development of an access scheme satisfying the key requirements of data privacy and controlled, authorized access to the EPES CTI data by each stakeholder in a federated topology.

The deliverable is focusing on the CyberSEAS partners as participants to such of dissemination process and also a survey on the tools belonging to CyberSEAS ecosystem and the possible interaction with such a system.

Considering the evolution of the tools development and integration in version 2 of deliverable new chapters were introduced that encapsulates the new advancements. All this are detailed in Chapters 6, 7, and 8, focusing on cybersecurity protocols and federated machine learning (FML) within the context of the CYBERSEAS project.

Chapter 6: MISP Protocol introduces the Malware Information Sharing Platform (MISP), an advanced protocol designed for sharing cybersecurity threat information efficiently. The introduction provides an overview of the MISP's capabilities, emphasizing its role in enhancing collaborative cybersecurity efforts. Key components such as MISP Taxonomy and MISP Galaxy are introduced, each playing a crucial role in standardizing threat information and enabling synergistic analyses of threat data across different platforms.

Chapter 7: Federated Machine Learning models for Privacy EPES sensitive data : explores the application of Federated Machine Learning (FML) in protecting the sensitive data of Energy Power and Energy Systems (EPES). It lays down the basics of FML architectures, presenting a novel approach for decentralized learning without compromising data privacy. The chapter delves into various data privacy protection mechanisms within FML, including Data Anonymisation, Differential Privacy, Secure Aggregation, and Private Aggregation of

Teacher Ensembles (PATE), each ensuring that sensitive information remains confidential while allowing for beneficial data analysis and machine learning outcomes.

Chapter 8: Achievements in CYBERSEAS project in secure and privacy-preserving data exchange among operators : details the achievements of the CYBERSEAS project, emphasizing the secure and privacy-preserving data exchange among operators. It illustrates the deployment of FML algorithms in ALIDA (ENG) and IDS (SYN), highlighting the advancements in proactive notification and workflow optimization in threat detection systems. The chapter also discusses the seamless data interchange through Data Spaces (CINI) and the efficacy of the MISP protocol in the exchange of Cyber Threat Intelligence (CTI) within the CYBERSEAS framework. Further, it describes the integration of the SAPPAN tool with MISP for enhanced threat intelligence and outlines the successful implementation of the CTI data transfer from the CVIAT tool using the STIX format.

In conclusion, these chapters underscore significant developments in cybersecurity practices, particularly the integration of FML for the safeguarding of sensitive data and the implementation of the MISP protocol for comprehensive threat intelligence sharing.

1 Introduction (UPDATED)

The CyberSEAS project is a European Union funded collaborative project improving the cyber security of the European electrical power energy systems (EPES).

CyberSEAS (Cyber Securing Energy dAta Services) projects aims to improve the overall resilience of energy supply chains, protecting them from disruptions that exploit the enhanced interactions, the extended involvement models of stakeholders and consumers as channels for complex cyber-attacks, the presence of legacy systems and the increasing connectivity of energy infrastructures, data stores and services retailers.

The work package WP6 main objective is to define ways of linking EPES operators and other stakeholders in the Cyber Security problems and finally to create a cyber-secure energy common data space. In particular, this WP will define the rules for the governance of the cybersecurity aspects among players of the energy supply chain; enable the authorized and controlled usage of data among operators, leveraging the federated learning approach to preserve the data ownership while, at the same time, allowing for a more effective and productive usage of data spread across the energy supply chain; provide solutions for the orchestration of communications among operators about data breaches and other cyber incidents, while preserving the privacy of energy customer's data and provide rules and tools for quick and effective reporting to CERTs, thus easing stakeholders collaboration in the management of cyber-attacks and incidents on EPES infrastructures.

The actual document is the second version deliverable form **Task 6.2 Secure and privacy preserving data exchange among operators** – The goal of this task lies into the design and development of an access scheme satisfying the key requirements of data privacy and controlled, authorized access to the EPES data by each stakeholder in a federated topology. Specifically, within this task, privacy preserving secure federated ML models will be trained without compromising EPES sensitive data, since they will not be extracted from their original sources. T6.2 is responsible for the development of machine/deep learning (ML/DL) models, trained under the Federated Learning (FL) paradigm, including the local training, parameters and model updates based on secure aggregation and decision regarding the weighted average that constructs the global (i.e. federated) model.

This document is a report over the actual status of communications focusing the cyber–Security Intelligence, the standard ways used today for secure and privacy preserving communications and concerning Cyber Security Intelligence (CSI), the industry standards used for this purpose and how these ways and standard can be used by the CyberSEAS developed tools and procedures.

1.1Intended Audience

The audience for this document is mainly composed by the CyberSEAS partners that will be able to analyse and define how the ways of CSI transfer in a secure and privacy preserving proposed in this deliverable will work for the CyberSEAS tools and procedures.

1.2 Relations to other activities

This deliverable is a result of the T6.2 task. The goal of this task lies into the design and development of an access scheme satisfying the key requirements of data privacy and controlled, authorized access to the EPES data by each stakeholder in a federated topology. This task is in direct interaction with the other tasks in WP6 mainly to:

- Task 6.3 Orchestrated management of data breaches among supply chain operators
- Task 6.4 Rules & tools for operators' coordination and reporting to CERTs in case of incidents.
- Task 3.3 CyberSEAS toolset architecture and integration approach
- Task 3.4 Infrastructure for federated and self-sovereign data analytics

1.3 Document structure overview.

The document structure is based on eleven main Chapters.

- Introduction
- Cyber Security Intelligence
- Industry Standards for CTI communications
- STIX Protocol
- TAXII Protocol
- MISP Protocol
- Federated Machine Learning models for Privacy EPES sensitive data
- Achievements in CYBERSEAS project in secure and privacy preserving data exchange among operators.
- CyberSEAS project secure and privacy preserving data exchange.
- Instructions and implementation guidelines for a CTI communication system among Pilots
- Conclusions

In the first chapter **Introduction** the documents main characteristics and focuses are defined.

The second chapter **Cyber Security Intelligence** will define the notion of Cyber Security Intelligence, the strategies used in collecting the CSI information, how this information are communicated and disseminated in a secure way.

The third chapter **Industry Standards for CTI communications** will focus on the actual industry standards used in communication of the CSI information. There are two standard protocols used STIX and TAXI that will be defined in this chapter.

The fourth chapter **STIX Protocol** will define the protocol considering the implementation and technical requirements.

The fifth chapter **TAXII Protocol** will define the protocol considering the implementation and technical requirements.

The sixth chapter **MISP Protocol** will focus on a description of MISP protocol used for CTI exchange .

The seventh chapter **CyberSEAS project secure and privacy preserving data exchange. Federated Machine Learning models for Privacy EPES sensitive data** explains how the federated ML is used for sharing the results of training the ML without sharing the training data that can be subject of privacy or being sensitive.

The eight chapter **Achievements in CYBERSEAS project in secure and privacy preserving data exchange among operators** contains considerations about the implementations of protocols and technologies described in previous chapters in the CYBERSEAS ecosystem.

The nineth chapter **CyberSEAS project secure and privacy preserving data exchange**. will focuses on the intercommunications needs between the project's entities and tools.

The tenth chapter **Instructions and implementation guidelines for a CTI communication system among Pilots** will analyse the possible use of the communication tools defined in the deliverable inside the pilots.

The chapter number eleven **Conclusions** will extract conclusions and insights from the development of T6.2 defining the future steps to be done.

2 Cyber Security Intelligence

Cyber Security Intelligence enable the process of gathering and analysing data to identify potential cyber threats and to develop strategies to prevent attacks. To enable an efficient communication among the CyberSEAS stakeholders, the process requires advanced technology, specifically Machine Learning and Data Analytics. These techniques enable to sift through large amounts of data and detect patterns that may indicate a potential threat. The implementation of cyber security intelligence enables CyberSEAS pilots to be proactive in managing risks and preventing potential threats, thus preventing any disruptive outcomes. Furthermore, cyber security intelligence enables CyberSEAS pilots to comply with regulations and safeguard sensitive information.

The energy sector, as any other critical domain, is subject to rigorous regulatory requirements concerning cyber security. Failure to comply with these regulations can result in severe penalties, legal action, and loss of reputation. For sake of clarity, we briefly describe results of the IBM report [1] on the estimation of costs for data breaches, the average total cost of a data breach, obtained by collecting data from 17 different countries and 17 different sectors, amounted to $4.35 million. Figure 1 IBM report : Cost of Data breach 2022 [1] describe the average total cost of a data breach over the last years.

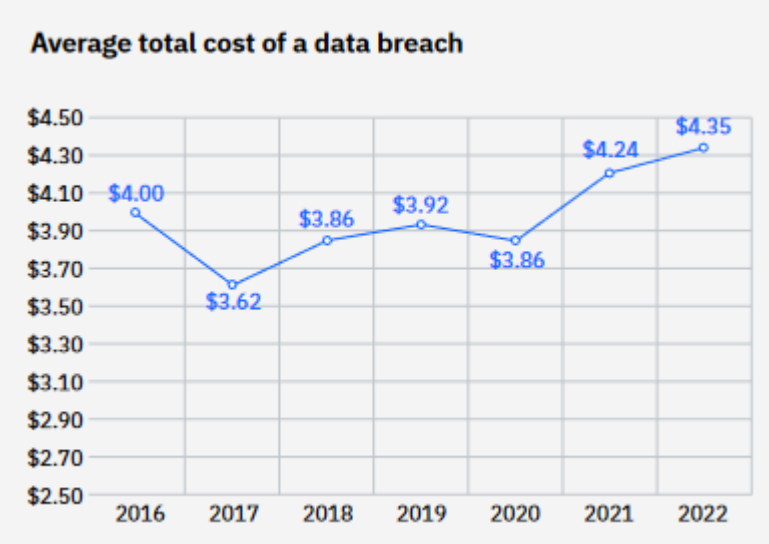

Figure 1 IBM report : Cost of Data breach 2022 [1]

To enhance the cybersecurity and resilience of critical infrastructure in the EPES, the CyberSEAS project has incorporated Machine Learning techniques. However, the success of this endeavour depends heavily on the availability of large amounts of data to train and validate the ml-based models. It is crucial for all parties to share data to build better-performing models. However, two criticisms must be considered. The first is the lack of a standardized method to share data among companies, and the second is the need for data anonymization to comply with GDPR and prevent the exposure of sensitive data in the event of a cyber-attack. Considering the current state of the art [2], the CyberSEAS project proposes solutions to address the issues at hand. The lack of standardized data models arises

due to the differences in the environments in which data are collected. Operators, pilots, and technical providers operate within distinct business contexts, resulting in heterogeneity that must be considered when collecting data for CTI purposes. The intention to answer this problem is identified in Strategic Objective 3 (SO3) of the CyberSEAS project, where adopting a dataspace view and agreeing on standard data models can mitigate this issue. In addition, the security of the dataspace, also to be addressed in SO3, is a fundamental aspect of the CyberSEAS project.

Concerning technical aspects, several approaches for training machine learning models have been considered to tackle these issues. Local training is not an ideal solution as each stakeholder would train its own data to build the model, which is not in line with the aim of the project to create a cooperative environment among partners. An alternative training model that aligns with the project's objective is centralized learning, which involves a centralized server collecting data from different stakeholders for training on a vast amount of data. While this method seems optimal, it comes with the risk of a single point of failure. If the server is compromised, there is a possibility of a significant data breach, thereby exposing sensitive data. The most optimal approach is federated learning, which allows data to remain within the owner's network, thereby preserving the privacy and integrity of sensitive user information. This paradigm involves local training for each stakeholder, which results in a trained model. These models are then sent to the central server, which aggregates and builds the final model.

2.1 Cyber Security Intelligence Strategy

The CyberSEAS project aligns strongly with the European Cyber Security Intelligence Strategy [3], recognizing that cyberspace has a profound impact on fundamental rights, social interactions, and economies, which are all heavily reliant on information and communication technology and sharing. An objective of this project is to establish a cooperative environment where stakeholders can proactively contribute data and access information that is essential for cybersecurity purposes. In line with NIS2, it is important to consider not only the technical aspects but also the political ones when staying informed and making decisions. The CyberSEAS project aims to provide guidelines and best practices to EPES operators, leveraging the CTI platform to disseminate knowledge on the latest cyber-attacks, thereby enhancing the resilience of critical infrastructures.

2.2 Cyber Security Intelligence Communications and Data Space

The communications are a fundamental part of the Cyber Security Intelligence. Even if communication takes place through various channels, such as email, websites, conference calls, and others, in the context of this project there's a need to exchange information and best practices, share EPES data and develop proactive strategies in a federated topology. To obtain this goal beyond the technical and technology support, a common data space and standardized data format are needed.

The CyberSEAS stakeholder could benefit from a heavy communication to respond to potential cyber threats in a collaborative manner. Sharing complete and accurate

information about cyber threats and attacks is essential in defining a collaborative strategy to prevent or respond to attacks in EPES systems.

The Cyber Security Intelligence communications need to comply with the ENISA (European Union Agency for Cybersecurity) directives. The ENISA programming document for 2023-2025 [4] highlights the crucial nature of Activity 4, which pertains to promoting operational collaboration among Member States, Union institutions, and relevant offices. This activity seeks to bolster the Union's capacity to respond to cyber incidents and enhance preparedness for large-scale cyber incidents. Furthermore, the activity 4 supports the implementation of the NIS2 Directive, particularly in terms of coordinated vulnerability disclosure and a European vulnerability database. By leveraging effective communication channels, stakeholder can stay ahead of potential threats and respond quickly and effectively in the event of an attack against EPES infrastructure.

Further, Cyber Security Intelligence is closely linked to the concept of dataspace, as it involves the collection, analysis, and correlation of various types of data to identify potential cyber threats and attacks. In CyberSEAS context, using Data Spaces and collecting EPES data in standardized manner could enhance the capabilities of CSI software and experts.

Another critical aspect of cyber security intelligence related to the strategic objective 3 of CyberSEAS project is to protect sensitive data threatened in the dataspace. By analysing network traffic with ML techniques and identifying vulnerabilities, cyber security professionals can develop approaches to protect against data breaches and other cyber-attacks.

2.2.1 ENISA

Established in 2004, the European Union Agency for Cybersecurity (ENISA) is an important entity within the European Union (EU) that aims to enhance cybersecurity capabilities across EU member states. ENISA is tasked with providing expert advice and support to the EU and its member states on various cybersecurity issues. The agency strives to promote cooperation between member states and improve their collective cybersecurity readiness by providing relevant resources, recommendations, and assistance. Ultimately, ENISA plays a crucial role in helping the EU and its member states to mitigate cyber threats and safeguard against potential attacks. It operates as a center of excellence for cybersecurity in Europe, providing information, guidance, and support to both the public and private sectors.

ENISA holds a significant role in cyber security intelligence, owing to its pivotal role in strengthening cybersecurity throughout the European Union. Its proficiency and expertise are highly regarded in the CyberSEAS context, as it assists in formulating cybersecurity policies, recognizing and minimizing potential risks, and responding to cyber-attacks.

ENISA works closely with other organizations such as CERT-EU, the European Cybercrime Centre (EC3), and other relevant bodies to ensure that information about cyber threats and attacks is shared in a timely and effective manner.

ENISA is also responsible for providing guidance and recommendations on cybersecurity best practices, as well as identifying emerging trends and threats. The agency conducts research and analysis to better understand the evolving threat landscape and works with relevant stakeholders to develop solutions that enhance cybersecurity resilience. Further, Enisa sustains the development of the Information Sharing and Analysis Centers (ISACs) in order to enhance information sharing connected to cyber threats [5]. It has been published a report [6] that aims to analyse Europe-Based ISACS, to identify common challenges and best

practise to share, additionally, the report itself can be used to create an ISAC. It has been bought to attention that there exists a lack of trust between the private and public sectors and a deficiency of a governance model. ENISA recommends that ISACs focus on enhancing their capabilities in threat intelligence analysis, incident response, and information sharing. It also recommends that ISACs collaborate with each other and with other stakeholders, such as national cybersecurity agencies and law enforcement, to improve their effectiveness.

In conclusion, ENISA is essential for European Union's cybersecurity of EPES infrastructure. Its role in providing stakeholders advice and support, promoting cooperation, and enhancing cybersecurity intelligence capabilities across the EU.

2.2.2 CERT-EU

CERT-EU, the Computer Emergency Response Team for the EU Institutions [7], is an integral part of the EU's cybersecurity strategy. Established in 2011, its role is to provide a rapid response to cyber incidents that affect EU institutions, agencies, and bodies. As a part of the European External Action Service, CERT-EU works closely with other EU bodies and agencies, such as ENISA, to provide a coordinated response to cyber threats. Its main functions include incident response, vulnerability management, and threat analysis. CERT-EU's expertise and resources are a valuable asset to the EU's cyber security intelligence efforts, as it allows for quick and effective response to cyber incidents and the sharing of information and best practices between member states.

2.2.3 European Cybersecurity Competence Centre and Network – Romania

The ECCC (European Cybersecurity Competence Centre) [8] aims to increase Europe's cybersecurity capacities and competitiveness, working together with a Network of National Coordination Centres (NCCs) to build a strong cybersecurity Community. The European Cybersecurity Competence Centre and Network is in establishing and development stage.

The main mission of ECCC, together with the Network of National Coordination Centres (NCCs), is Europe's new framework to support innovation and industrial policy in cybersecurity [9]. This ecosystem will strengthen the capacities of the cybersecurity technology Community, shield our economy and society from cyberattacks, maintain research excellence, and reinforce the competitiveness of EU industry in this field.

The ECCC, which will be located in Bucharest, will develop, and implement, with Member States, industry and the cybersecurity technology Community, a common agenda for technology development and for its wide deployment in areas of public interest and in businesses, in particular SMEs.

The Centre and the Network together will enhance our technological sovereignty through joint investment in strategic cybersecurity projects.

The mission will be achieved by fulfilling the task of making strategic investment decisions and pool resources from the EU, its Member States and, indirectly, the industry to improve and strengthen technology and industrial cybersecurity capacities, enhancing the EU's open

strategic autonomy. The Centre will play a key role in delivering on the ambitious cybersecurity objectives of the Digital Europe Programme and Horizon Europe programmes.

The Centre together with the Network will support the deployment of innovative cybersecurity solutions. It will also facilitate collaboration and the sharing of expertise and capacities among all relevant stakeholders, in particular research and industrial communities, as well as public authorities, in the Community.

2.2.4 Cybersecurity Intelligence databases and frameworks

Cyber intelligence databases serve as an essential source of information for CyberSEAS stakeholders to assess potential cyber threats and attack techniques. They comprise a variety of data sources that provide insight into software and process vulnerabilities. These databases are useful in identifying and prioritizing potential risks to an EPES critical infrastructure offering information on known threats, vulnerabilities, and potential attack vectors. Moreover, the data provided by these databases can also aid in selecting and implementing controls to mitigate identified risks. By integrating cyber intelligence databases into their risk assessment procedures, Pilot providers can make informed decisions to enhance their security position.

There are several cyber threat intelligence databases available, both commercial and open source. Among these, the National Vulnerability Database (NVD) is a U.S. government repository of standards-based vulnerability management information. It serves as a comprehensive resource for information security vulnerabilities and provides a means for sharing information among different organizations. In addition, the Common Vulnerabilities and Exposures (CVE) [10] database and the Common Vulnerability Scoring System (CVSS) are used to identify and categorize software vulnerabilities. These databases provide a standardized approach to tracking vulnerabilities and assessing their potential impact, which can help organizations prioritize their security efforts.

Furthermore, in pursuit of an enhanced cyber security intelligence framework, several European strategies have been developed to facilitate the sharing and analysis of information among different stakeholders. The primary objective is to establish a platform and provide guidelines that can be utilized by various players across the European Union to improve their cyber security posture.

The EU Cybersecurity Certification Framework for Information and Communications Technology (ICT) [11] has been developed to offer customizable and risk-based certification schemes in the EU, which can set guidelines for enhancing cybersecurity intelligence capabilities. The framework incorporates a set of technical requirements, standards, rules, and procedures, which enable the creation of a cybersecurity intelligence-building schema. Furthermore, the certificate issued under the framework will be accepted in all EU member states, which facilitates cross-border business operations.

ENISA promoted a significant initiative, CyCLONe that stands for European Cyber Crises Liaison Organization Network [12], which is a network designed to keep the European Union's cybersecurity entities updated and enable a timely and effective response to cyberattacks. The fundamental principle underlying this initiative is the recognition that an attack on a Member State is an attack on the European Community and must be met with a common

response. The objective is not only to foster increasingly effective connections between the CSIRTs of various Member States but also to establish a political link with IPCRs (integrated political crisis response), which must provide a political response to the incident. This type of response to large-scale crises meets the need for an intermediary between the technical and political levels, as identified directly by NIS2, which formally establishes CyCLONe.

It is important to highlight another significant platform, MeliCERTes, which has the objective of promoting confidence and trust among the national Computer Security Incident Response Teams (CSIRTs) of the Member States, as well as facilitating their operational cooperation. MeliCERTes is a modular platform that comprises several essential features, with each module specializing in a specific task related to cyber security response. Member States' CSIRTs participate on an equal footing in the MeliCERTes Core Service Platform (CSP) within verified Trust Circles, which serve as forums for sharing information and collaborating on computer security incidents.

In 2020, a publication of ENISA on Threat Intelligence [13] highlighted the significance of cyber threat intelligence (CTI) as a crucial element in addressing cyber threats. Apart from this publication, there are other noteworthy initiatives related to CTI. One of these is Cybrary [14], an online platform that provides cybersecurity courses and information. The platform aims to assist professionals in acquiring the necessary knowledge and skills to understand and respond to cyber threats. In particular, it offers a course that is dedicated to CTI collection and data analysis.

Another significant framework linked to cybersecurity intelligence is the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) [15] developed by MITRE. This framework serves as a common language for cybersecurity professionals to share information and defend against cyber-attacks. ATT&CK is designed as a matrix of tactics that attackers may use, with each technique being mapped to a specific tactic. The framework provides a comprehensive understanding of attack strategies and enables organizations to develop a proactive approach to threat detection and response.

Another important initiative related to CTI is Insikt [16] which is a CTI platform utilized by various companies to detect threats and prevent attacks. The platform's capabilities are linked to monitoring and analysing potential threat actor activity using different sources, such as open-source intelligence (OSINT), dark web data, and technical indicators of compromise.

2.2.5 MITRE

The MITRE Corporation is a non-profit organization recognized for its creation of numerous cybersecurity frameworks and tools. MITRE significantly contributes to the advancement of cybersecurity intelligence by promoting collaborative environments and providing databases and tools that offer a comprehensive overview of cyber threats, responses, and procedures. Through its strong collaboration with the EU and its member states, MITRE has made significant progress in cybersecurity intelligence and facilitated cooperation in the field of cybersecurity. As previously noted, MITRE has developed the ATT&CK framework, which comprises an exhaustive inventory of tactics, techniques, and procedures that an organization can employ to enhance its defences by comprehending attack methods and, in turn, adapting cybersecurity strategies accordingly.

2.2.6 NESCOR

NESCOR, which is an acronym for "National Security and Emergency Preparedness Communications Operations and Resources," is a US government program designed to ensure uninterrupted communication during national emergency situations. The primary objective of the program is to enable essential communication between critical infrastructure operators in times of crisis. To achieve this goal, NESCOR collaborates with various organizations, including MITRE, to develop effective cybersecurity strategies aimed at mitigating and preventing disruptive events that may arise due to cyber-attacks.

2.2.7 NIST Cybersecurity framework

The National Institute of Standards and Technology (NIST) has developed a framework that provides guidelines, best practices, and standards to manage and reduce cybersecurity risks. The primary focus is to protect critical infrastructure, which if subject to attacks, can cause destructive cascading events. The framework is primarily composed of five fundamental functions:

- Identify: This function encompasses the elements necessary to perform a proper risk assessment. Its goal is to identify critical assets of the organization, define risks, and possible mitigation actions.
- Protect: The framework introduces best practices for the protection of critical assets. Among these are personnel training, management of security measures to be implemented, and policies on physical security.
- Detect: Detection focuses on the timeliness with which harmful events are detected. It requires a careful monitoring phase of the system.
- Respond: The framework provides guidelines on proper emergency management and incident response procedures with the aim of minimizing the negative effects of a possible attack.
- Recover: This function focuses on the proper resumption of activities after a possible cyber-attack. The speed at which the organization returns to the point before the attack identifies an important parameter to evaluate.

The objective is to ensure a panoramic view of possible risks and attack scenarios that afflict critical infrastructure, with the aim of protecting the most important assets and ensuring an efficient incident response process.

2.3 Cyber Threats Intelligence dissemination needs.

In CyberSEAS project there's the need to disseminate Cyber Threat Intelligence procedures and best practices among EPES operator in order to prevent cyber incidents. Proper sharing of the right information allows different stakeholder, also not directly involved in the project, to implement relevant cybersecurity strategies. It is essential to stay updated on possible threats in order to implement the right strategy for risk identification and mitigation. To ensure proper dissemination, several factors must be considered, including:

- Timeliness: It is crucial that information regarding threats or ongoing attacks is provided as quickly as possible to the pilot to prevent any cascading effect that can cause disruptive outcomes.
- Relevance: The data and information that is shared must be relevant and easy to interpret.
- Accuracy: The information must be directed and accurate to enable critical infrastructure experts or businesses professionals to make the right decisions.
- Context: The cybersecurity information should provide an exhaustive background, such as information on the severity of an attack or the potential impact an attack could have.
- Privacy: The shared information must be anonymized.
- Collaboration: Different players must create a collaborative environment, including governments and critical infrastructures operators.

CyberSEAS CSI will contribute to dissemination of data among EPES operator, also using MeliCERTes.

3 Industry Standards for CTI communications

Cyber Security is a common effort, executed in an orchestrated manner from many participants and stakeholders. Cybersecurity involves protecting computer systems, networks, and sensitive data from unauthorized access, theft, damage, and other cyber threats. It is a complex field that requires collaboration and cooperation between various stakeholders, including individuals, businesses, government agencies, and cybersecurity experts.

One of the main reasons why cybersecurity is an orchestrated effort is that cyber threats are constantly evolving and becoming more sophisticated. Hackers and cybercriminals are always looking for new vulnerabilities and weaknesses to exploit, and they can target anyone, from individual users to large corporations and government agencies. Therefore, it is essential that everyone takes responsibility for their own cybersecurity and works together to prevent cyber-attacks and mitigate their impact.

For example, individuals can protect themselves by using strong passwords, keeping their software up-to-date, and being careful about clicking on suspicious links or downloading suspicious attachments. Businesses and organizations can implement cybersecurity policies and protocols, conduct regular training for employees, and invest in cybersecurity technologies and services. Government agencies can enact regulations and legislation that promote cybersecurity and work with private sector partners to share threat intelligence and coordinate response efforts.

3.1 Developments in the area of CTI

To be able to run such an orchestrated effort the cybersecurity industry needs to use common approach . A common approach is based on standardization and standards.

Cyber threat information standardization is the process of establishing common standards for how threat information is collected, analysed, and shared across organizations and industries. Standardization helps to ensure that cyber threat information can be easily exchanged and understood by different parties, regardless of their technical capabilities or organizational structures.

There are several benefits of standardizing cyber threat information. First, standardization enables more effective and efficient sharing of threat intelligence, which can help organizations and industries to detect and respond to cyber threats more quickly and effectively. Second, standardization can help to reduce the costs and complexity of threat intelligence sharing, as it eliminates the need for custom integrations and translations between different systems and formats. Finally, standardization can help to promote greater collaboration and cooperation between organizations and industries, as it establishes common ground for discussing and addressing cyber threats.

There are several organizations and initiatives working to standardize cyber threat information, including the Cyber Threat Alliance (CTA) [17], and the Open Cybersecurity Alliance (OCA) [18]. These efforts aim to establish common standards for threat intelligence sharing, including how threat information is collected, analysed, and shared, as well as how

it is represented and formatted. By standardizing cyber threat information, these initiatives are helping to improve the overall security and resilience of the digital ecosystem.

Such an effort for developing standardized data interfaces to support an open ecosystem where cybersecurity tools interoperate without the need for custom integrations by OCA [18] is based on a number of principles :

- Product interoperability
- Security Tool Integration
- Open Security
- Trust and Transparency
- Collaborative community
- Open Governance

Figure 2 OCA principles [18]

The Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) standards are a result of such a standardization effort and collaborative community effort,

3.2 STIX Protocol

STIX is an open-source standard, initially defined in 2012 by the OASIS Cyber Threat Intelligence TC [15]

STIX is a language for describing and interchanging cyber threats intelligence objects.

Figure 3 STIX Logo [25]

Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI) [19].

STIX enables organizations to share CTI with one another in a consistent and machine-readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively.

STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection, and response, and more.

Figure 4 STIX relationship example [19]

STIX operates with different STIX Domain Objects (SDOs) . In Figure 4 STIX relationship example are shown such of objects interacting between them . The central object is a "campaign" that can be attributed to a "Threat Actor" and targets a "vulnerability". The campaign can be indicated by some "indicators". There are also "indicators "that points out a "Threat actor".

The actual version of STIX is STIX 2.1.

STIX 2 objects are represented in JSON. An example of a campaign described in STIX is shown.

```
{
    "type": "campaign",
    "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "spec_version": "2.1",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:23.000Z",
    "name": "Green Group Attacks Against Finance",
    "description": "Campaign by Green Group against targets in the financial services sector."
}
```

Figure 5 STIX Campaign Example [19]

3.3TAXII Protocol

Trusted Automated Exchange of Intelligence Information (TAXII) is an application layer protocol used to exchange cyber threat intelligence (CTI) over HTTPS. TAXII enables organizations to share CTI by defining an API that aligns with common sharing models. Specifically, 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. Collections and Channels can be organized by grouping them into an API Root to support the needs of a particular trust group or to organize them in some other way. Note: This version 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 this specification. [20]

TAXII is specifically designed to support the exchange of CTI represented in STIX. As such, the examples and some features in the specification are intended to align with STIX. This does not mean TAXII cannot be used to share data in other formats; it is designed for STIX but is not limited to STIX. [20]

Figure 6 TAXII logo [19]

The TAXII API is described as sets of Endpoints. Each Endpoint is identified by the URL that it is accessible at and the HTTP method that is used to make the request. For example, the "Get Collections" Endpoint is requested by issuing a GET to `{api-root}/collections/`. Each Endpoint identifies its URL, which parameters it accepts (including both path parameters and standard parameters), which features it supports (e.g., filtering), and which content types it defines for request and response. It also identifies common error conditions and provides guidance on how to use the Endpoint.

This section defines behaviour that applies across Endpoints, such as normative requirements to support each Endpoint, sorting, filtering, and error handling.

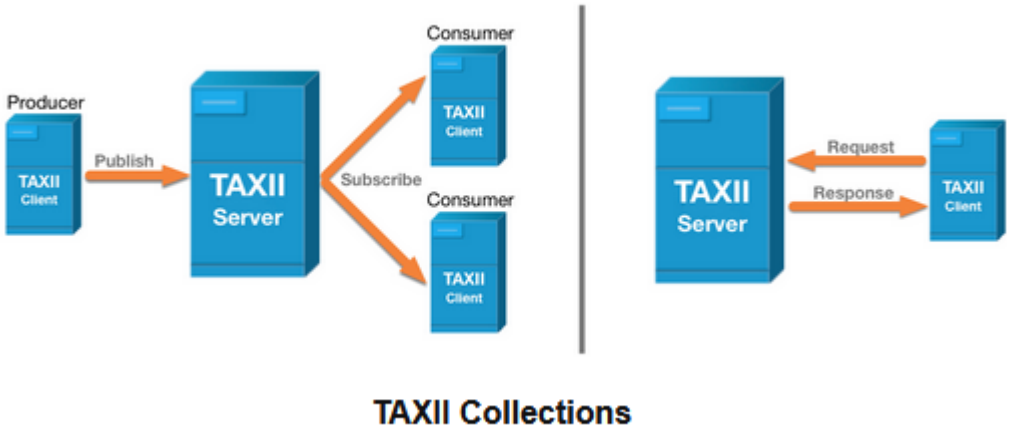

Figure 7 TAXII Collections [19]

A TAXII server can operate as a message broker. A client is publishing a message that is sent to the subscribing clients .

3.4 MISP Threat Sharing Platform

MISP is an open-source Threat intelligence sharing platform.

MISP is a threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. [21]

MISP is used today in multiple organizations. It is used not only to store, share, collaborate on cyber security indicators, malware analysis, but also to use the IoCs (Indicator of Compromise) and information to detect and prevent attacks, frauds, or threats against ICT infrastructures, organizations, or people.

MISP allows users to create and share events, which contain relevant information about specific security threats. The platform also provides a range of automated features, such as attribute tagging, correlation, and clustering, to help users identify and respond to threats more effectively. Further details on MISP are in Chapter 6.

3.5 Selection criteria

MISP (Malware Information Sharing Platform) and STIX/TAXII (Structured Threat Information Expression/Trusted Automated Exchange of Indicator Information) are two different frameworks used in the field of cybersecurity for sharing and exchanging threat intelligence information.

MISP is an open-source platform that enables organizations to share, store, and collaborate on threat intelligence information, including indicators of compromise (IOCs), malware samples, and vulnerabilities.

On the other hand, STIX/TAXII is a set of standards developed by the Cyber Threat Intelligence (CTI) community for sharing and exchanging structured threat intelligence information. STIX provides a standardized language and format for describing and sharing threat intelligence information, while TAXII enables the exchange of this information between different organizations.

Compared to MISP, STIX/TAXII is more focused on standardizing the format of the threat intelligence information, whereas MISP provides a platform for sharing, storing, and analysing this information. However, MISP does support the STIX format for importing and exporting data, and it can also be used to ingest data from other sources that use STIX/TAXII.

In summary, MISP and STIX/TAXII serve different but complementary roles in the cybersecurity community. MISP provides a platform for sharing, storing, and analysing threat intelligence information, while STIX/TAXII provides a standard language and format for describing and exchanging this information.

For the task envisaged in the document to establish a CTI information sharing we are considering that a standardized approach is a better, long-lasting solution.

4 STIX Protocol

4.1 Introduction to Structured Threat Information eXpression (STIX)

Structured Threat Information eXpression or STIX [22] is a standardized XML programming language and serialisation 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 Cybersecurity Threat Information (CTI) with each another 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, initially defined in 2012 by the OASIS Cyber Threat Intelligence TC [23]. The current version of STIX is 2.1 and was released in March 2020.

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. The available STIX Domain objects are briefly presented in Table 1 STIX Domain Objects (SDOs), below.

Table 1 STIX Domain Objects (SDOs)

SDO Name	SDO Description
Attack Pattern	Attack Patterns are a type of tactics, techniques, and procedures (TTP) that describe ways that adversaries attempt to compromise targets. They are used to help categorize attacks, generalize specific attacks to the patterns that they follow and provide detailed information about how attacks are performed.
Campaign	A Campaign is a grouping of adversarial behaviours that describes a set of malicious activities or attacks (sometimes called waves) that occur over a period of time against a specific set of targets. Campaigns usually have well defined objectives and may be part of an Intrusion Set.
Course of Action	A recommendation from a producer of intelligence to a consumer on the actions that they might take in response to that intelligence. A Course of Action is an action taken either to prevent an attack or to respond to an attack that is in progress. It may describe technical, automatable responses (applying patches, reconfiguring firewalls), but can also describe higher level actions like employee training or policy changes.
Grouping	It explicitly asserts that the referenced STIX Objects have a shared context, unlike a STIX Bundle (which explicitly conveys no context). A STIX Grouping object might represent a set of data that, in time, given sufficient analysis, would mature to convey an incident or threat report, as a STIX Report object.
Identity	Identities can represent actual individuals, organizations, or groups, as well as classes of individuals, organizations, systems, or groups (for instance the finance sector). The Identity SDO can capture basic identifying information, contact information and the sectors that the Identity belongs to. Identity is used to represent targets of attacks, information sources, object creators and threat actor identities.

Indicator	Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity. For example, an Indicator may be used to represent a set of malicious domains and use the STIX Patterning Language to specify these domains.
Infrastructure	It represents a type of TTP and describes any systems, software services and any associated physical or virtual resources intended to support some purpose (e.g., servers used as part of an attack, device or server that are part of defence, database servers targeted by an attack, etc.). The Infrastructure SDO represents a named group of related data that constitutes the infrastructure.
Intrusion set	An Intrusion Set is a grouped set of adversarial behaviours and resources with common properties that is believed to be orchestrated by a single organization. An Intrusion Set may capture multiple Campaigns or other activities that are all tied together by shared attributes, indicating a commonly known or unknown Threat Actor. New activity can be attributed to an Intrusion Set even if the Threat Actors behind the attack are not known. Threat Actors can move from supporting one Intrusion Set to supporting another, or they may support multiple Intrusion Sets. While the Campaign represents a set of attacks over a period of time against a specific set of targets to achieve some objective, an Intrusion Set is the entire attack package and may be used over a very long period of time, in multiple Campaigns, to achieve potentially multiple purposes.
Location	A Location represents a geographic location. The location may be described as any, some or all of the following: region (e.g., North America), civil address (e.g., New York, US), latitude and longitude. Locations are primarily used to give context to other SDOs. The Location SDO can be related to an Identity or Intrusion Set to indicate that the Identity or Intrusion Set is located in that location. It can also be related with a malware or attack pattern to indicate that they target victims in that location.
Malware	Malware is a type of TTP that represents malicious code. It generally refers to a program that is inserted into a system, usually covertly. The intent is to compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or otherwise annoy or disrupt the victim.
Malware Analysis	Malware Analysis captures the metadata and results of a particular static or dynamic analysis, performed on a malware instance or family.
Note	A Note is intended to convey informative text to provide further context and/or to provide additional analysis, not contained in the STIX Objects, Marking Definition objects or Language Content objects, which the Note relates to. Notes can be created by anyone (not just the original object creator).
Observed Data	Observed Data conveys information about cyber security related entities, such as files, systems and networks using the STIX Cyber-observable Objects (SCOs). For example, Observed Data can capture information about an IP address, a network connection, a file, or a registry key. Observed Data is not an intelligence assertion, it is simply the raw information without any context for what it means.
Opinion	An Opinion is an assessment of the correctness of the information in a STIX Object produced by a different entity. The primary property is the opinion property, which captures the level of agreement or disagreement using a fixed scale. That fixed scale also supports a numeric mapping, to allow for consistent statistical operations across opinions.
Report	Reports are collections of threat intelligence, focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including context and related details. They are used to group related threat intelligence together, so that it can be published as a comprehensive cyber threat story.
Threat Actor	Threat Actors are actual individuals, groups or organizations believed to be operating with malicious intent. A Threat Actor is not an Intrusion Set but may support or be affiliated with various Intrusion Sets, groups, or organizations over time. Threat Actors leverage their resources and, possibly, the resources of an Intrusion Set, to conduct attacks and run

	Campaigns against targets. Threat Actors can be characterized by their motives, capabilities, goals, sophistication level, past activities, resources they have access to and their role in the organization.
Tools	Tools are legitimate software that can be used by threat actors to perform attacks. Knowing how and when threat actors use such tools can be important for understanding how campaigns are executed. Unlike malware, these tools or software packages are often found on a system and have legitimate purposes and may be used by a Threat Actor during an attack.
Vulnerability	A Vulnerability is a weakness or defect in the requirements, designs, or implementations of the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that can be directly exploited to negatively impact the confidentiality, integrity, or availability of that system. The Vulnerability SDO is primarily used to link to external definitions of vulnerabilities or to describe 0-day vulnerabilities that do not yet have an external definition.

STIX also defines a set of STIX Cyber-observable Objects (SCOs) for characterizing host-based and network-based information. SCOs are used by various STIX Domain Objects (SDOs) to provide supporting context. SCOs document the facts concerning what happened on a network or host and do not capture the who, when or why.

By associating SCOs with SDOs, it is possible to convey a higher-level understanding of the threat landscape and to potentially provide insight as to the who and the why particular intelligence may be relevant to an organization. The available STIX Cyber-observable Objects (SCOs) are briefly presented in Table 2, below.

Table 2 Cyber-observable Objects (SCOs)

SCO Name	SCO Description
Artifact Object	The Artifact object permits capturing an array of bytes (8-bits), as a base64-encoded string or linking to a file-like payload.
Autonomous System (AS) Object	This object represents the properties of an Autonomous System (AS).
Directory Object	The Directory object represents the properties common to a file system directory.
Domain Name Object	The Domain Name object represents the properties of a network domain name.
Email Address Object	The Email Address object represents a single email address.
Email Message Object	The Email Message object represents an instance of an email message, corresponding to the internet message format described in [RFC5322] and related RFCs.
File Object	The File object represents the properties of a file. A File object MUST contain at least one of hashes or name.
IPv4 Address Object	The IPv4 Address object represents one or more IPv4 addresses expressed using CIDR notation.
IPv6 Address Object	The IPv6 Address object represents one or more IPv6 addresses expressed using CIDR notation.

MAC Address Object	The MAC Address object represents a single Media Access Control (MAC) address.
Mutex Object	The Mutex object represents the properties of a mutual exclusion (mutex) object.
Network Traffic Object	The Network Traffic object represents arbitrary network traffic that originates from a source and is addressed to a destination. The network traffic MAY or MAY NOT constitute a valid unicast, multicast, or broadcast network connection. This MAY also include traffic that is not established, such as a SYN flood.
Process Object	The Process object represents common properties of an instance of a computer program as executed on an operating system. A Process object MUST contain at least one property (other than type) from this object (or one of its extensions).
Software Object	The Software object represents high-level properties associated with software, including software products.
URL Object	The URL object represents the properties of a uniform resource locator (URL).
User Account Object	The User Account object represents an instance of any type of user account, including but not limited to operating system, device, messaging service, and social media platform accounts. As all properties of this object are optional, at least one of the properties defined below MUST be included when using this object.
Windows Registry Key Object	The Registry Key object represents the properties of a Windows registry key. As all properties of this object are optional, at least one of the properties defined below MUST be included when using this object.
X.509 Certificate Object	The X.509 Certificate object represents the properties of an X.509 certificate, as defined by ITU recommendation X.509. An X.509 Certificate object MUST contain at least one object specific property (other than type) from this object.

Furthermore, STIX also defines relationship objects, which is a link between STIX Domain Objects (SDOs), STIX Cyber-observable Objects (SCOs), or between an SDO and a SCO that describes the way in which the objects are related. Relationships can be represented using an external STIX Relationship Object (SRO) or, in some cases, through certain properties which store an identifier reference that comprises an embedded relationship. The available SRO are briefly presented in Table 3, below.

Table 3 STIX Relationship Objects (SROs)

SRO Name	SRO Description
Relationship	The Relationship object is used to link together two SDOs or SCOs in order to describe how they are related to each other. If SDOs and SCOs are considered "nodes" or "vertices" in the graph, the Relationship Objects (SROs) represent "edges". STIX defines many relationship types to link together SDOs and SCOs. These relationships are part of the definition of each SDO and SCO.
Sighting	A Sighting denotes the belief that something in CTI (e.g., an indicator, malware, tool, threat actor, etc.) was seen. Sightings are used to track who and what are being targeted, how attacks are carried out and to track trends in attack behaviour. The Sighting relationship object is a special type of SRO; it is a relationship that contains extra properties that are not present on the Generic Relationship object. These extra properties are included to represent data specific to sighting relationships (e.g., count, representing how many times something was seen), but for other purposes a Sighting can be thought of as a Relationship with a name of "sighting-of". Sighting is captured as a relationship because

	you cannot have a sighting unless you have something that has been sighted. Sighting does not make sense without the relationship to what was sighted.

5 TAXII Protocol

TAXII is a general protocol used to exchange CTI and transport STIX encapsulated Threat Information

5.1 Introduction to Trusted Automated eXchange of Intelligence Information (TAXII)

Trusted Automated Exchange of Intelligence Information (TAXII) [24] 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 8 TAXII - the logical structure of an API Root below depicts the logical structure of an API Root.

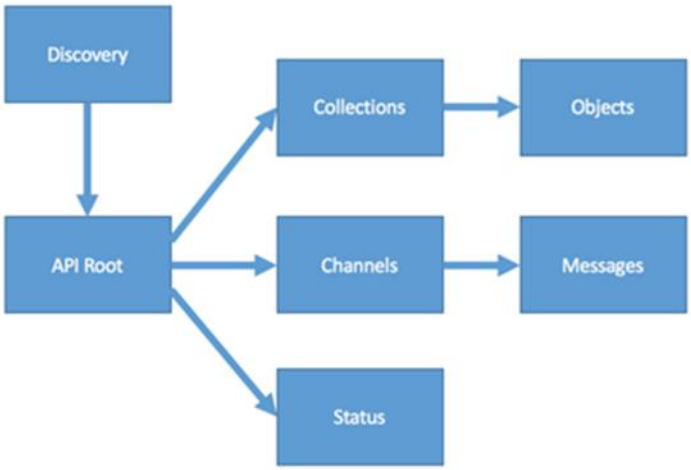

Figure 8 TAXII - the logical structure of an API Root

Discovery information can be used to learn about the API Roots hosted by a TAXII Server.

Collections objects 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, using 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.

6 MISP Protocol (UPDATED)

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. [21]

6.1Introduction in MISP Protocol

MISP Prtotocol can be used to share both technical and non-technical information about malware samples, incidents, attacks, and general cyber threat intelligence.

The primary objective of MISP is to facilitate the real-time exchange of valuable threat intelligence among organizations, aiding in the prevention of cyber-attacks. It enables users to share indicators of compromise (IoC), threat intelligence, and other security-related information in a structured and standardized manner, such as through shareable cybersecurity playbooks. This fosters alignment among security teams and enables swift action to mitigate potential security threats.

Figure 9 MISP Overview [21]

One of MISP's notable strengths lies in its adaptability, allowing organizations to share and store information without requiring mandatory data contributions. This flexibility empowers organizations to tailor the tool to meet their specific cybersecurity needs and facilitates rapid and efficient sharing of threat intelligence. Moreover, MISP's structured data storage format

enhances automation capabilities for utilizing databases, while its user interface supports export to various data formats, including Snort, STIX, OpenIOC, text, and CSV.

Moreover, MISP provides multiple import and integration functionalities, encompassing feed import and the integration of threat intelligence or OSINT feeds. This enables automated synchronization of events and attributes with other MISP instances, along with the ability to delegate sharing functionalities.

Two key components are developed to support the data representation in the MISP platform: the MISP Taxonomy and MISP Galaxy.

6.2 MISP Features

MISP is a threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. MISP is used today in multiple organisations not only to store, share, collaborate on cyber security indicators, malware analysis, but also to use the IoCs and information to detect and prevent attacks, frauds, or threats against ICT infrastructures, organisations, or people. [21]

- An efficient IoC and indicators database allowing to store technical and non-technical information about malware samples, incidents, attackers, and intelligence.
- Automatic correlation finding relationships between attributes and indicators from malware, attacks campaigns or analysis. Correlation engine includes correlation between attributes and more advanced correlations like Fuzzy hashing correlation (e.g. ssdeep) or CIDR block matching. Correlation can be also enabled, or event disabled per attribute.
- A flexible data model where complex objects can be expressed and linked together to express threat intelligence, incidents or connected elements.
- Built-in **sharing functionality** to ease data sharing using different model of distributions. MISP can automatically synchronize events and attributes among different MISP. Advanced filtering functionalities can be used to meet each organization sharing policy including a **flexible sharing group** capacity and an attribute level distribution mechanism.
- An **intuitive user-interface** for end-users to create, update and collaborate on events and attributes/indicators. A graphical interface to navigate seamlessly between events and their correlations. An event graph functionality to create and view relationships between objects and attributes. Advanced filtering functionalities and warning list to help the analysts to contribute events and attributes.
- **Storing data** in a structured format (allowing automated use of the database for various purposes) with an extensive support of cyber security indicators along fraud indicators as in the financial sector.
- **Export**: generating IDS (Suricata, Snort and Bro are supported by default), OpenIOC, plain text, CSV, MISP XML or JSON output to integrate with other systems (network IDS, host IDS, custom tools
- **Import**: bulk-import, batch-import, free-text import, import from OpenIOC, GFI sandbox, ThreatConnect CSV or MISP format.
- Flexible **free text import** tool to ease the integration of unstructured reports into MISP.

- A gentle system to **collaborate** on events and attributes allowing MISP users to propose changes or updates to attributes/indicators.
- **Data-sharing**: automatically exchange and synchronization with other parties and trust-groups using MISP.
- **Feed import**: flexible tool to import and integrate MISP feed and any threat intel or OSINT feed from third parties. Many default feeds are included in standard MISP installation.
- **Delegating of sharing**: allows a simple pseudo-anonymous mechanism to delegate publication of event/indicators to another organization.
- **Flexible API** to integrate MISP with your own solutions. MISP is bundled with PyMISP which is a flexible Python Library to fetch, add or update events attributes, handle malware samples or search for attributes.
- **Adjustable taxonomy** to classify and tag events following your own classification schemes or existing taxonomies. The taxonomy can be local to your MISP but also shareable among MISP instances. MISP comes with a default set of well-known taxonomies and classification schemes to support standard classification as used by ENISA, Europol, DHS, CSIRTs or many other organisations.
- **Intelligence vocabularies** called MISP galaxy and bundled with existing threat actors, malware, RAT, ransomware or MITRE ATT&CK which can be easily linked with events in MISP.
- **Expansion modules** in Python to expand MISP with your own services or activate already available misp-modules.
- **Sighting support** to get observations from organizations concerning shared indicators and attributes. Sighting can be contributed via MISP user-interface, API as MISP document or STIX sighting documents. Starting with MISP 2.4.66, Sighting has been extended to support false-negative sighting or expiration sighting.
- **STIX support**: export data in the STIX format (XML and JSON) including export/import in STIX 2.0 format.
- **Integrated encryption and signing of the notifications** via PGP and/or S/MIME depending on the user preferences.
- **Real-time publish-subscribe channel** within MISP to automatically get all changes (e.g. new events, indicators, sightings or tagging) in ZMQ (e.g. misp-dashboard) or Kafka.

6.3 MISP Taxonomy

The MISP Taxonomy is a data storage structure articulated through JSON, employing Machine Tags (or "Triple Tags") for a versatile and modifiable system of event classification and tagging. MISP enhances this with a PyMISP API, permitting events to be organized and marked using an extensive array of pre-existing taxonomies or bespoke classification systems. These taxonomies may be exclusive to a local environment or disseminated across various MISP installations. Additionally, there is support for sightings to circulate information on observed indicators and attributes. Furthermore, MISP incorporates secure notification methods such as PGP and S/MIME for encryption and signing, along with a real-time publish-subscribe mechanism to facilitate the exchange of threat intelligence..

6.4 MISP Galaxy

In contrast, the MISP Galaxy framework offers a uniform method for classifying data and ensures consistent representation of data across various entities. Comprising a collection of predetermined classifications like threat actors, malware types, assault methods, and toolsets, each classification in the MISP Galaxy is encapsulated within its own JSON file, complete with predefined tags. These tags are designed for application within the MISP ecosystem to systematically categorize events and their associated details.

6.5 MISP Dashboard

MISP allows uses of dashboards to visualize information helping analysts to have an image over the MISP processes. Having access to a large amount of Threat information through MISP Threat Sharing communities gives you outstanding opportunities to aggregate this information and take the process of trying to understand how all this data fits together telling a broader story to the next level.

Figure 10 Example of MISP Dashboard [21]

MISP is transforming technical data or indicators of compromise (IOCs) into cyber threat intelligence. MISP comes with many visualization options helping analysts find the answers they are looking for.

MISP usage in CyberSEAS project become important in the second part of the project due to development of SAPAN tool and the CTI exchange to CERTS in WP6 Task 6.4 that are detailed in Chapter 8.4.

7 Federated Machine Learning models for Privacy EPES sensitive data (UPDATED)

Federated machine learning (FML) allows for collaborative Machine Learning training with decentralized data. Unlike traditional methods, the data are decentralized as they are kept in the participating nodes. This means that no data is exchanged between the nodes, and data can be kept private. As a result, the nodes train the ML models locally and share model updates, which are aggregated to improve the global model. Keeping the data private alleviates the security risks, including data breaches. Data privacy allows alignment with regulatory constraints which may not allow or limit data sharing.

Another benefit of FML is related to scalability as multiple (or all nodes) participate in training, each one training its own model.

On the other hand, federated ML scenarios should be treated with care as the aggregated model, which depends on the data of each node (which can be of different distribution). Sharing model updates can be resource intensive.

7.1 Basics of federated ML architectures

Federated learning has gained the attention of the research and ML community. Indicative federated framework include:

- NVIDIA FLARE (Federated Learning Application Runtime Environment) building upon open-source components such as FLARE (Federated Learning Application Runtime Environment) as well as proprietary components. [https://developer.nvidia.com/flare/]
- TensorFlow Federated, which is open source, integrated with TensorFlow, with a flexible API for customization and experimentation. [https://www.tensorflow.org/federated]
- Federated Learning Over Wireless Networks (FLOWER) which is relatively lightweight and easy to integrate with existing infrastructure supporting privacy-preserving algorithms [https://flower.ai/].
- Federated AI Technology Enabler (FATE) is open source with privacy techniques, supporting horizontal and vertical federated learning, oriented at enterprise solutions. It is primarily focused on the Chinese market. [https://fate.fedai.org/]
- Sherpa.ai focuses on privacy-preserving federated learning, offering a Software as a Service (SaaS) platform that allows organizations to train machine learning models collaboratively without sharing their sensitive data. Sherpa.ai offers a user-friendly platform accessible through a subscription model. [https://sherpa.ai/]
- Federated Deep Learning with PaddlePaddle (PaddleFL) is an open-source framework based on the PaddlePaddle deep learning platform, for federated learning (FL). [https://github.com/PaddlePaddle/PaddleFL]

For the purpose of FML in project CyberSEAS the FLOWER framework has been selected, considering its lightweight approach as well as its modular architecture which allows the integration of workflows from ML applications independent of the underlying ML/DL framework (PyTorch, TensorFlow, etc.).

Specifically, FLOWER is compatible with almost any machine learning framework, and it collaborates with different operating systems, programming languages and hardware types, without restrictions on the number of clients. It also supports a wide range of machine learning algorithms, including deep learning, reinforcement learning and classical machine learning. FLOWER provides a high-level API for federated learning that abstracts the complexity of distributed systems and allows developers to focus on machine learning logic. It also includes model aggregation and fault tolerance, which are critical components of federated learning system.

The FLOWER framework is compatible with the ALIDA framework (provided by the coordinator, ENG) which is used in the project and FML on IDS tool provided by SYN.

7.2 Data Privacy Protecting Mechanisms in FML

The fact that the private data, in Federated Machine Learning, are not shared with the central server is a strong advantage, however, adversaries could potentially extract private information from the information exchanged between the central and the distributed nodes.

Such malicious actions could exploit the sharing of the trained parameters (model weights) sent from clients to the server. Additional mechanisms for privacy preservation in FL are employed to protect the data from different attacks. Typical approaches include data anonymisation, differential privacy (DP) and homomorphic encryption (HE).

7.2.1 Data Anonymisation

Data anonymisation is the process of converting data into certain forms that cannot be traced back to individuals. This procedure can be either implemented by removing critical/private information, or by adding random values to the input dataset.

There are two main types of identifiers on the input data: direct and indirect. Direct identifiers correspond to obvious attributes linked with sensitive information. Indirect identifies refer to the combinations of variables that reveal sensitive information. The decision on data anonymisation strategy depends on the type of data and application.

7.2.2 Differential Privacy

Differential privacy (DP) randomizes part of the mechanism's behavior to provide privacy as considered in the article "Deep learning with differential privacy." [25]. The motivation behind

adding randomness is to make it impossible to reveal behavior patterns that correspond either to the model and the learned parameters or to the training data.

The more typical scenario of differential privacy is based on Local Differential Privacy (LDP) described in "Local differential privacy for deep learning." [26], where noise is added to the individual inputs locally. Noise distributions are added to each one of these nodes, ending up in the untrusted aggregator. Adding controlled noise to the model updates before aggregation ensures that the global model cannot be used to accurately infer any information about an individual participant's data, even if an attacker manages to access the aggregated updates. The operators of the local nodes (CyberSEAS pilots in our case) are responsible for adding noise to their own data before they share it with the central server.

FLOWER supports DP algorithms including a) Gaussian noise addition (adding random noise drawn from a Gaussian distribution to the model updates) and b) Clipping (limiting the magnitude of updates before adding noise). As expected, there is a trade-off between the performance of a model and the privacy guarantee for its training data: as a higher level of noise is added, the model accuracy decreases. As such, in many practical scenarios, low levels of noise are selected which in return do not provide strong privacy guarantees.

7.2.3 Secure Aggregation

Secure aggregation techniques verify that the weights of the distributed models are not directly shared, i.e. they contribute to the global model, without revealing individual participant's weights. This can be achieved through Federated Averaging and Secure Sum.

In Federated Averaging (FedAvg, supported by FLOWER) each client updates its local model on its own data and sends only the average difference between the updated and initial weights to the server. The server then aggregates these averages to update the global model.

In Secure Sum, clients encrypt their updates using cryptographic techniques like homomorphic encryption. The server then performs the necessary computations on the encrypted updates to obtain the aggregated results without decrypting individual contributions.

Homomorphic encryption ensures that standard mathematical operations can be applied directly to the ciphertext, in such a way that the decrypted result is equivalent to performing analogous operations to the original unencrypted data as described in "Privacy-preserving deep learning via additively homomorphic encryption." [27] article. As an example, NVIDIA FLARE provides Homomorphic Encryption and Decryption filters that can be used by clients to encrypt Shareable data before sending it to the server. The server does not have a decryption key but using HE can operate on the encrypted data to aggregate and return the encrypted aggregated data to clients. Clients can then decrypt the data with their local key and continue local training.

However when mathematical computations/ functions are required to be implemented within the ciphertext space, homomorphic encryption schemes confront performance – related limitations.

7.2.4 Private Aggregation of Teacher Ensembles (PATE)

Private Aggregation of Teacher Ensembles (PATE) [28] introduces a teacher-student scheme.

Contrary to traditional ML algorithms, PATE separates the data into disjoint sets and trains a specific model at each set. The Teachers train private models using sensitive and private data. Using the public dataset the aggregated teacher asks for predictions of each teacher and aggregates the output to a unified prediction, guaranteeing in this way privacy. The student in the PATE framework learns to predict a result, which depends on noisy voting among all teachers.

The student cannot directly access the teacher's data or parameters The students access is restricted to their teachers so DP (Differential Privacy) can be applied. PATE also imports random Laplacian noise (LNMax) or a Gaussian based noise distribution (GNMax).

Other mechanisms can also be applied for data privacy preserving, such as Secure multiparty computation (SMC), which enables distributed parties to jointly compute an arbitrary function without revealing their own private input and output pairs described in "Secure Multi-Party Computation: Theory, practice and applications" [29].

The FML approach for ML in the CyberSEAS project considered in WP6 is needed by the specific of the critical infrastructure operators and EPES involved into the project due the need to conserve privacy of data collected.

8 Achievements in CYBERSEAS project in secure and privacy preserving data exchange among operators (UPDATED)

8.1 Federated Machine Learning algorithms implemented in ALIDA

The task T3.4 introduced a building block for the CyberSEAS toolset enabling the analysis of (big) data through Machine Learning techniques and algorithms at each EPES operator, as well as the support for the exchange of information required for federated learning, such as the latest version of the central model computed, or model updates computed by the participants on their local data.

The infrastructure has been leveraged on ENG asset ALIDA, evolving it from requirements and architectural indications from tasks 3.2 and 3.3.

The task 3.4 has been concluded along with the Deliverable D3.6 [30], providing software and reference guidelines the extended ALIDA tool, enabling FML capabilities to train models in a decentralized way without any data leaks and deploying the aggregator server in the ALIDA cloud platform.

One of the main features of the extensions of the ALIDA tool is support for the Flower framework (https://flower.ai/, https://arxiv.org/abs/2007.14390), a FL framework that offers new facilities to execute large-scale FL experiments. Its design integrates workflows independent of the ML/DL framework (PyTorch, TensorFlow, etc.) with minimum performance overhead. It supports a wide range of machine learning algorithms, including deep learning, reinforcement learning and classical machine learning. It also includes model aggregation and fault tolerance, which are critical components of any federated learning system. Flower allows building scalable federated learning systems that can be deployed on a range of devices, including mobile phones, edge devices, and cloud servers.

The FML task flow used in ALIDA is shown in Figure 11 below, where the main actors are:

- FML algorithm creator, which is the developer of FML BDA (Big Data Application) services for ALIDA using the Flower framework to enable federation.
- FML task creator, the one who defines and starts a BDA application through the ALIDA GUI with the model weights aggregator server.
- FML participants, who can define through ALIDA GUI (Graphical User Interface) the BDA application that contain the participant service, export, and start it locally (in any other machine) pointing to the exposed aggregator server and the own data that will remain in place.

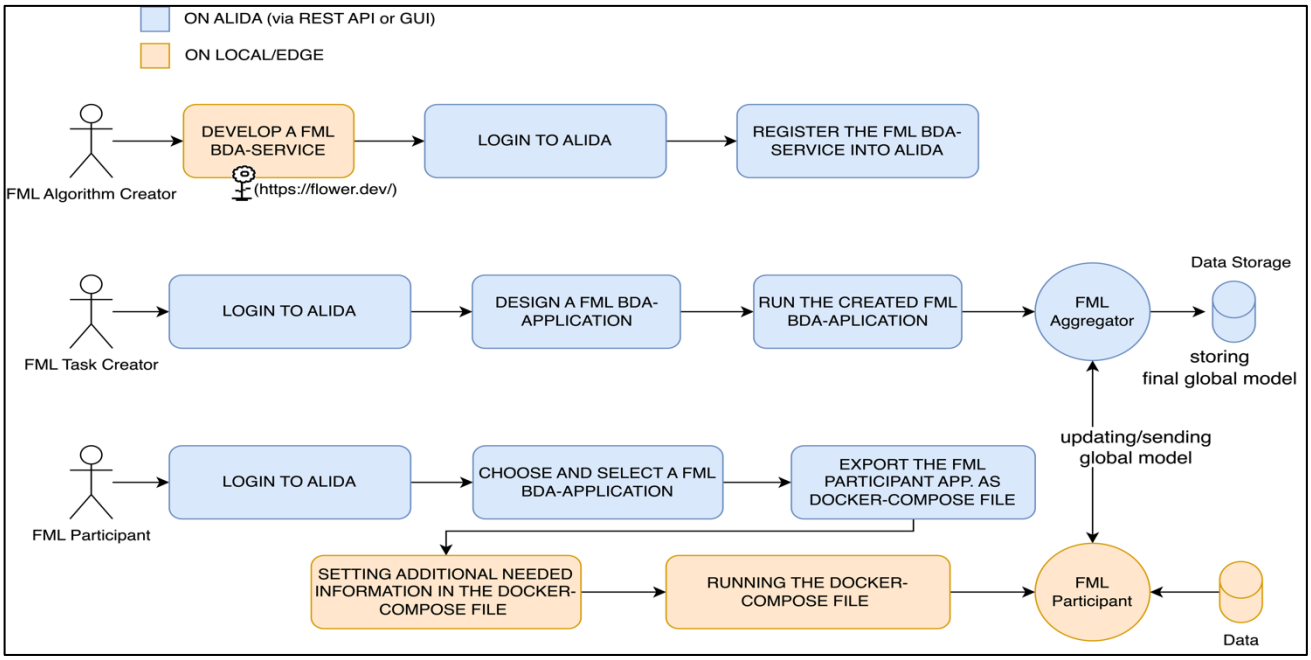

Figure 11 FML Task Flow in ALIDA Platform

FML-templates have been created within the CyberSEAS project as a guide for the development of applications based on FML and integrable within the ALIDA platform. The example provided within the template makes use of the *ScikitLearn* library, in conjunction with the FLOWER framework, to train a logistic regression type machine learning model. The FML templates were then uploaded within the project repository among the artifacts produced for task 3.4.

To summarize the FML-templates show:

- a complete example of code and instructions for starting locally, and on ALIDA, federated training using open source data.
- how to enable a secure connection between clients and the FML aggregator server using SSL certificates.
- how to enable sending messages as notifications sent by the ALIDA platform.
- how to containerize the developed applications, and as well as how to test everything locally using Docker Compose, a tool for running multi-containers applications.

Another FML-based application, built within the CyberSEAS project, is a text classification application in the social engineering area. For training, it started from an open-source Google pre-trained model (https://www.kaggle.com/models/google/nnlm/frameworks/tensorFlow2/variations/en-dim50/versions/1) which focuses on pre-processing, tokenization and embedding of sentences from simple English text. Then applying transfer learning techniques and using the TensorFlow framework for training deep neural networks, an FML application has been

implemented for classifying e-mails as legit or malicious based on the Enron (Enron Email Dataset (cmu.edu)) open-source labelled dataset. This application was then used and presented for the use case of the Finnish cluster with the company ENERIM in reference to a spear phishing attack; since e-mails are sensitive data, they are well suited for a Federated Machine Learning scenario as shown in Figure 12 below. In ALIDA, only the aggregator server of the model weights that are sent from the multiple external participating nodes (EPES operators) is thus started; FML participants will perform the actual local training close to where their data resides; this also allows multiple companies to collaborate simultaneously on their machines without centralizing the data somewhere.

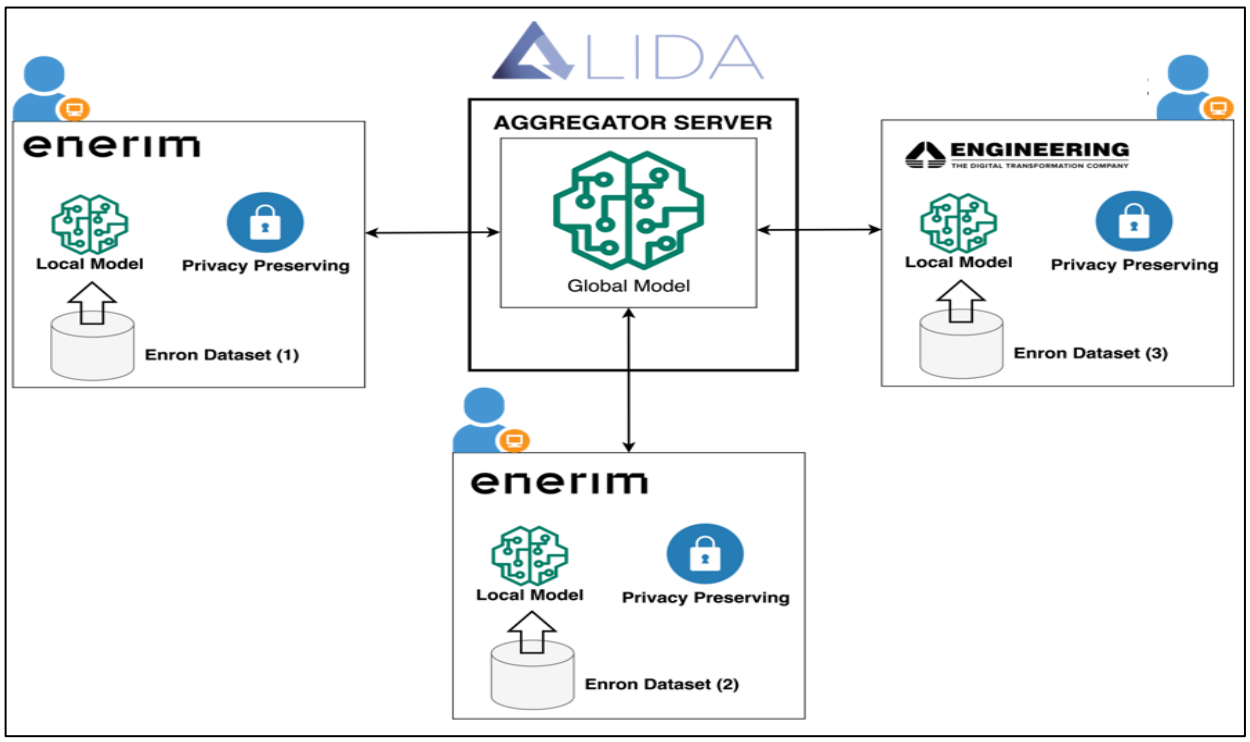

Figure 12 Spear Phishing Detection FML-training in the Finnish Use Case Pilot

Once the model is trained, it can be exported directly from the ALIDA platform for use in an external machine, or ALIDA also allows models to be deployed on the platform itself, and reachable via REST invocations using a secure HTTPS connection. In this way one or more bodies of e-mails can be sent to the model and receive as a response a score between 0 and 1 where "0" represents a legitimate e-mail, and "1" a malicious e-mail.

Figure 14 below shows the completed application in ALIDA containing the FML aggregator server and the assets that are also sent by the participating nodes themselves and transmitted to and then aggregated by the FML aggregator server such as number of participants per training rounds, confusion matrix, and other useful metrics/information to also monitor the application in real time during its execution.

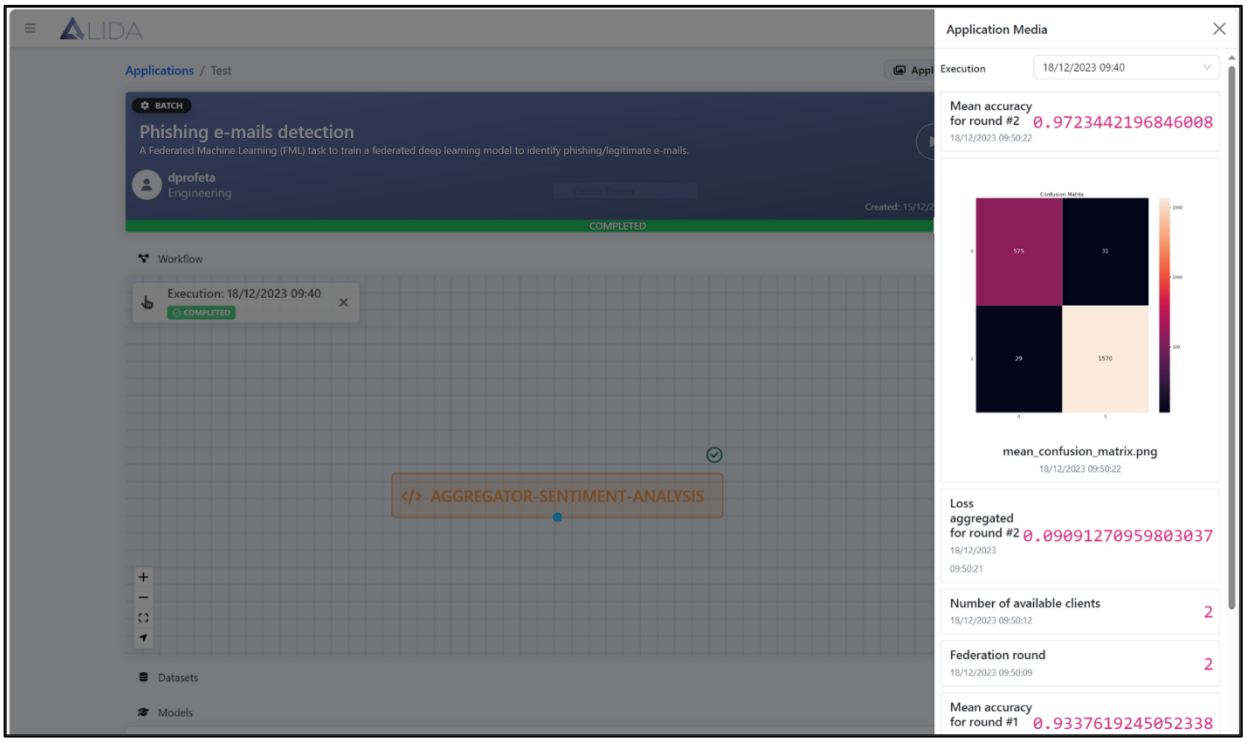

Figure 13 Spear Phishing Detection FML Aggregator Server in the ALIDA platform.

ALIDA is processing e-mail messages through ML protocols to detect offensive e-mails for cyber security threads. The e-mails used in training and also for detecting threats are private data of the operators and cannot be shared between them without a privacy conserving algorithm, so it is needed to be operated by FML algorithms.

8.2 Federated Machine Learning algorithms implemented in FML on IDS

The 'FML on IDS' is security tool offering proactive notifications, based on IDS logs. The starting point is the IDSs (Intrusion Detection Systems) which evaluate network packets and characterize them as benign (normal) or malicious.

The FML on IDS module receives current output of IDS and predicts whether there will be malicious packets in the future packets (i.e., whether there will be an attack or not). Specifically, given a window of N received packets, the model predicts the existence of a malicious packet for the next K packet. It treats IDS – based packet characterization as a time series prediction (and only not as a classification). In case of a predicted attack, a notification is generated. This way the operator can act proactively and tighten or loosen the security protection dynamically.

8.2.1 Application of FML for Proactive Notification used in FML on IDS

CyberSEAS pilots have their own infrastructures, protected by IDS, and produce their own data. Such data may not be shared as this could entail privacy/security issues. While the FML on IDS tool can operate on its own, being trained solely using its own data, a federated ML approach offers benefits (as more sources of data will be considered). The Federated ML (FML) approach allows collaboratively creating a shared model, without sharing their data, the data (IDS logs) stay in the local premises, and they are processed in the participating nodes (clients).

We have included support for privacy preserving techniques (DP in the case of FLOWER FML framework). However, as these take their toll in terms of computational efficiency and complexity imposed, the mechanism will be configured and applied according to pilot needs.

8.2.2 FML on IDS Workflow

Raw network packets offer features (46 in total) including sender IP, packet length, packet start time, which can be both numerical and categorical. In each node data pre-processing and ML training is performed, followed by the exchange of the new weights (potentially applying differential privacy) to the aggregator so that the individual weights are consolidated.

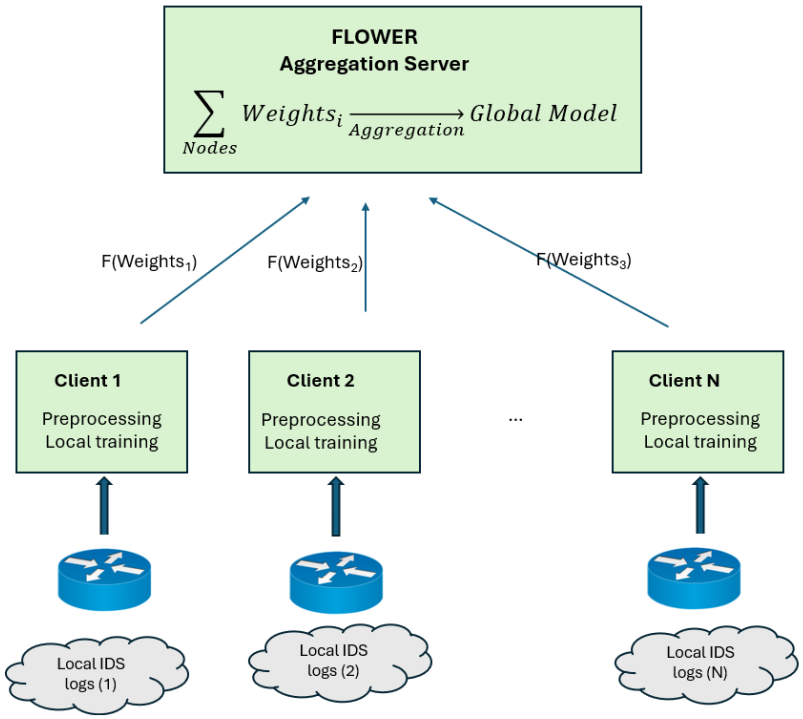

Figure 14 Integration of Flower framework with the ML on IDS

Figure 14 Integration of Flower framework with the ML on IDS depicts N clients with different local datasets and a local ML on IDS model. These models are trained on these separate datasets. The updated model is sent back to the server and the server aggregates these

models creating a global model that is sent back to the clients for the next federated round. Depending on the pilot selection and subsequent framework configuration, differential privacy may be applied upon the weights exchanged (depicted in the figure as the result of the DP function, F).

Pre-processing involves four main steps: a) Data cleaning, b) one-hot encoding, c) data scaling, and d) timeseries formatting.

- During data cleaning, we discard not-a-number (nan) and corrupted values, including erroneous values (e.g. negative packet length).
- In one-hot encoding, the categorical features are transformed into the format that can be understood by machine learning algorithms. It involves creating a new binary column for each possible value of the categorical variable, with a value of 1 in the column corresponding to the categorical value that the input data takes on, and 0 in all other columns. This results in a sparse binary matrix, where each input data point is represented by a vector of all 0's and a single 1, indicating the value of the categorical variable. An example is the parameter "service", which indicates the type of packet and can be: "dns", "http", "smtp", etc.
- Data scaling is performed using Min-Max scaler. The values of numeric variables are transformed into a common scale to ensure that variables with different units or scales of measurement do not dominate the analysis or skew the results of machine learning algorithms.
- The tabular dataset is formatted into a time-series to perform time-based analysis and forecasting. The dataset is sorted by timestamp in ascending order. After that, each row is indexed by its timestamp and the columns are reorganized so that each variable represents a series of values over time.

The Long Short-Term Memory (LSTM) model is used for time-series prediction as it provides more accurate results, after testing a) a Convolutional Neural Network (CNN) model, with 3 layers, b) a multilayer perceptron (MLP) model also with 3 layers for the same task. LSTM is a type of recurrent neural network (RNN) well-suited for time series prediction tasks. LSTM networks process sequential data and maintain a memory of past observations, allowing them to make predictions based on historical patterns in the data. This makes them well-suited for intrusion detection systems, where previous network traffic patterns can be used to identify and predict future malicious activities.

More information on the FML on IDS approach is included in Deliverable D5.7, "Proactive security for energy operators" [30] and relevant publications Time-Series Modelling for Intrusion Detection Systems [31].

The implementation of FML techniques considered here for ALIDA and FML on IDS are providing the needed privacy level and security required by critical infrastructure operators in using ML means to increase the cybersecurity resilience for EPES.

8.3 Data interchange trough Data Spaces

In today's interconnected world, existing systems are asked to fulfil increasing data-sharing requirements. The rapid expansion of data-centric applications underscoring the real value of data [32] [33] also affected smart grids and the energy supply chains. With a specific focus on energy exchange, current data exchange methods exhibit limitations, particularly when multiple stakeholders, including Transmission System Operators (TSOs) and Distribution System Operators (DSOs), need to collaborate and share sensitive information. The evolution introduced by the `Common European Dataspaces' represents a strategic response to these challenges, fostering an environment where data can be exchanged securely and efficiently while respecting privacy and data sovereignty [33] [34]. While the importance of a unified data-sharing ecosystem is evident, the energy sector faces specific privacy and security challenges that need to be addressed. As an example, the integration and exchange of data among energy stakeholders necessitates robust privacy-preserving mechanisms to prevent unauthorized access and to ensure the integrity and confidentiality of the exchanged information. This is crucial for maintaining operational security and trust within and across the energy supply chain [35]. Hence, prioritizing privacy-preserving data exchange and ensuring data sovereignty are basic.

In response to the European Commission's call for the establishment of data spaces [36], including those within the energy sector, CyberSEAS has directed the attention towards aligning with these objectives. This approach is significant for several reasons. Firstly, it emphasizes the importance of creating secure and efficient data-sharing mechanisms within the energy sector, which is crucial for ensuring energy security, optimizing resource management, and supporting the transition to sustainable energy sources. CyberSEAS contributes to the broader effort of standardizing data exchange practices across industries, enhancing interoperability, and fostering innovation. The management framework of the European Data Space is founded on European values and regulations, such as the General Data Protection Regulation (GDPR) [37] [38]. The goal of these regulations is to safeguard the movement of data within a secure setting. Organizations like the International Data Spaces Association (IDSA), GAIA-X foundation, and FIWARE, all of which are promoting the use of data-centric technologies for achieving data sovereignty are guiding this technological evolution. From a technical standpoint, as shown in Figure 10, the development of a data space relies on multiple fundamental components. These elements collectively ensure a secure, effective, and interoperable platform for data sharing:

- Policies and Regulations are at the core of a data space, defining the legal and regulatory landscape within which it operates. This includes adherence to privacy laws, data protection standards, and compliance requirements, ensuring ethical and responsible data handling. An important aspect of this component is self-descriptions, which allow data sources to provide metadata about the data they offer. This metadata includes descriptions of data content, quality, and any applicable usage restrictions, fostering transparency and trust among participants.
- The Shared Vocabulary ensures that all participants have a consistent understanding and interpretation of data across different systems and domains. This is achieved through standardized data models, formats, and terminologies, facilitating interoperable data exchange.
- Certificates contribute to the security framework, enabling authentication and encryption to safeguard data exchanges. The management of these certificates,

including issuance and revocation, is critical for maintaining a secure communication environment.

Another important aspect is the definition of key roles within the data space, these include Providers, who supply data, and Consumers, who utilize this data. These roles come with specific responsibilities, rights, and obligations. Providers are tasked with ensuring the quality and integrity of their data, while Consumers must comply with usage policies and respect data privacy. Beyond these, there are Brokers, who assist in data discovery and access; Service Providers, offering tools and services for data processing; and Regulators, ensuring compliance with policies and regulations. Additionally, Data Custodians play a crucial role in managing and safeguarding data, and Auditors oversee adherence to standards and policies, ensuring accountability and transparency.

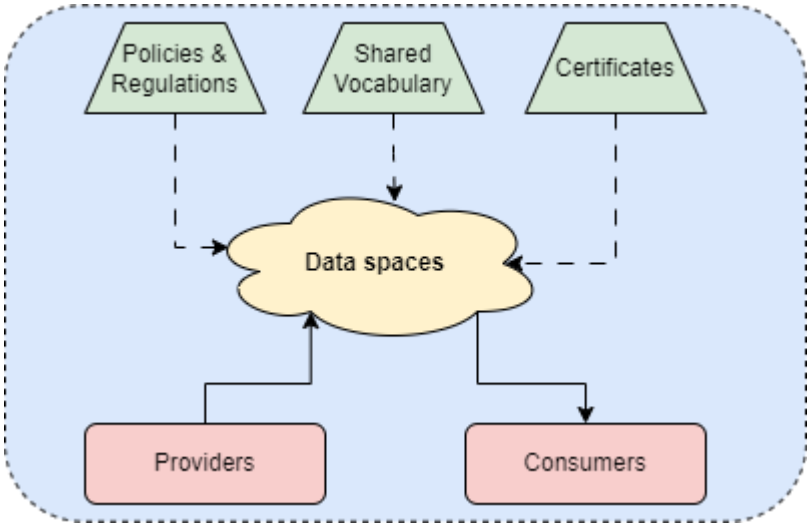

Figure 15 Dataspace High Level Overview

The primary aim of this section is to elucidate the concept of a dataspace. It seeks to address questions such as what defines a dataspace, the requirements for establishing a dataspace, and the crucial mechanisms that support the creation of privacy-enhancing techniques for data exchange.

- **What a Dataspace is.**

A dataspace is an open ecosystem facilitating data sharing and accessibility among different entities. This shift towards dataspaces relies on principles of transparency and trust that govern these ecosystems. Traditional data exchange methods face numerous challenges: a primary concern dataspace seek to mitigate is the complexities stakeholders experience when establishing legal frameworks for collaboration.

Stakeholders across vital sectors, like energy, encounter obstacles in creating contracts and establishing reliable data-sharing policies, hindering broader participation and innovation due to legal complexities. Conventional data exchange lacks full control over post-

exchange data, posing risks in scenarios where data governance is crucial, potentially resulting in financial losses.

- **What a Dataspace Requires.**

To establish a collaborative and open environment for data sharing, developing a trusted ecosystem where each participant is recognized, has assigned roles, and is authorized for dataspace activities, is essential. Techniques ensuring privacy-preserving data exchange, authentication, authorization, and overall security are vital, as highlighted in the European Claim for dataspaces. For this reason, dataspaces are designed to ensure data sovereignty, providing a framework where data owners maintain control over the usage and sharing of their data. This is a key concept in establishing trust and encouraging more entities to participate in data sharing, as it ensures the respect of their data rights and privacy. In a dataspace, ensuring compliance with regulations and ethical standards is vital, alongside an interoperable infrastructure supporting data sharing across diverse systems, achieved through common standards, vocabulary, and protocols.

- **Privacy-Preserving Data Exchange**.

In the dataspace paradigm, data exchange is enabled through connectors, which can be deployed on-premises or in a cloud environment, primarily using helm charts and Kubernetes clusters, following an architecture ensuring security mechanisms. As depicted in Figure 11, establishing the data marketplace requires, among others, a Certification Authority (CA) and a shared vocabulary.

The former ensures that different stakeholders can be identified and authorized to participate in the marketplace, while the latter enables participants to comprehend a shared language. This common understanding is essential for facilitating machine-to-machine (M2M) communication and simplifying the creation of privacy-preserving policies. From a technical perspective, it is also essential to guarantee the minimum requirements needed for stakeholders' computing nodes, verify the level of security provided (e.g., Trusted Execution Environment support, and confirm their geographical locations. Stakeholders can publish descriptions of their data offerings on a data broker, while developers can provide applications that utilize this data to create added-value services.

All transactions between different connectors are recorded by a clearing house, to ensure the accurate processing of payments and data exchanges. Examples of policy enforcement in dataspaces include restrictions on the duration of data usage, the rights to view and utilize data, and the conditions under which data may be shared or processed. For instance, policies might dictate that certain data can only be accessed for a limited time or specify that data must not be transferred to unauthorized parties. Additionally, policies can enforce data anonymization or de-identification before it is shared to protect privacy. These rules ensure that all data handling within the dataspace adheres to agreed-upon ethical and legal standards, fostering a secure and trusted environment for all participants.

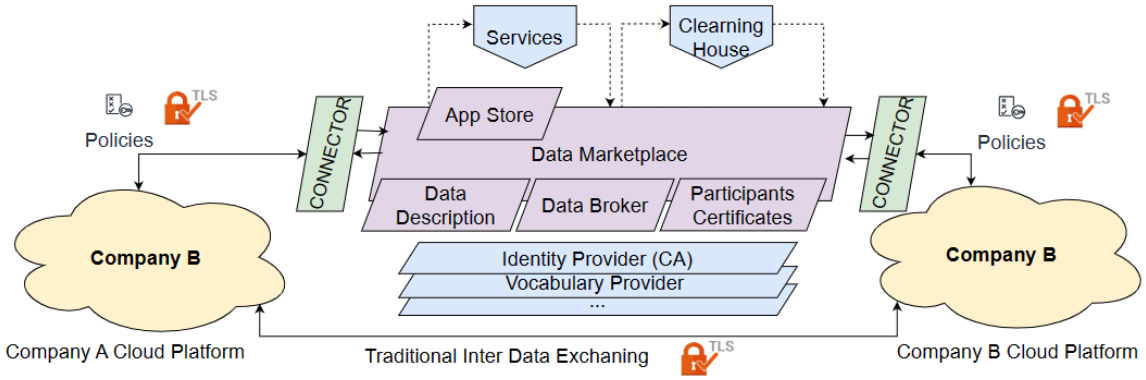

Figure 16 Dataspace-based Data Exchanging

8.4 CTI informations exchange trough MISP protocol in CyberSEAS project

The purpose of MISP is to enable organizations and SOCs to share threat intelligence on completed cases or events, such as IoCs and other artefacts, in real time to help each other prevent cyber-attacks. Organizations and SOCs are connected through their participation in communities. Figure 17 CTI sharing with communities presents the concept of CTI sharing with communities.

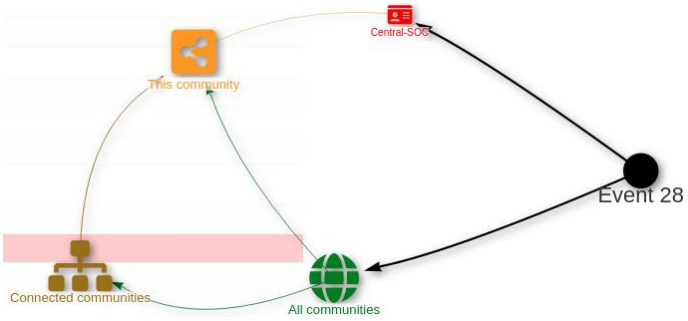

Figure 17 CTI sharing with communities through MISP [34]

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. For example, SI-CERT follows several data

feeds for systems in Slovenia that show newly discovered vulnerabilities or unusual behaviour that may be the result of cybersecurity incidents. However, SI-CERT encourages Operators of Essential Services (OESs) and other entities, such as government 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. This requires appropriate authentication. Authentication keys are used 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.

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 and demonstrated in the SLO&CRO pilot by INF and SI-CERT. Here, we describe its design briefly to show the concept of IoC exchange and utilisation based on the MISP protocol. Please refer to the D6.8 deliverable for details as the main purpose of this approach is to establish and propose a standard procedure for the coordination between SOCs and CERTs.

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 synchronised. 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.

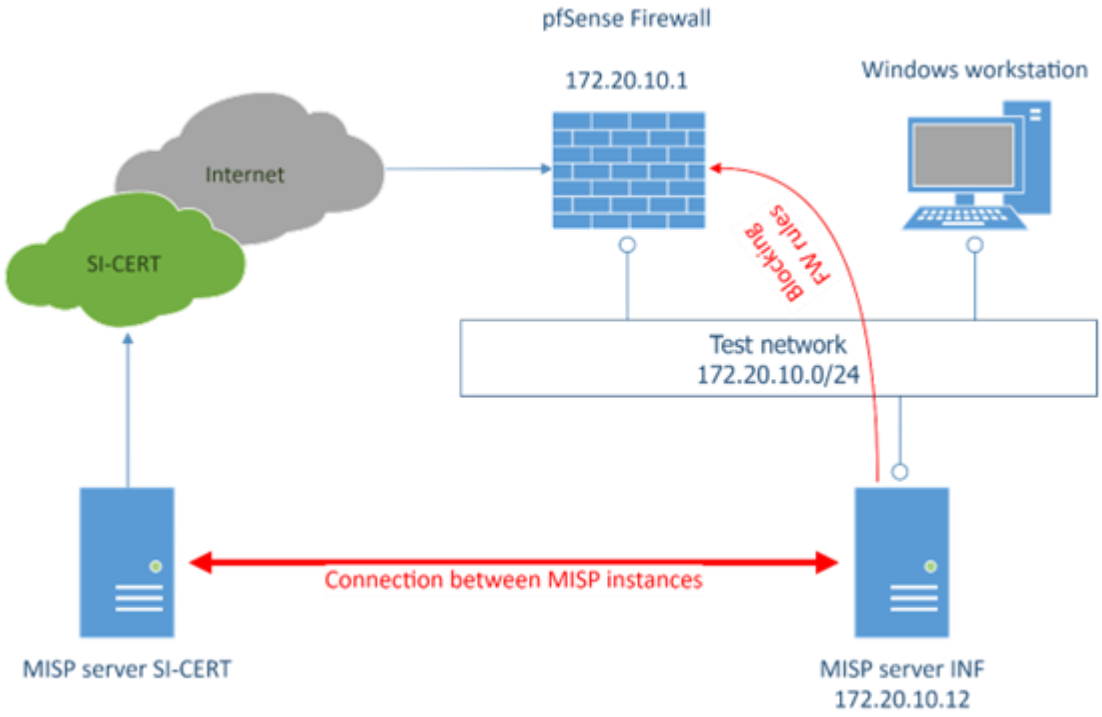

Figure 18 Architecture for communication trough MISP in SLO&CRO and national CERT [34]

This procedure demonstrated 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 (Slovenian National Plan for Cyber Incident Response) object is defined and implemented. It includes attributes, such as reference number, subject, reporting organisation, reporter name, 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.

In the CyberSEAS project for CTI Sharing between operators 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 consist of a simulated remote MISP instance, playing the role of outside MISP parthers that SI-CERT is exchanging data with and playes 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, that is exchanging data with EPES local partners.

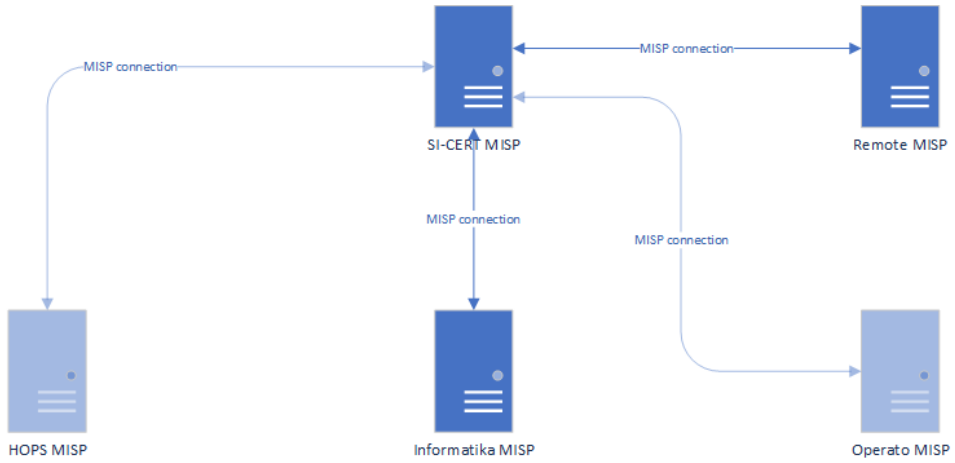

Figure 19 CyberSEAS internal MISP infrastructure [34]

8.4.1 MISP and SAPPAN

SAPPAN is a capturing tool that utilises playbook management. Users can create, modify, delete, convert, search, share, and view playbooks and their resources in the capturing tool. Playbook is a (partially) executable incident response procedure. It includes several sequential and/or parallel steps that contain certain levels of detail. The more details are provided, the higher level of automation can be achieved. With few details, a step or action is merely descriptive. The CACAO format is supported by SAPPAN to increase the level of possible details and automation. The BPMN notation is also utilised for the visualisation of playbooks. This graphical representation is widely used in different fields, including security response and recovery.

In the GUI (Graphical User Interface) of the SAPPAN capturing tool, an operator can navigate through the steps and modify their detailed information. The playbooks can be viewed in the knowledge base, exported to JSON format, or shared via the MISP platform. The connection to the STIX platform is also considered, but it still has not been developed.

In addition to playbook management and visualisation, several key functionalities are relevant for playbooks: playbook execution, playbook sharing, CTI exchange, SIEM (Security Information and Event Management) integration and analysis, reporting facilities, and collaboration and work coordination facilities. These 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 standardised 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 the members of the community 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 standardised incident response procedure suited to a specific type of cyber-attack. It can hence 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 the steps to exchange CTI information on the identified IoCs and to 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.

For more details on the integration of MISP and SAPPAN, the reader is encouraged to refer to the deliverable D6.8 [39].

8.5 CTI data transfer from CVIAT tool using STIX format

The Common Vulnerability Assessment Tool (CVIAT) enhances data transferability, interoperability, and standardization for cyber threat intelligence, among its functionalities, by supporting the export of cyber threat data into the STIX format, a widely adopted standard in this domain. This feature facilitates collaboration and information sharing within the cybersecurity community (either within a specific organization or among different organizations/authorities), with contribution in the implementation and maintenance of more secure systems.

Data from CVIAT is exported as STIX objects, utilizing a bundle object to collect all the STIX Domain Objects and Relationships. Specifically, CVIAT exports its data by making the following assumptions, following STIX Documentation [40] [30] on STIX Domain Object(SDO) and STIX Domain Relationship(SRO)

Identity SDO:

Identity is a STIX Domain Object that is used to relate the Organization in which the users work, for example, a company. In each bundle that holds the objects, there is only one Identity, and it has an identity_class equal to organization. Other properties that provide informational context for the Organization are the unique id, a name, and a description. The Identity is responsible for the correlation of the asset instances that were reported and their reporter.

Infrastructure SDO:

Asset Instances are represented as Infrastructures in STIX Vocabulary. STIX supports infrastructure Domain Objects, and they mainly refer to technology resources, such as hardware, software, and network devices. In our case, an infrastructure is something more general that can act on Information, Human, Business, Communication, PES Component, Functional and IM Component assets. These infrastructure types (asset classes), as well as the infrastructures themselves (assets) are represented as asset_class and asset custom properties. The Infrastructure object has several properties including a unique id, a name that describes the particular asset, a short description, a revoked property which defines if the asset is active or inactive (False/True value accordingly), and a created_by_ref property that includes an identity STIX object used to represent the Organization who created the infrastructure object.

Vulnerability SDO:

In CVIAT, it is described the vulnerability instances that an asset instance has, and this is encoded in STIX as the vulnerability Domain Object. As it is described above, the infrastructures are not limited to technical components and therefore their vulnerabilities have not only Cyber, but also Physical and Human/Organizational aspects. These aspects constitute the vulnerability types or classes that are encoded into the custom vulnerability_class property of the vulnerability object. Additionally, the vulnerability property is referred to the known vulnerability that this instance is about. To get more information about this vulnerability instance there is a unique id, a name, a description, an x_cvss property and some external_references. The x_cvss is a custom made property, used to describe all the scores of a vulnerability based on the Common Vulnerability Scoring System (CVSS 4.0). It is defined as a list of score objects, each one of them having as sub properties the basic metrics that are used to calculate the CVSS Score. External references are related to the source where the vulnerability was reported and are defined by the sub properties source_name, in which it is mentioned the source that reported the vulnerability and a custom default description. This helps provide additional context for the Vulnerability Domain object.

Relationship SRO:

STIX predefined relationship 'has' is used between Vulnerability Instances and Infrastructures (Asset Instances) to connect each vulnerability with an infrastructure. The relationship is directed from the Infrastructure to the Vulnerability, indicating that an Infrastructure has some Vulnerability objects. This approach allows us to understand the impact of a vulnerability on an asset and helps us to prioritize remediation efforts. The 'has' relationship consists of the source_ref and a target_ref that relate the Infrastructure and the Vulnerability accordingly.

In conclusion, the STIX modelling provides a structured and standardized way to represent asset instances, identities, and vulnerabilities in our software system. It allows us to provide context for each object and establish relationships between objects to better understand the risk posed by vulnerabilities to our assets.

Below, it is provided an example of a STIX bundle object that was exported from CVIAT into a json file:

Table 4 JSON file from CVIAT formatted in STIX.


```
{
  "type":"bundle",
  "id":"bundle--609e7678-8cf6-4086-a838-c8b31e8c03a7",
  "objects":[
```

```
{
"type":"infrastructure",
"spec_version":"2.1",
"id":"infrastructure--79d0f582-95e2-4501-a277-0e3aa6f804c5",
"created_by_ref":"identity--ccb656e9-53f0-4b6c-8f43-cf5ce27c3c24",
"created":"2024-01-12T10:36:19.996061Z",
"modified":"2024-01-12T10:36:19.996077Z",
"name":"Database - possibility to manipulate data",
"description":"Possibility to destroy metering data due to elevated rights",
"revoked":false,
"asset":"Access Rights Management Mechanism",
"asset_class":"Functional"
},
{
"type":"infrastructure",
"spec_version":"2.1",
"id":"infrastructure--157dd4b8-c664-4752-8dd1-fa4e7c4b2015",
"created_by_ref":"identity--ccb656e9-53f0-4b6c-8f43-cf5ce27c3c24",
"created":"2024-01-12T10:46:42.493545Z",
"modified":"2024-01-12T10:46:42.493560Z",
"name":"MS Defender Firewall",
"description":"Antivirus software",
"revoked":false,
"asset":"Antivirus Scanning Software",
"asset_class":"Functional"
},
{
"type":"infrastructure",
"spec_version":"2.1",
"id":"infrastructure--b53b3219-f90f-4b1f-9a01-a5c310d5725c",
"created_by_ref":"identity--ccb656e9-53f0-4b6c-8f43-cf5ce27c3c24",
"created":"2024-01-12T10:52:17.613380Z",
"modified":"2024-01-12T10:52:17.613396Z",
"name":"Customer support",
"description":"Human factor - phishing",
"revoked":false,
"asset":"Customer service operator",
"asset_class":"Human"
},
{
"type":"vulnerability",
"spec_version":"2.1",
"id":"vulnerability--1dbed00b-b05c-452c-840c-4928afcab7cb",
"created":"2024-01-12T10:37:48.001770Z",
"modified":"2024-01-12T10:37:48.001796Z",
"name":"An attacker has access to all the data of an employee's account taking advantage of the use of weak password",
"description":"Malicious act",
"revoked":false,
"external_references":[
{
"source_name":"NIW",
"description":"This is a vulnerability created by NIW"
}
],
"vulnerability":"An attacker has access to all the data of an employee's account taking advantage of the use of weak password",
"vulnerability_class":"Cyber",
"x_cvss":[
{
"score_id":"aad9c49c-46ac-407f-9341-b759b39628d5",
"name":"name",
"description":"",
"created":"2024-01-12T10:42:52.593915Z",
"vulnerability_instance":"4804d667-7dbb-4a26-8f48-ea97a885c5f0",
"attack_vector":"N",
"attack_complexity":"H",
"attack_requirements":"P",
"privileges_required":"H",
"user_interaction":"N",
"vulnerable_system_confidentiality":"H",
"vulnerable_system_integrity":"H",
"vulnerable_system_availability":"N",
"subsequent_system_confidentiality":"H",
"subsequent_system_integrity":"H",
"subsequent_system_availability":"N",
"score":8.7,
"qualitative_score":"H"
}
]
},
{
"type":"vulnerability",
"spec_version":"2.1",
"id":"vulnerability--aba39511-ba04-4177-8fa3-d1fe4e725627",
"created":"2024-01-12T10:47:36.283958Z",
"modified":"2024-01-12T10:47:36.283973Z",
"name":"Poorly configured firewall",
"description":"Firewall failure.",
"revoked":false,
"external_references":[
{
"source_name":"ITC",
"description":"This is a vulnerability created by ITC"
}
],
```

```
"vulnerability":"Poorly configured firewall",
"vulnerability_class":"Cyber",
"x_cvss":[
{
"score_id":"6db97806-4f63-4d41-83ec-897927b7119f",
"name":"name",
"description":"",
"created":"2024-01-12T10:49:29.527486Z",
"vulnerability_instance":"7c6cab88-1241-423f-b8de-a57317a8f8a0",
"attack_vector":"P",
"attack_complexity":"L",
"attack_requirements":"N",
"privileges_required":"N",
"user_interaction":"N",
"vulnerable_system_confidentiality":"N",
"vulnerable_system_integrity":"L",
"vulnerable_system_availability":"L",
"subsequent_system_confidentiality":"N",
"subsequent_system_integrity":"L",
"subsequent_system_availability":"L",
"score":2.4,
"qualitative_score":"L"
}
]
},
{
"type":"vulnerability",
"spec_version":"2.1",
"id":"vulnerability--637e6517-3d7d-4023-be92-77499823ca06",
"created":"2024-01-12T10:53:18.145286Z",
"modified":"2024-01-12T10:53:18.145306Z",
"name":"Inadequate Security Training and Awareness Program",
"description":"Company policy of security training.",
"revoked":false,
"external_references":[
{
"source_name":"SCC",
"description":"This is a vulnerability created by SCC"
}
],
"vulnerability":"Inadequate Security Training and Awareness Program",
"vulnerability_class":"Human_Organizational",
"x_cvss":[
{
"score_id":"2c4a4a1a-6d97-4033-a50a-48c85adee6f8",
"name":"name",
"description":"",
"created":"2024-01-12T10:56:49.683791Z",
"vulnerability_instance":"21fbb777-4e6f-404e-a857-b27b4dae8069",
"attack_vector":"P",
"attack_complexity":"L",
"attack_requirements":"N",
"privileges_required":"N",
"user_interaction":"N",
"vulnerable_system_confidentiality":"L",
"vulnerable_system_integrity":"N",
"vulnerable_system_availability":"N",
"subsequent_system_confidentiality":"N",
"subsequent_system_integrity":"N",
"subsequent_system_availability":"N",
"score":2.4,
"qualitative_score":"L"
}
]
},
{
"type":"vulnerability",
"spec_version":"2.1",
"id":"vulnerability--351c1ea5-be22-4104-9cf9-29b1f43c3a98",
"created":"2024-01-12T10:54:07.268376Z",
"modified":"2024-01-12T10:54:07.268390Z",
"name":"Human error in adherence to policies and procedures",
"description":"Company policy of procedures.",
"revoked":false,
"external_references":[
{
"source_name":"NES",
"description":"This is a vulnerability created by NES"
}
],
"vulnerability":"Human error in adherence to policies and procedures",
"vulnerability_class":"Human_Organizational",
"x_cvss":[
{
"score_id":"68f4646e-a2b2-4eca-84dc-57ba9f535785",
"name":"name",
"description":"",
"created":"2024-01-12T10:56:04.145753Z",
"vulnerability_instance":"34c95199-ae0d-4e53-929a-ba8d52766a0f",
"attack_vector":"A",
"attack_complexity":"L",
"attack_requirements":"P",
"privileges_required":"H",
"user_interaction":"A",
```

```
            "vulnerable_system_confidentiality":"H",
            "vulnerable_system_integrity":"H",
            "vulnerable_system_availability":"N",
            "subsequent_system_confidentiality":"L",
            "subsequent_system_integrity":"L",
            "subsequent_system_availability":"N",
            "score":5.3,
            "qualitative_score":"M"
            }
            ]
            },
            {
            "type":"identity",
            "spec_version":"2.1",
            "id":"identity--ccb656e9-53f0-4b6c-8f43-cf5ce27c3c24",
            "created":"2024-01-12T11:06:50.312985Z",
            "modified":"2024-01-12T11:06:50.312985Z",
            "name":"ENERIM                                                                                    (test)",
            "description":"ENERIM                              (for                          testing                          purposes)",
            "identity_class":"organization",
            "revoked":false
            },
            {
            "type":"relationship",
            "spec_version":"2.1",
            "id":"relationship--c2c025f1-2e4f-464c-8e94-9ec2dee2d1dd",
            "created":"2024-01-12T10:37:48.001770Z",
            "modified":"2024-01-12T10:37:48.001796Z",
            "relationship_type":"has",
            "source_ref":"infrastructure--79d0f582-95e2-4501-a277-0e3aa6f804c5",
            "target_ref":"vulnerability--1dbed00b-b05c-452c-840c-4928afcab7cb",
            "revoked":false
            },
            {
            "type":"relationship",
            "spec_version":"2.1",
            "id":"relationship--7307ce19-15ad-46d3-a693-f5c39b2b2208",
            "created":"2024-01-12T10:47:36.283958Z",
            "modified":"2024-01-12T10:47:36.283973Z",
            "relationship_type":"has",
            "source_ref":"infrastructure--157dd4b8-c664-4752-8dd1-fa4e7c4b2015",
            "target_ref":"vulnerability--aba39511-ba04-4177-8fa3-d1fe4e725627",
            "revoked":false
            },
            {
            "type":"relationship",
            "spec_version":"2.1",
            "id":"relationship--6d0181a5-008e-4791-a07d-92901ae2ef2d",
            "created":"2024-01-12T10:53:18.145286Z",
            "modified":"2024-01-12T10:53:18.145306Z",
            "relationship_type":"has",
            "source_ref":"infrastructure--b53b3219-f90f-4b1f-9a01-a5c310d5725c",
            "target_ref":"vulnerability--637e6517-3d7d-4023-be92-77499823ca06",
            "revoked":false
            },
            {
            "type":"relationship",
            "spec_version":"2.1",
            "id":"relationship--85eba388-bcde-4bc7-a7f5-bff10528c13b",
            "created":"2024-01-12T10:54:07.268376Z",
            "modified":"2024-01-12T10:54:07.268390Z",
            "relationship_type":"has",
            "source_ref":"infrastructure--b53b3219-f90f-4b1f-9a01-a5c310d5725c",
            "target_ref":"vulnerability--351c1ea5-be22-4104-9cf9-29b1f43c3a98",
            "revoked":false
            }
  ]
}
```


From the JSON file, formatted in STIX in Table 4, the following information can be extracted:

1. Identity: from the object of type identity, it can be concluded that this bundle holds information for an organization (identity class = organization) named *ENERIM (test)*


```
{
            "type":"identity",
            "spec_version":"2.1",
            "id":"identity--ccb656e9-53f0-4b6c-8f43-cf5ce27c3c24",
            "created":"2024-01-12T11:06:50.312985Z",
            "modified":"2024-01-12T11:06:50.312985Z",
            "name":"ENERIM (test)",
            "description":"ENERIM (for testing purposes)",
            "identity_class":"organization",
            "revoked":false
            },
```

2. Infrastructure: the sum of the objects of type infrastructure refers to the assets that are vulnerable for the specific identity that created the bundle file. For example, the first vulnerable asset is called *Database - possibility to manipulate data* it belongs to the type of *Access Rights Management Mechanism* and to the class *Functional*, it not revoked (revoked = False), which means it is an active asset on their domain.


```
{
          "type":"infrastructure",
          "spec_version":"2.1",
          "id":"infrastructure--79d0f582-95e2-4501-a277-0e3aa6f804c5",
          "created_by_ref":"identity--ccb656e9-53f0-4b6c-8f43-cf5ce27c3c24",
          "created":"2024-01-12T10:36:19.996061Z",
          "modified":"2024-01-12T10:36:19.996077Z",
          "name":"Database - possibility to manipulate data",
          "description":"Possibility to destroy metering data due to elevated rights",
          "revoked":false,
          "asset":"Access Rights Management Mechanism",
          "asset_class":"Functional"
          },
```


3. Vulnerability: the sum of the objects of type vulnerability refer to the vulnerabilities, denoting the weaknesses of each asset. For example, the first assessed vulnerability that the bundle file holds is called *An attacker has access to all the data of an employee's account taking advantage of the use of weak password*, it belongs to the class of *Cyber*. This vulnerability is assessed with CVSS 4.0 scoring system, and this object presents all the metrics given for the calculation of the score (e.g. *attack_vector":"N"*).


```
{
          "type":"vulnerability",
          "spec_version":"2.1",
          "id":"vulnerability--1dbed00b-b05c-452c-840c-4928afcab7cb",
          "created":"2024-01-12T10:37:48.001770Z",
          "modified":"2024-01-12T10:37:48.001796Z",
          "name":"An attacker has access to all the data of an employee's account taking advantage of the use of weak password",
          "description":"Malicious                                                                                                act",
          "revoked":false,
          "external_references":[
          {
          "source_name":"NIW",
          "description":"This          is          a          vulnerability          created          by          NIW"
          }
          ],
          "vulnerability":"An attacker has access to all the data of an employee's account taking advantage of the use of weak
password",
          "vulnerability_class":"Cyber",
          "x_cvss":[
          {
          "score_id":"aad9c49c-46ac-407f-9341-b759b39628d5",
          "name":"name",
          "description":"",
          "created":"2024-01-12T10:42:52.593915Z",
          "vulnerability_instance":"4804d667-7dbb-4a26-8f48-ea97a885c5f0",
          "attack_vector":"N",
          "attack_complexity":"H",
          "attack_requirements":"P",
          "privileges_required":"H",
          "user_interaction":"N",
          "vulnerable_system_confidentiality":"H",
          "vulnerable_system_integrity":"H",
          "vulnerable_system_availability":"N",
          "subsequent_system_confidentiality":"H",
          "subsequent_system_integrity":"H",
          "subsequent_system_availability":"N",
          "score":8.7,
          "qualitative_score":"H"
          }
          ]
```

```
        },
```

9 CyberSEAS project secure and privacy preserving data exchange.

9.1 CyberSEAS involved operators for data exchange.

The operators from the CyberSEAS project are mainly the partners in project. A description of the partners in project will follow. The main focus is on the Energy operators involved in project that are TSOs, data operators from energy industry, cybersecurity organisations.

9.1.1 Engineering Ingegneria Informatica SpA

ENGINEERING Ingegneria Informatica S.p.A. (ENG) is the head company of the ENGINEERING Group. Founded in 1980, Engineering became the first IT group in Italy and among the top 10 IT groups in Europe, with 12,000 professionals in 65 locations in Europe, South and North America (Italy, Belgium, Germany, Norway, Republic of Serbia, Spain, Sweden, Switzerland, Brazil, Argentina, and United States) and a consolidated revenue portfolio in 2019 of about 1.27 billion Euros. The Engineering Group serves clients in more than 20 countries, designing, developing, and implementing innovative solutions for all major business areas in which digitalization has or will have the biggest impact. Engineering operates through sector focused business units: Digital Finance, Smart Government, Local Government and e-Health, Smart Energy & Utilities, Digital Industry and Telecoms, delivering innovative IT solutions to main vertical markets: Aerospace, Insurance, Automotive, Banks, Consumer Products, Defence and Aerospace, Energy & Utilities, Training, Central & Local Government, Homeland Security, Life Science, Manufacturing, Media, International Organisation, Retail, Healthcare, Telecommunications, Transports, Welfare. Across these markets, the group designs and delivers IT innovation to more than 1000 large accounts, with a complete offer combining system and business integration, outsourcing, cloud services, consulting, deployed around both open and proprietary solutions. The Group also has a strong presence in the outsourcing and cloud computing market via an integrated network of 4 data centres located in Pont-Saint-Martin, Turin, Vicenza, and Milan, exploiting its own infrastructure continuously updated to reflect the best technological, quality and security standards. ENGINEERING Data Centres offer business continuity and IT infrastructure management to 21000 servers and 250000 workstations. The unique combination of services and hosting capability combined with the European based hosting infrastructure position ENGINEERING as a prime choice for its client base.

9.1.2 Consorzio Interuniversitario Nazionale per l'Informatica (CINI)

CINI is a research consortium founded in 1989 as a no-profit organization to foster the cooperation of Italian computer scientists and engineers in nation-wide and international projects in the area of Information and Communication Technology (ICT). It currently

comprises the main Italian universities with Computer Engineering and Computer Science departments. The Research Team, which will be contributing to the project, is the Fault and Intrusion Tolerant Networked SystemS (FITNESS) Research Group (http://www.fitnesslab.eu/), located in Naples, Italy, which consists of researchers who are currently at the University of Naples Parthenope.

9.1.3 Airbus Cybersecurity GmbH

As part of the Airbus Defence and Space, which is a worldwide leader in global security solutions and systems, providing Lead Systems Integration and value-added products and services to civil and military customers around the globe, the Airbus Cybersecurity is entirely dedicated to cyber security as a "pure player" aiming at protecting governments, national agencies, strategic industries, and critical infrastructure from increasingly sophisticated cyber threats. Operating worldwide, with offices in the UK, France, Germany, Middle East and North America, Airbus Cybersecurity provides high grade cyber security solutions and services to its customers. The German Legal entity "Airbus Cybersecurity GmbH" mainly works on industrial cyber security (OT risk assessment, OT Security Operations Center setup, transition, and operations) and general cyber security services (cyber defence professional services and managed security services) for Airbus itself and for the external customers in Germany.

9.1.4 Fraunhofer-Gesellschaft

The Fraunhofer-Gesellschaft is the leading organization for applied research in Europe. Its research activities are conducted by 72 institutes and research units at locations throughout Germany. The Fraunhofer-Gesellschaft employs a staff of more than 26,600, who work with an annual research budget of 2.6 billion euros. Of this sum, 2.2 billion euros is generated through contract research. Around 70 percent of the Fraunhofer-Gesellschaft's contract research revenue is derived from contracts with industry and from publicly financed research projects. International collaborations with excellent research partners and innovative companies around the world ensure direct access to regions of the greatest importance to present and future scientific progress and economic development. Fraunhofer is a founding member of the Big Data Value Association (BDVA) and the International Data Spaces Association (IDSA), each having more than 100 members with a strong representation of European industry. For more than 35 years, the Fraunhofer Institute for Applied Information Technology FIT has been conducting R&D on user-friendly smart solutions that blend seamlessly in business processes. Our clients benefit from more efficient processes and increased quality, internal connectivity, and staff satisfaction. In the field of AI and data technologies, Fraunhofer FIT bundles competences in semantic technologies, distributed as well as centralised data management and analytics, as well as process mining. Regarding data hubs, FIT has a leading role in the International Data Spaces (IDS) activities, including the role of component owner of the app store and information model components of the IDS Reference Architecture. Fraunhofer FIT cooperates with RWTH Aachen in the development of a new Center called Digital Energy Aachen with the goal to support energy industry in the transition to a digital economy. Thanks to this alliance, FIT is extending its experience in the field of data management in the energy field using the large experience built in other fields such as Health or Industry.

9.1.5 Guardtime OÜ

Guardtime OÜ is a system engineering company, with deep experience in data-centric cyber security solutions and is heavily engaged in R&D in hash-based cryptography. Guardtime's core technology - KSI Blockchain® - is designed to provide massively scalable digital signature-based authentication for electronic data, machines, and humans. Guardtime has a team of cryptographers, developers, and security architects. Guardtime's offices are located in Estonia (Tallinn, Tartu), Netherlands (Amsterdam), Switzerland (Lausanne), United States (Irvine, CA and Alexandria, VA), United Kingdom (Guildford) and Singapore. Established in 2007 in Estonia, Guardtime's largest office with its core R&D division and development teams are located in Tallinn (EE) and Tartu (EE). With over 40 patents filed and more pending, Guardtime has a proven track record in transforming foundational research into practical solutions. With product deployments in Europe, Middle East, Asia, and the Americas, Guardtime provides data-centric cyber security solutions for verticals such as governance, healthcare, insurance, telecommunications, energy, and defence. In the energy and cybersecurity domain, Guardtime has conducted several cyber exercised to critical infrastructure and nuclear power plants. We are developing cyber security and privacy solutions to smart grids operated by TSO. Guardtime is a technology and cyber security solutions provider to large telecom operators (Ericsson, Verizon) and Defence sector (Lockheed Martin).

9.1.6 IKERLAN

IKERLAN (IKE) is a private non-profit Technological Research Centre in the North of Spain, with a vocation for public service. IKE is a point of reference for innovation and comprehensive product development. IKE works closely with companies to improve their competitiveness, through the application of technological knowledge to develop innovative products and new tools and methodologies for implementation in design and production processes. It has a staff of more than 300 qualified researchers and engineers, with experience in interdisciplinary work and capable of tackling complex problems. From its creation in 1974, IKE has maintained close relations with companies from the machinery and capital goods, domestic appliance, electronics and computing, automotive and energy sectors. As a centre of excellence in the transfer of technology, more than 800 R&D projects were completed so far in cooperation with companies, developing new products and implementing customized systems in design and manufacturing processes.

9.1.7 INFORMATIKA

INFORMATIKA is a development-oriented company and a trusted business partner in the electric power distribution environment in Slovenia. It has 40 years of experience in the development of ICT solutions and in providing services to different customers, primarily DSOs (Distribution System Operators). By using modern information technologies, the company supports customers in achieving the best possible, secure, and transparent business operations assuring optimal costs. The synergy between related businesses and possible new market opportunities is always taken into consideration. The company offers complete solutions that are custom tailored to meet the needs of customers. INFORMATIKA has a deep knowledge and a wide portfolio of products that pertain to the electricity grid, energy

consumption metering and billing, supply chains of electricity related products and services, data exchange and processes in the energy sector, and cybersecurity of critical utility infrastructures, particularly related to DSOs. It can hence contribute to all goals and use cases of the proposal, including cybersecurity governance, coherent cross organisational security in cooperative energy utility systems, data security within specific ecosystems and on the level of electronic data exchange, as well as security models and technologies that span complete business processes involving different stakeholders in the energy utility domain.

9.1.8 Institute for Corporative Security Studies, ICS Ljubljana

Institute for Corporative Security Studies, ICS-Ljubljana (ICS) is organized as non-government research institution. The vision of the ICS Ljubljana is to create top-level knowledge, technologies, and processes in the area of corporative security while managing the entire scope of security risks. With a responsible and professional provision of comprehensive services in the area of corporative security, we create safer and richer future for the users of our services and knowledge. With good organization, innovative approach, top-level experts, and equipment as well as with established solutions, we, at the Institute of Corporative Security Studies – ICS Ljubljana will provide for comprehensive management of security risks in business and other environments, economic effectiveness, and satisfaction of the users of our services. In close relation with the interested entities in, both, public and private environments, we will provide for long-term development of scientific and professional knowledge in the field of corporative security. Security risk management is one of the crucial factors in achieving excellence and competitive position which especially become evident in business and economic environments. Critical Infrastructure has in this respect special importance. The strategic objectives of the ICS Ljubljana are directed to intensive participation in the promotion of development of comprehensive security systems in the area of corporative security, which directly influence risk management in business, development, economic, national security, critical infrastructure, and other environments. Main activities of ICS are divided in to following area: education, research, business counselling, standardization and evaluation, security geopolitics and publishing.

9.1.9 RWTH Aachen

As one of the Universities in Germany awarded the status of "Excellence University", RWTH Aachen University, established in 1870, is a leading technical university in Germany and Europe with over 40,000 students and more than 500 professors. The E.ON Energy Research Center, a public private partnership between E.ON SE and RWTH Aachen University funded in 2006, fosters innovative energy research with a strong link with industry in an interdisciplinary approach, with five institutes from four different faculties. Within this research center, the Institute for Automation of Complex Power Systems focuses on research for the automation, modernisation and restructuring of electrical energy distribution systems. This research area deals with solutions for monitoring, maintaining and developing complex power systems. Both the simulation of dynamic processes in complex network systems as well as development of a stable and secure communication infrastructure are areas of expertise of the scientists working at ACS. The institute is developing the science and technology for the transition to the next generation energy grid based on network distributed control systems,

agent-based control, distributed observer and measurements, complex system theory and control under uncertainty. The key scientific research areas of the institute ACS are the following:

- Future power grids as cyber-physical infrastructures
- Electrical power distribution and utilization in buildings, neighbourhoods, and urban energy systems
- ICT solutions for advanced energy services
- Distributed monitoring and control of electrical power grids
- Advanced simulation methods based on High Performance Computing
- Real time simulation and Hardware in the Loop testing

9.1.10 Software Imagination & Vision (SIMAVI)

Software Imagination & Vision S.R.L. (SIMAVI) is a spinoff company of SIVECO Romania SA – a large software company established in 1992. SIMAVI has inherited all the assets related to the software development activities, the related experience in the field, the implementation teams, the certificates, and the authorizations held by SIVECO Romania SA. SIMAVI has taken over also the software products and projects references from the following fields of activity: R&D, eLearning & eTraining, eHealth, Security, Customised Applications, ERP & BI, Customs, and Government. SIMAVI is acting as technology / integration partner in more than 35 Horizon 2020 projects where it has a main role as integrator. Moreover, SIMAVI is leading EnergyShield project funded in 2019 on SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches. As integrator, in energy related projects, SIMAVI contributed to integrating all developed components in the back end in order to obtain the functional distributed and networked system based on Web applications, services and the underlying platform. This means solving all dependencies, starting from simple function calls between different modules and components, to remote procedure calls (including the language-neutral remote procedure call for Web services), messaging or any other form of communication. Integration will also include the inclusion and adaptation of reusable open-source components (web application framework, AI algorithms implementation, etc.).

9.1.11 Software Quality Systems S.A.

Software Quality Systems, S.A. is an independent testing house expert in the design and implementation of verification and validation processes and tools, that was founded in 1998 and since then provides service for Software Quality assurance. SQS offers support and advice for Quality applied to processes as well as to products. SQS's customers are relevant players within the automotive, aeronautics, railway, pharmaceutical, telecoms, electronics, and banking sectors. Its main expertise in these field is testing validation and certification, against the most reliable standards of safety risks embedded systems. SQS helps companies and developers in their activities, giving a valuable contribution to finish projects within budget and time, according to the defined product requirements, by providing systematic software quality assurance. Some of its services are Design, follow-up, and implementation of software development processes | Design and implementation of benchmark process |

Design and implementation of product certification programmes. SQS has designed the Certification Vodafone Mobile Partner Programme (VMPP) | Design and implementation of verification and validation processes for safety critical systems and infrastructures, fulfilling sectorial standards (CENELEC, FDA) | Design and implementation of verification and validation processes for manufacturing processes such us 3D dimensional metrological software and certification against PTB standards | Testing outsourcing.

9.1.12 STAM SRL

STAM is an Italian engineering SME providing engineering and consulting services in the following sectors: security and transports, space, and defence, automation, and robotics, energy, and environment. The firm serves a broad range of industries, public and private companies, research organizations, no-profit agencies. A large part of STAM's activities is related to security aspects of critical infrastructures and public spaces. STAM has also established partnerships with key players, end-users, and operators in the field of security. The company has experience in the analysis and simulation of blast effects and consequences, modelling and simulation of crowd behaviour and terrorist attacks, risk assessment and decision-support platforms for the protection of infrastructures, soft targets and citizens and the implementation of security countermeasures. STAM is a key member of the following clusters and institutions: START 4.0, the Italian Competence Centre for the Security and Optimization of Strategic Infrastructures, funded by the Ministry of Economic Development; the Italian CBRN-P3 cluster, a technological, industrial and institutional cluster focused on prevention and protection of the citizens and the environment from CBRN risks; AIAD, the Italian industries federation for aerospace, defence and security; Istituto Affari Internazionali, a non-profit think tank focused on international issues in security, defence, economy and foreign politics; SOSIA, the R&D cluster focused on systems engineering, cyberphysical security and intelligent automation.

9.1.13 Synelixis Solutions S.A.

Synelixis is a high-tech SME that delivers advanced automation solutions including energy efficiency, precision agriculture, warehouse automation, AI, cybersecurity, and advanced networking. With respect to energy efficiency, its solutions focus on smart grid control and energy consumption optimization. By utilizing modern software technologies, hardware installation and open platforms, Synelixis engineers are able to ensure an optimized solution that fulfils the project requirements. Synelixis Solution technology superiority is a result of extensive R&D activities. Synelixis' personnel bring with it extensive research background, working for more than 20 years, in the RACE I & II, ACTS, ESPRIT and IST European frameworks in numerous projects and long cooperations with well renowned companies in EU and USA.

Synelixis is member of the AIOTI, the NEM, the NESSI, the eMobility and the Net!Works technology platforms. Moreover, Synelixis has been the coordinator of the H2020 project COSSIM-644042 and the Technical Coordinator of a number of EU funded projects (PHOENIX, SEA, BeyWatch, COAST, DOLFIN, SOFIE) cooperating with prestigious companies like STMicroelectronics, Engineering, Philips, Vodafone, Telefonica, NEC, EDF, Thales, Siemens, Ericsson, ABB. The product-oriented core competencies of Synelixis include expertise in Content-Centric Networking and solutions and services for resource and energy monitoring in different environments. Aiming to offer professional high-tech solutions, Synelixis has made

strategic partnerships with world-wide leading corporations. Synelixis is a registered Cisco/Linksys partner, HP Business Partner, and SUN Partner. In 2017, Synelixis partnered with Hewlett Packard Enterprise (HPE) to commonly offer IoT services. Synelixis SynField solution has been integrated with HPE Universal IoT to offer secure, vertical solutions for smart cities and precision agriculture. Through its long and continuous involvement in National and EU RIA R&D activities over the years, Synelixis possesses a successful track record of delivering advanced services, applications, and complete digital solutions for a broad area of ICT, especially in the areas of industrial IoT, cloud computing and energy efficiency. Synelixis has proven expertise in conceptual system architecture and design analysis, user-centric information marketplaces and portal management, online/offline data monitoring and analysis, software integration services, infrastructure management, virtualisation and cloud communication services, and project technical management. Synelixis currently focuses on extending product-oriented services and analysing business functionals created by digital transformation of the supply chain based on cybersecurity, Machine Learning and Privacy Preserving/ Federated Machine Learning, blockchain networks and interoperability enablers over heterogenous, complex IoT environments and use cases. SYN is a member of AIOTI (alliance for Internet of Things Innovation), 5G-PPP and a member of the NetWorld 2020, ETP4HPC (European Technology Platform for High Performance Computing), NESSI (Networked European Software and Services Initiative), NEM (New European Media), European Technology Platforms and NGI (Next Generation Internet) initiative. Synelixis owns 81% of Power Operation Ltd, a UK based spin-off specialized in energy data analytics. Within 2019, Power Operation Ltd. received the 2nd prize at IET Innovation Awards 2019 and was finalist at the UK IT Industry Awards 2019). Finally, in Q1 2020, Synelixis implemented the first fully digital kiosk platform for the Greek Ministry of Digital Governance and the Ministry of Rural Development and Food, hosted at the Greek Governmental Cloud and remotely serving more than 400.000 Greek Farmers.

9.1.14 WINGS ICT Solutions

WINGS ICT Solutions is an SME, which focuses on the development of solutions (software and hardware) for various vertical areas. The areas are utilities (water, energy, gas), smart/digital/liveable cities (providing the means for managing the air quality, the transportation infrastructure, and buildings, as well as delivering services for health, parking and user mobility, and citizen security/safety), food security/safety (safety of meat/milk/oil, smart aquaculture, etc.), and, more recently, industry/logistics. The foundation for the solutions comprises IoT technologies (all types of sensors and actuators, diverse devices/vehicles, etc.), advanced wireless networks (4G, WiFi, 5G, etc.), cloud and big data platform, artificial intelligence (AI) algorithms, and security mechanisms (such as blockchain, distributed ledgers, etc.). For these sectors WINGS develops specific platforms/products (powered by AI, IoT, cloud/big data, advanced wireless, and security mechanisms). Artemis for proactively managing utilities, Starlit for realizing the vision of smart/digital and liveable cities, Agnes for proactively optimizing the food security and safety levels. Finally, Nestor is an advanced simulation platform (for ICT infrastructures primarily). WINGS is proud to collaborate, since its founding in 2012, with large companies that have a multi-national footprint, like IBM, Intrasoft-International, Intel (DE), Pole Star Global (UK), and others. Moreover, there have been partnerships will most of the major operators and vendors, e.g., in the context of collaborative projects, and through other instruments. In parallel, as part of its strategy, WINGS aims at attracting investments for expanding its business and/or for

creating affiliate businesses. For example, WINGS created a spin-out company, Incelligent (www.incelligent.net). Incelligent focuses on the proactive management of resources and of the customer experience of broadband/cloud infrastructures, as well as in the delivery predictive/prescriptive products for certain areas of the Fintech, Social Security, and other Government sectors.

9.1.15 ZIV Aplicaciones y Tecnología S.L.

ZIV (Spain): ZIV Aplicaciones y Tecnología focuses its activity on the design, development, manufacture, and marketing of intelligent solutions based on elements of protection, control, communication, and measurement designed to be incorporated into high, medium, and low voltage power grids. ZIV applies numerical technologies to algorithms of protection, control, and automation. It has innovative products such as:

- Integrated protection and control equipment.
- Integrated systems with distributed functions for supervision and automation of substations and telecommunications.
- Definition of automation protocols.
- Monitoring and control equipment, measurement.
- Software tools and associated services.

ZIV was founded in 1993, and its mission is to be the user's ally to improve the safety, quality of service and profitability of its electrical systems. The vision is to lead the market by means of excellence in innovative, cost effective, customer-oriented solutions. Thanks to a commitment to innovation, to an open and flexible approach and to teamwork, ZIV has grown to become a leader in intelligent solutions for HV, MV and LV Grids. Solutions based on the integration of protection, control, communication, and measurement technologies. Today, ZIV is a team of around 500 professionals, with worldwide presence, serving the needs of both consumers and utilities offering a full range of products with in-house developed technology and related engineering services. ZIV participate in the main international technical forums, as well as in the alliances that are promoting the development of standard solutions that will facilitate the generation of new interoperable and open solutions.

9.1.16 Comune di Berchidda

Berchidda is a municipality in the Province of Sassari in the Italian region Sardinia, located about 170 kilometres (110 mi) north of Cagliari and about 30 kilometres (19 mi) southwest of Olbia. The Ministry of Productive Activities has granted the Municipality of Berchidda the concession for the distribution of electricity on medium and low voltage distribution networks for delivery to final customers. The Municipality, therefore, carries out transportation and transformation of the electrical power on medium and low voltage distribution networks until the delivery to final customers.

9.1.17 BENETUTTI

Benetutti is a municipality in the Province of Sassari in the Italian region Sardinia, located about 190 kilometres (120 mi) north of Cagliari and about 91 kilometres (57 mi) southeast of Sassari. The Ministry of Productive Activities has granted the Municipality of Benetutti the concession for the distribution of electricity on medium and low voltage distribution networks. The municipality is the stage of an ongoing project for the creation of an advanced smart grid that foresees the deployment of PV, wind turbines, geothermal, solar thermal and storage units. Actually, the Benetutti's technological innovation level and the high number of citizen Prosumers (energy consumers and producers), put the municipality in the front line in the Smart City development and the optimized energy management system achievement.

9.1.18 ELES, d.o.o.

The ELES d.o.o. Company has the exclusive right to perform the service of transmission network system operator in the Republic of Slovenia. It is established and owned by the state. ELES ensures the safe, reliable, and uninterrupted transmission of electricity. ELES is the guardian of Slovenia's electric power transmission system, which is closely connected to the transmission networks of neighbouring countries and integrated into the European energy system. ELES is the operator of the electric power transmission network of the Republic of Slovenia. With a professional approach, know-how and advanced technology, ELES has been providing safe, reliable, and uninterrupted electric power transmission throughout Slovenia and across the borders for 90 years. Thus, the company connects people and ensures quality of life. ELES endeavours to plan, construct and maintain Slovenia's high-voltage transmission network in three voltage levels: 400 kV, 220 kV and a part of 110 kV strategically, responsibly and sustainably. ELES is an important and solid backbone of the Slovenian electric power industry and a guardian of the Slovenian electric power system. Its key responsibility is the safe and reliable operation of the electric power system. It interconnects all the main actors in the Slovenian electric power transmission network: power plants providing electric power for the transmission network; five distribution companies; five larger consumers, the so-called direct customers, which offtake electricity from the transmission network, and four larger consumers (steelworks and TALUM) with the status of a closed distribution system.

9.1.19 Petrol, Slovenian Energy Company d.d., Ljubljana

Petrol, the leading Slovenian energy company – with a sales revenue 4.4 billion EUR and a staff of 1951 – is growing from the Slovenian oil trader to a comprehensive regional provider of energy and environmentally friendly services. Our clear strategic policies and development priorities significantly co-shape not only the Slovenian energy field but also make us an important player on the energy field of South-eastern Europe. The principal development direction of the Petrol Group is the introduction of new energy business activities, which includes the marketing of gas, heating, and electricity, managing larger environmental projects and the marketing of renewable energy in the long-term. In line with the challenges of the contemporary world, we developed and provided a range of

integrated solutions in the fields of district energy systems, water supply systems, efficient lighting, buildings, energy management, demand-side integration, and mobility. Our activities contribute to the reduction of energy and water consumption and environmental impact. We perform our services to lower the operating and maintenance costs in public, sports, business and industrial buildings, residential buildings and on district heating, water supply and public lighting systems. Petrol is tightly connected with partners involved in this project as an aggregator and generator within a platform for providing a tertiary regulation.

9.1.20 SI-CERT (Slovenian Computer Emergency Response Team)

SI-CERT (Slovenian Computer Emergency Response Team) is the national cyber security incident response center for the Republic of Slovenia (SI). SI-CERT operates within the framework of the Arnes (Academic and Research Network of Slovenia) public institute. The operations of SI-CERT are defined under Article 28 of the Information Security Act (ZInfV, Uradni list RS, št. 30/18). SI-CERT helps in computer and network security incident handling and provides incident coordination functions for all incidents involving systems and networks of Operators of Essential Services in Slovenia. It also provides consultancy on a number of issues (e.g., technical, operational) to a myriad of relevant stakeholders, ranging from the general public to internet service providers and other European-wide CERTs. Since 2011, SI-CERT is conducting a national awareness raising programme "Safe on the Internet" (sl. Varni na Internetu, VNI). The aim of the year-round programme is raising awareness of cybersecurity threats, promoting cybersecurity among citizens and organizations, and providing resources for online protection, through education and sharing of good practices. Within the national awareness programme, SI-CERT actively takes part in ECSM - the EU's annual awareness campaign that takes place each October across Europe. Accredited by the Trusted Introducer program, SI-CERT is a member of the CSIRT Network defined by the EU NIS Directive, member of the Forum of Incident Response and Security Teams (FIRST), the group of national response centres at CERT Division (Software Engineering Institute of the Carnegie-Mellon University, formerly CERT/CC) and the wider European response centre working group (TF-CSIRT). As such, it takes part in all relevant events (e.g., conferences, workshops, cybersecurity exercises, member meetings) aimed at strengthening cooperation, developing and sharing know-how and fostering good practices. SI-CERT also serves as the Slovenian contact point for the security department of the General Secretariat of the EU Council and as the national focus point for the IMPACT program of the International Telecommunications Union (ITU).

9.1.21 Hrvatski Operator Prijenosnog Sustava DOO

Croatian Transmission System Operator Ltd. (abbreviated HOPS) mission is electric power system operation and maintenance, electricity transmission, as well as construction and development of electricity transmission network in order to maintain security of supply with minimal costs and environmental protection. HOPS is the sole electricity transmission system operator in the Republic of Croatia, and the owner of the entire Croatian transmission network (400 kV, 220 kV and 110 kV included voltage levels). HOPS has the license to carry out electricity transmission as a public service. The company performs its functions transparently and independently in accordance with the Croatian Companies Act. In

performing its functions HOPS cooperates with all energy market participants in accordance with the regulations in the field of electricity transmission and Croatian Energy Regulatory Agency (HERA). HOPS cooperates with other European system operators and foreign market participants, as well as with many Croatian and international institutions in the field of electricity transmission. HOPS is a member of ENTSO-E, and a shareholder of TSCNet, JAO, SEE CAO and Croatian power exchange CROPEX. HOPS has participated so far in FP7 project PEGASE, that has developed new tools to enhance the cooperation among transmission system operators for the real-time control and operational planning of the Pan-European transmission network. With Slovenian TSO ELES, and Slovenian and Croatian DSOs, SODO and HEP ODS, HOPS has established a consortium for application of a SINCRO.GRID project to be founded by EU CEF. SINCRO.GRID project is developing a methods and tools for TSO-DSO cross-border coordination, for optimal operation of transmission and distribution grid, concerning load flows and voltage issues, aiming for larger integration of renewables, ensuring at the same time the security of supply. Role and main tasks HOPS is Croatian TSO and will within project provide both its infrastructure and experts. Within pilot HOPS work on two concrete use cases. One will be focused on uninterrupted collection of non-energy related data (environmental) HOPS is collecting close to real time to improve utilization of its system and minimize curtailment of power flows in the network. Second case is directed in secure exchange of data between system operator and aggregators in economically reasonable way.

9.1.22 Enerim Oy

Enerim Oy (ENERIM) is an independent service provider from Finland whose main business domain is the energy markets and related services. We provide a wide range of different flexible energy market services and IT solutions to our customers in Finland and other Nordic countries. Our services can be divided into three different categories: Energy market services, Smart Grid Solutions and Energy Sector IT Systems. In addition to the services, we have our own IT-systems in the fields of Customer Information Management, Energy Data Management and Energy Management. We develop our expertise of electricity markets and knowledge of energy business domain constantly; so that we can provide solutions to our customers to ensure that our customers can focus on improving their own competitive edge against their competition. We have participated in several EU research projects as well as several national Finnish research projects. Enerim Oy is a responsible for information exchange of several energy market needs, including wholesale trading, reserve market trading, balance settlement and metering data provision.

9.1.23 Elektrilevi OÜ (ELV)

Elektrilevi OÜ (ELV) supplies electricity to almost all households and companies in Estonia. We cover over 90% of Estonia. Our challenge is that 60% of the grid supplies 5% of consumption. Our role as a network operator is to ensure the constant supply of electricity to our customers. We maintain and repair almost 61,000 kilometres of power lines and more than 22,000 substations. Elektrilevi has almost 475,000 customers across Estonia. Our network area does not include Lääne County, Viimsi or Narva and its surrounding areas, where electricity is supplied by other network operators. Network operators manage electricity distribution networks of up to 110 kV, transferring electricity from the transmission system to the consumer.

9.1.24 CNTEE Transelectrica SA (TEL)

Transelectrica is the Romanian Transmission and System Operator (TSO), which plays a key role in the Romanian electricity market. We manage and operate the electricity transmission system and provide the electricity exchanges between the central and eastern European countries as an ENTSO-E member (European Network of Transmission and System Operators for Electricity). Transelectrica is responsible for electricity transmission, system and market operation, grid and market infrastructure development ensuring the security of the Romanian power system. It also serves as the main link between electricity supply and demand, matching all the time power generation with demand. Transelectrica SA is the only operator providing the services of electricity transmission, operational technical management of the Romanian Power System and electricity market administration (by means of its legal personality subsidiary OPCOM SA). Transelectrica SA carries out these activities under the license that ANRE has granted it, charging regulated tariffs that allow a non-discriminating and fair access of all market participants to the electricity transmission grid, with no additional revenues from other activities. Transelectrica's task is to keep the Romanian Power System operating uninterruptedly under safe conditions while observing the quality standards provided in the Grid technical code. To this effect, the company uses its own resources called functional system services and purchases technological system services from the electricity generators. Transelectrica SA purchases the technological system (ancillary) services from the electricity generating companies under a procedure regulated by ANRE.

9.1.25 Romanian Energy Center (CRE)

CRE (Romanian Energy Center) is a non-governmental sectoral association in the energy field, active in the following areas: electricity, oil and gas, coal, renewables, energy equipment and services. CRE organization was established in 2011 through the two offices opened in Brussels and Bucharest, having the main objective to promote the active participation of Romanian state-owned and private energy companies in European partnerships, EU projects and the European decision-making process, including but not limited to promote infrastructure investments and offering support for the transition to a decarbonized energy system. By strengthening the RDI department with a series of expert profiles with experience in energy, economics and CSR, project management, education systems, ICT and European projects exposure, CRE has intensified its involvement in projects funded by the H2020 and ERASMUS programs, currently having in its portfolio a number of 10 completed and ongoing projects addressing a complex expertise. CRE's vision is represented by a global context based on safety, comfort, and respect for the environment, built on energy infrastructure, in which the Romanian energy plays an active role aligned international goals. One important pillar in the CRE strategy is the role the association plays as an interface between general and individual interests of its members and local and international energy institutions with the vision of achieving a sustainable future. As an active member of projects consortiums in the context of coordinating actions on regulation, socio-economic analysis, and dissemination, CRE conducted extensive consultation activities with a complex interaction, which allowed it through an efficient networking to develop a wide network of stakeholders.

9.1.26 Timelex

Timelex (TLX) is a boutique law firm based in Brussels (Belgium) specialised in information and technology law in the broadest sense, including privacy protection, data, and information management, ebusiness, intellectual property and telecommunications. Its activities cover all legal issues encountered in the creation, management and exploitation of information and technology, in all of its diverse forms. Timelex as an independent firm was founded in 2007, and many of its lawyers started their career in international law firms and multinational companies. The team is internationally recognised, being both a Legal 500 Top Tier firm in Information Technology, and a Chambers Europe Recommended Firm for TMT - Information Technology, Intellectual Property, Data Protection and Entertainment. Timelex has a proven track record in every aspect of information and technology law, from an academic, business and policy perspective. At Timelex, all legal facets of the modern information society are our area of expertise, which we continuously cultivate by assisting policy makers, public and private organizations with all their legal problems in this area. The Timelex team provides support from a pragmatic perspective as lawyers at the bar of Brussels, and from a policy perspective as advisors to various governments, public administrations, and legislative bodies in Belgium, at the European level, and internationally. The Timelex team is specifically known for its European policy studies in a variety of subjects, including data protection, electronic signatures, electronic identity management, e-business, and e-government, in which they can rely on an extensive network of IT law experts covering all European countries. From a business perspective, Timelex frequently assists companies in establishing suitable policies and legal frameworks in their data management activities, including with regard to the cross-border transfer and processing of personal data, data security and liability management issues. Its clients include private companies and public sector bodies in the IT sector, financial services, e-health, marketing, and e-commerce.

9.2 Project requirements for secure and privacy preserving data exchange among operators.

To evaluate better the requirements of a local system of dissemination of CTI information based on STIX/TAXII suite in the context of CyberSEAS project we will consider the CyberSEAS ecosystem with the architecture shown in Figure 20 CyberSEAS ecosystem architecture. In the architecture is indicated a MISP/STIX adapter that is processing tool reports and also CyberSEAS Incident data models making them available to EU CERTS and other organisations working with CTI information.

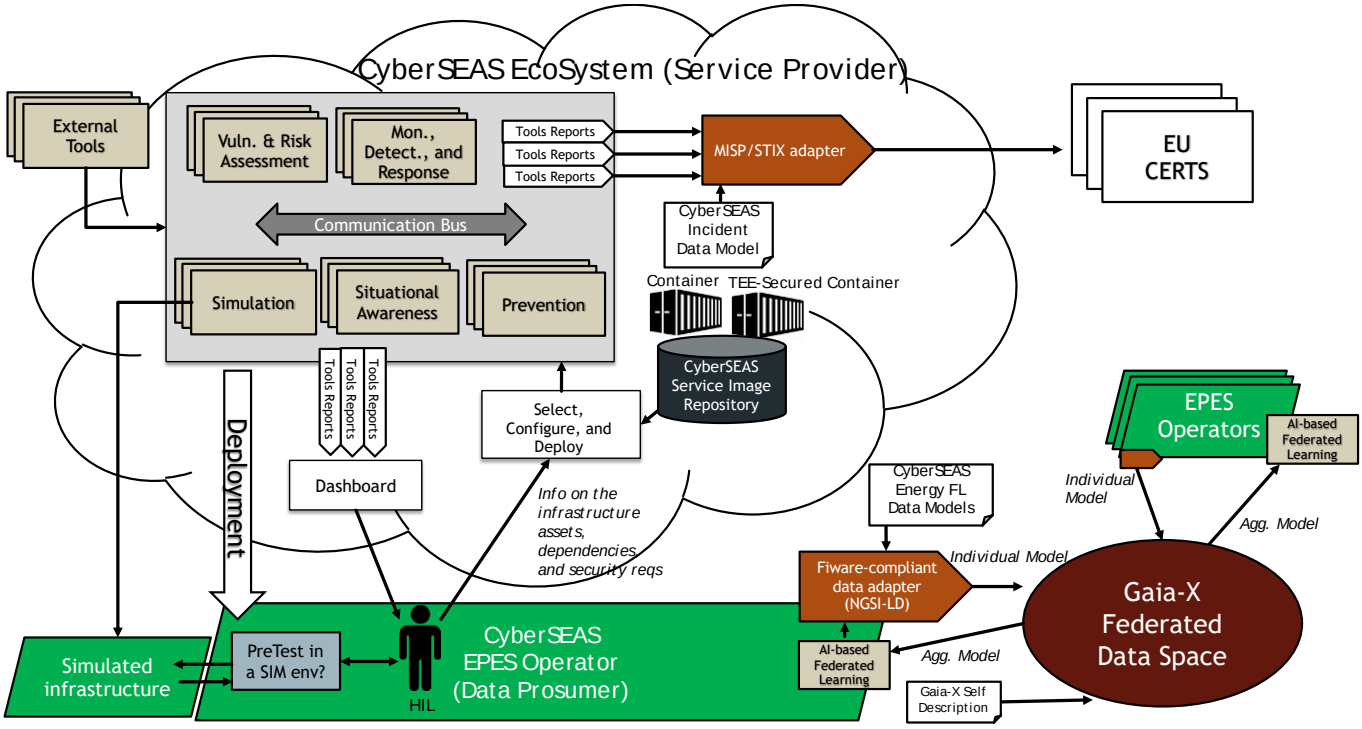

Figure 20 CyberSEAS ecosystem architecture

In order to get more information, the processing and disseminating CTI by CyberSEAS tools a survey was deployed among the tool developers The questions of the survey are indicated in following table.

Table 5 question for the survey on CyberSEAS tools

Question Number	Question
Q2	Does your tool need to receive CTI information from other stakeholders?
Q3	Can your tool provide CTI information to other stakeholders ?
Q4	Can your tool interface with CTI exchanged in STIX format
Q4	Does your tool use machine learning ?
Q5	Does your tool use in ML training information in STIX format
Q6	Is your tool able to communicate with CERT in STIX format

The questions are focusing on CTI processing and dissemination and also on the possibility of sending CTI information to ML algorithms.

9.2.1 CyberRange - Energy sector awareness scenario

CyberRange is our tool used for simulation and training. The tool uses digital twins (virtual representations of the physical world) to mimic a use case. The digital twins are then used as a basis to test the behaviour of the network whenever a new actor (attacker) gets access,

and it allows the user to add protective measures and to test its response. The complete setup is used for training, to show network admins how to implement and configure technology, and how to respond when an incident raises.

Table 6 Answers from CyberRange tool

Question number	Answer
Q2	It can be configured to receive CTI if the work zone is simulating a CSIRT environment. As a simulation and modelling tool, it is not within the core capabilities to receive or provide CTI.
Q3	It can be configured to receive CTI if the work zone is simulating a CSIRT environment. As a simulation and modelling tool, it is not within the core capabilities to receive or provide CTI.
Q4	Depending on the tool inside CyberRange, information exchange can be done in several formats. As a simulation and modelling tool, it is not within the core capabilities to receive or provide CTI.
Q4	No. However, as a simulation and modelling tool, it can process ML if the simulating environment contains tools that use it.
Q5	No. However, as a simulation and modelling tool, it can process ML if the simulating environment contains tools that use it.
Q6	No. However, as a simulation and modelling tool, a work zone in CyberRange can run the tools required to communicate with CERT in any format.

9.2.2 Business Process-Intrusion Detection System (BP-IDS)

The Business Process Intrusion Detection System (BP-IDS) introduces a novel technique for detecting intrusions through the supervision of the system's FIWARE-compliant digital twin representation. The behaviour of the digital twin is described by means of a finite state machine that leverages the business process workflow of the monitored system as provided by the EPES operator. The primary aim of the BP-IDS is to recognize anomalies, i.e., deviations from the established workflow.

Table 7 Business Process-Intrusion Detection System

Question Number	Answer
Q2	No, currently BP-IDS does not use CTI information but information from the field. BP-IDS models could be adjusted by the operator based on the received CTI.
Q3	No. Detected anomalies and alerts could serve as input to a CTI but it is much more likely that other tools (e.g., the SIEM) will collect alerts form the BP-IDS and feed an information sharing tool
Q4	No. The tool does not provide nor consume CTI, thus no interface.
Q4	No. The tool does not use ML, or other subsets of AI.
Q5	No. The tool does not use ML training information in any shape or form.
Q6	No. The tool is able to generate alerts, but it is not meant to act as an information sharing tool, as such it not designed to interact with CERT.

9.2.3 Enhanced SIEM solution for SOC with features dedicated to Cis.

A complete solution to correlate context information, also coming from SLAs monitoring system related to the business process evolution, with events related to the digital domain. The solution is also enhanced with the storage capability to store sensitive information in a tamper-resistant fashion.

The SIEM is able to detect cyber-attacks to the applications and systems of the pilot partners. The systems and applications are monitored through a set of cyber-related probes. The data is collected, parsed out, processed, and correlated to produce an alert. The correlation logic is rule-based. To enable an efficient integration with a SOC environment, the rule designer and the rule manager components enable creation, visualization, and management of correlation rules. The alerts produced are displayed on dedicated dashboards, supporting the eventual mitigation actions.

Table 8 SIEM survey answers

Question Number	Answer
Q2	SIEM can use CTI information but, in the current version for CyberSEAS, it only correlates information from IDSs. The benefits of using information received from a CTI will be investigated.
Q3	No. In its current form the SIEM is not provided with an information sharing module, we are exploring the opportunity to integrate such a feature.
Q4	The tool is not thought to directly act as an information sharing tool, thus no need to use STIX. The SIEM has a modular design that enables the possibility to interact with additional tools. If in the future the need to perform information sharing will be envisioned, a dedicated tool will be selected and integrated with the SIEM.
Q4	No. The tool does not use ML, or other subsets of AI.
Q5	No. The tool does not use ML training information in any shape or form.
Q6	No. The tool is able to generate alerts, but it does not send them to CERT. The SIEM has a modular design that enables the possibility to interact with additional tools. If in the future the need to communicate with CERTs will be envisioned, a dedicated tool will be selected and integrated with the SIEM.

9.2.4 Secure deployment support

A software solution to support the secure deployment of applications with a trusted execution environment (TEE) and cryptographic features. The final goal is to enable a protection of sensitive data processing in a Trusted Execution Environment, transparent shielding of off-the-shelf applications, and automatic and easy-to-use tools for building and deploying shielded applications.

Table 9 SDS tool survey answers

Question Number	Answer
Q2	No. SDS does not use and does not benefit from CTI information.
Q3	No. SDS is a support solution for software deployment.
Q4	No. SDS is a support solution for software deployment.
Q4	No. The tool does not use ML, or other subsets of AI.
Q5	No. The tool does not use ML training information in any shape or form.
Q6	No. SDS is a support solution for software deployment, and it does not need to communicate with CERT.

9.2.5 Virtual Testbed

It is a cyber-range where users can simulate specific scenarios to assess the impact of attacks on the cybersecurity status.

Table 10 VTB survey answers

Question number	Answer
Q2	No. VTB does not use and does not benefit from CTI information.
Q3	No. VTB does not use and does not benefit from CTI information.
Q4	No. VTB does not use and does not benefit from CTI information.
Q4	No. The tool does not use ML, or other subsets of AI.
Q5	No. The tool does not use ML training information in any shape or form.
Q6	No. VTB does not use and does not need to report to CERT.

9.2.6 TO4SEE

Tool for Social Engineering Exposure (a.k.a. Social Engineering Detection (SED) tool). The SED tool analyses the header, body, and attachments of an email to check if it is a vector for a social engineering attack. E.g., by sharing a malicious URL or attachment.

Table 11 TO4SEE survey answers

Question number	Answer
Q2	No, TO4SEE does not receive CTI data from other stakeholders. It could be useful to integrate other CTI info about malicious URLs/IPs or malware hashes.
Q3	We are thinking about an email analysis report to be published/shared to summarize the malicious indicators we found in the email.
Q4	No, the tool does not use CTI-STIX data.
Q4	Yes, we use NLP for email anonymization and text-analysis. We also use ML for malicious PDF attachments classification.
Q5	No, the training is based on email body text and PDF file features.
Q6	No, the core of the tool is mainly developed in Java which lacks official/updated STIX support.

9.2.7 ALIDA

Edge-cloud Data Science and Machine Learning Platform

Table 12 ALIDA tool survey answers

Question number	Answer
Q2	Yes, if we consider CTI information as the labelled data needed for the e-mail phishing detection use case (in order to train a ML/DL model).
Q3	Yes, it can provide CTI information. For instance, in the e-mail phishing detection use case the relevant information is to identify if an e-mail is spam or not.
Q4	No, actually the tool doesn't support STIX format.
Q4	Yes, in the tool service catalogue can be registered new developed services that make use of ML/DL techniques.
Q5	No, generally ML training is performed using data in tabular format (as CSV), or taking directory containing image/text data, depending on the type of training.
Q6	No, actually the tool is not able to communicate with CERT in STIX format.

9.2.8 MDPI

Multidimensional data processing and intelligent (MDPI) framework: MDPI is a middleware tool that allows to collect and aggregate data from the various levels of the CyberSEAS architecture to generate a Situational Picture of the CI status.

Table 13 MDPI tool survey answers

Question number	Answer
Q2	No currently MDPI does not need to receive CTI info. However, it can use the output information from the CTI tools to make correlations.
Q3	The tool does not currently provide CTI information, but uses the output information of the tools that do CTI to correlate this information with information from other layers such as the detection layer or use this output to update the severity level of the SP.
Q4	MDPI can interface with CTI tools to retrieve risk assessment or severity information and does not use the STIX format. It rather uses the IDMEF v2 format. The need to carry out format conversions is analysed also contemplating STIX.
Q4	This tool makes use of ML for a better correlation between events.
Q5	The tool does not need to use the STIX format currently. The need is analysed.
Q6	The tool does not need to communicate data to the CERT. The data returned is useful for undertaking any mitigation actions.

9.2.9 MIDA cloud control tool

Compliance monitoring solution that enables the security team to verify the integrity of security control policies and the actual state of the digital assets, including infrastructure, and services in real time.

Table 14 MIDA tool survey answers

Question number	Answer
Q2	No, MIDA does not use CTI information. MIDA rules could be adjusted by the operator based on the received CTI.
Q3	No. Detected misconfigurations, anomalies, and otherwise changes in compliance could serve as input to form CTI.
Q4	No. Tool does not provide nor consume CTI, thus no interface.
Q4	No. Tool itself does not use ML, or another subset of AI.
Q5	No. Since it is not using ML, it does not use ML training information in any shape or form.
Q6	It could be configured to send alerts if need be but currently we do not see any reasonable justification for MIDA to send alerts directly to CERT.

9.2.10 ARTEMIS

ARTEMIS is the WINGS product for the management of energy, water, and gas networks. Key aspects of the platform are metering, consumption and capability prediction, handling of leakages, fault management, performance management, security, and others. In terms of security, ARTEMIS can detect anomalies in sensor's data. In this way the platform can notify the user in case data manipulation attempts are detected. Additionally, ARTEMIS can identify anomalies in network traffic as well as in data from SCADA system, so that the user is notified before damage occurs to the equipment.

Table 15 ARTEMIS tool survey answers

Question number	Answer
Q2	No, ARTEMIS does not receive CTI information but information from sensors installed in the infrastructure.
Q3	No, ARTEMIS does not provide CTI information, but the information it provides about detected anomalies could be used as input for CTI.
Q4	No, ARTEMIS does not interface with CTI
Q4	Yes. ARTEMIS uses machine learning algorithms to detect anomalies and make predictions.
Q5	No. It uses information in JSON format.
Q6	No, it does not communicate directly with CERT

9.2.11 CVIAT

CVIAT provides a systematic, repeatable and historized Risk Analysis, according to Risk Management ISO/IEC 27005 and implements the steps of:

- Risk Identification, using standards (NESCOR, NIST CVE and ISO/IEC 27005:2018) pilots' experience the results of actual penetration tests.
- Risk Estimation, using CVSS.

Additionally, through dashboard functionalities, CVIAT provides some initial support on Risk Evaluation

Table 16 CVIAT tool survey answers

Question number	Answer
Q2	Yes. In offline mode we receive vulnerabilities that have been deemed relevant for the CyberSEAS pilots. Vulnerabilities are entered in the tool through an offline loading process.
Q3	We provide scored vulnerabilities, together with the historical evolution of the score, linked with assets of the pilots. This information is provided on the screen of CVIAT.
Q4	No, under consideration, as potential extension.
Q4	No.
Q5	No.
Q6	No, it does not communicate directly with CERT

9.2.12 SAPPAN

SAPPAN is a playbook creation and management tool (Machine readable in CACAO and SAPPAN formats)

Table 17 SAPAN tool survey answers

Question number	Answer
Q2	Yes, SAPPAN knowledge capturing tool can receive CACAO/SAPPAN playbooks as CTIs in JSON format
Q3	Yes, SAPPAN knowledge capturing tool can provide CACAO/SAPPAN playbooks as CTIs in JSON format
Q4	No, SAPPAN does not support STIX format and only works via MISP for exchanging cybersecurity playbooks as CTI.
Q4	No, the tool does not use Machine Learning, or other subsets of Artificial Intelligence.
Q5	No, the tool does not use ML training information in any form.
Q6	No, SAPPAN does not support STIX format, but it works via MISP.

10 Instructions and implementation guidelines for a CTI communication system among Pilots

10.1 Estonian pilot

The Estonian cybersecurity pilot aims to resolve the issue of poorly secured operational technology (OT) device updates in energy substations. The pilot's goal is to ensure the integrity of the OT device configuration through firmware control and signing, which will only allow verified and validated firmware and install files to be used, mitigating some supply chain risks. The pilot depends on the vendor's ability to issue proper certificates or other verification methods.

The OT management's goal is to limit the use of unauthorized firmware and install files, ensuring that only centrally controlled and signed firmware can be applied to ICS devices. The expected result of the pilot is a novel control mechanism, reducing the risk of potential security incidents and consequences.

In Elektrilevi, a firmware validation tool is used to verify the integrity of the device's firmware. The validation tool is specific to Elektrilevi devices and is not considering the use cases for other tools. Elektrilevi is using a proprietary tool to manage the security of its devices, which may limit the tool's effectiveness in the broader context of cybersecurity. By not using the CTI transfer, Elektrilevi limits its ability to integrate with other tools and takes advantage of the benefits of using standardized interfaces.

10.2 Finnish Pilot

The Finnish pilot aims to study different cybersecurity aspects of an instant of Enerim CIS platform, as tool for automating utilities information and invoicing as well as enhancing its cybersecurity. The platform is a software module developed by Enerim company to help energy companies automate their customer information and invoicing. The platform is a flexible and modular tool for all multi-utility company functions. It comprises of customers contracting data and electricity consumption/production data.

The CIS platform provides variety of processes and services including but not limited to customer management, product management, contract management, consumption location management, invoicing, reporting and archiving for energy suppliers and distribution system operators. The platform increases speed of cashflow by doing calculations in real-time. The real-time calculation capability serves real-time data and dashboards which lead to full visibility and transparency to business operations.

The platform exchanges data with some other platforms including but not limited to online platform and customer relationship management (CRM) platform. The platform also indirectly exchanges data with national datahub for electricity retail services. The data exchange is through information exchange system (IXS) platform which is developed and operated by Enerim company.

The CIS platform has a modular architecture which enables microservices/functional modules being updated individually without interrupting the service. The platform has easy to browse interface for users and open APIs for easy integration with third-party modules.

10.3 Romanian Pilot

The Romanian pilot is hosted by Transelectrica. It is the Romanian national transmission operator .

Transelectrica is developing his own strategy for the cybersecurity topic transmission . The strategy is based on a set of procedures covering the main aspects on cyber threats.

- Procedures of response to cybersecurity incidents
- Procedures of cybersecurity vulnerabilities management
- Procedures of communication and cooperation

On Cybersecurity topics Transelectrica has to cooperate with a set of EPES entities that are connected into the National grid owned by Tel and operated by TEL

In this case the communication and cooperation procedure from Transelectrica states that the main objectives are :

- Maintaining contact with national authorities
  - The Information Security Manager acts as the single point of contact (SPOC) for all information security issues in the relationship between C.N.T.E.E. "Transelectrica" S.A. and ENTSO-E.
  - The Information Security Manager is in contact with national authorities (e.g., the National Cyber Security Directorate) so that they can advise ENTSO-E on national laws and regulations that may impact the Security Plan and OPDE services .
- Maintaining contact with special interest groups or other specialized security forums and professional associations
  - The Information Security Manager follows the decisions taken by the ENTSO-E special interest groups (e.g., the Cybersecurity Special Interest Group) on information security topics and the ENTSO-E IT strategy.
  - The Information Security Manager also maintains appropriate contacts with special interest groups or other specialized security forums and professional associations (by joining or subscribing to them).
  - The Information Security Manager analyses, together with the persons designated for the roles in PSMVS (Access Control Manager, IT Resource Manager, Network Manager, Crypto Custodian, Data Custodian) the received information. The Information Security Manager communicates with the organization's Management the information that may have an impact on the MVS Security Plan and the OPDE services, in order to establish the position that will be adopted by C.N.T.E.E. "Transelectrica" S.A. vis-à-vis this information.

For communication of CTI information now classic procedures are working. A system based on STIX/TAXII can be useful and facilitating the CTI information dissemination along the structure of Nation Energy Grid.

11 Conclusions

CyberSEAS project is focusing on improving the cyber security and resilience to cyber threats of EPES. The EPES and critical infrastructure are in a special condition. The EPES and electricity grids along with other actors involved in operating other critical infrastructure than electrical, are connected in a structure covering the supply network that they are using. They are forming a special hierarchized community and are exchanging large volumes of information and data starting from operational technology, network control, business logic and data.

To increase the resilience to cyber threats, the overall cyber security awareness and response of these communities to cyber threats, specific communication, based especially on cyber threat intelligence over events and threats from this community is very important.

Also, in these critical infrastructure networks and communities the cascading effect has to be considered as a very important threat affecting grid stability on huge geographical areas.

This aspect of dissemination cyber threats intelligence is already considered in multinational companies involved in electrical distributions and transmission activities. These companies developed internal CTI dissemination networks similar of CERTS structures and processing.

The tools form CyberSEAS that are analysed by the survey executed in first version of the deliverable, developed in little measure direct interface to CTI information. Most of the tools are middleware tools processing information in order to provide means of detection of cyber threats and not providing CTI as a final product. In the second part of CyberSEAS project due to integration of tools and developments that are done also in WP6 the exchange of CTI was considered in a better way. Inside CyberSEAS ecosystem are tools as SAPAN that are working with CTI and the actual format for structuring CTI is MISP.

A local dissemination network based on these protocols can be established among energy stakeholders and EPES to improve their ability to respond to cyber threats.

To set up such a network, stakeholders in the energy industry that are also focusing on cyber security would need first:

- to agree on the types of information they want to share.
- the frequency of sharing the CTI to be effective and useful.
- the protocols they will use for sharing CTI.

The most important aspect is the need to establish trust among themselves and define clear rules for data protection and sharing.

Once these issues are addressed, the stakeholders can set up a local server that implements the STIX and TAXII protocols or MISP as indicated in Chapter 8.4. This network of MISP instances would enable them to exchange cyber threat intelligence in a structured and automated manner, allowing for timely and accurate responses to emerging threats.

The dissemination network could be further enhanced by integrating it with other cybersecurity tools, such as security information and event management (SIEM) systems and intrusion detection systems (IDS). This would provide a more comprehensive view of the cybersecurity landscape, enabling stakeholders and EPES to respond more effectively to emerging threats.

Overall, establishing a local dissemination network based on MISP exchange can improve the ability of energy stakeholders and EPES to share and respond to cyber threats, ultimately improving the security and reliability of critical energy infrastructure.

A subset of CTI from the local infrastructure can also be sent to EU CERTS and cybersecurity organisations to disseminate the cyber-attacks occurred overt the Critical infrastructure . Also selected information from EU CERTS concerning threats that can endanger the critical infrastructure can be shared .

For the second version of D6.4 deliverable new conclusions were defined based on evolution on the project CyberSEAS. During the development of tools there was an increased interest of using MISP protocol that was not detailed in the first version of deliverable. Considering that a more detailed approach of this CTI sharing protocol was developed in the second version of deliverable.

The MISP Protocol is established as a framework for threat information sharing in Work package 6 task T6.4.

MISP Taxonomy and Galaxy provide structured methods for classifying and correlating threat information and was used in WP6 to exchange information to CERTS in T6.4 and through CERTS information was exchanged over CyberSEAS operators as indicated in Chapter 8.4 and also based on the MISP network shown in Figure 19 CyberSEAS internal MISP infrastructure The AI based tools developed in CyberSEAS project were facing the conditions imposed for data sharing of privacy-sensitive data on EPES.

Federated Machine Learning (FML) is applied to privacy-sensitive data in EPES, ensuring data privacy while allowing collaborative learning.

In the second version of the deliverable in Chapter 7 details various mechanisms and technologies like Data Anonymisation, Differential Privacy, Secure Aggregation, and Private Aggregation of Teacher Ensembles (PATE) that protect data privacy within FML architectures. These algorithms were used by ML CyberSEAS tools as indicated in Chapter 8.1for ALIDA tool and Chapter 8.2 for FML to IDS tool.

Achievements in CYBERSEAS project in secure and privacy-preserving data exchange among operators reached in the second half of the project are detailed in the second V2 version of deliverable in Chapter 8 sections as:

- Demonstrates the successful implementation of FML algorithms in the CYBERSEAS project to ensure secure and private data exchanges.
- The application of FML has been shown to enhance proactive notification and streamline workflows in Intrusion Detection Systems (IDS).
- Discusses the integration of Data Spaces (CINI) for secure data interchange.
- Defines how the MISP protocol and SAPPAN enhance the CyberSEAS project's CTI (Cyber Threat Intelligence) exchange among EPES and Energy operators.
- Presents methods for transferring CTI data using the STIX format from the CVIAT tool.

Conclusions for these new chapters added in second version V2 revolve around the effective implementation of new technologies for enhancing cybersecurity and privacy, particularly in the context of EPES. It could be concluded that the MISP protocol is a valuable tool for structured threat information sharing, while FML offers a promising approach to handling sensitive data with robust privacy-preserving mechanisms. Moreover, the achievements of the CYBERSEAS project could be highlighted as a case study for the successful application of these technologies in real-world scenarios.

12 References

[1] IBM, "Cost of Data Breach," [Online]. Available: https://www.ibm.com/reports/data-breach.

[2] M. L. S. M. N. e. a. J. N. S. M. Sarhan, "Cyber Threat Intelligence Sharing Scheme Based on Federated Learning for Network Intrusion Detection.," 2023.

[3] "Cybersecurity Strategy of the European Union:," JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, 07 02 2013. [Online]. Available: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

[4] ENISA, "Single Programming Document," [Online]. Available: https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-report-2023-2025. [Accessed 10 03 2023].

[5] ENISA, "Information Sharing and Analysis Requirements," [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing. [Accessed 10 03 2023].

[6] ENISA, "Cross-Sector Exercise Requirements," [Online]. Available: https://www.enisa.europa.eu/publications/cross-sector-exercise-requirements?v2=1.

[7] "CERT-EU," [Online]. Available: https://cert.europa.eu/.

[8] "ECCC European Cybersecurity Competence Centre and Network," [Online]. Available: https://cybersecurity-centre.europa.eu/index_en.

[9] "EU Cyber Security Strategy," [Online]. Available: https://www.itgovernance.eu/en-ie/eu-cybersecurity-strategy-ie.

[10] "MITRE," [Online]. Available: https://cve.mitre.org/.

[11] "Cyber Security Certification Framework," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.

[12] "EU-CyCLONe," [Online]. Available: https://www.enisa.europa.eu/topics/incident-response/cyclone/?tab=details. [Accessed 10 03 2023].

[13] ENISA, "Cyber Threat Intelligence Overview," [Online]. Available: https://www.enisa.europa.eu/publications/cyberthreat-intelligence-overview. [Accessed 10 03 2023].

[14] "Cybrary," [Online]. Available: https://www.cybrary.it/. [Accessed 10 03 2023].

[15] MITRE, "ATT&CK," [Online]. Available: https://attack.mitre.org/. [Accessed 10 03 2023].

[16] "Insiktintelligence," [Online]. Available: https://www.insiktintelligence.com/. [Accessed 03 10 2023].

[17] "Cyber Threat Alliance (CTA)," [Online]. Available: https://www.cyberthreatalliance.org/.

[18] "Open Cybersecurity Alliance," [Online]. Available: https://opencybersecurityalliance.org/.

[19] "Oasis Open CTI Doocumentation," [Online]. Available: https://oasis-open.github.io/cti-documentation/.

[20] "TAXII 2.1 Specifications," [Online]. Available: https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.docx.

[21] "MISP Threat Sharing," [Online]. Available: https://www.misp-project.org/.

[22] OASIS, "Introduction to STIX," [Online]. Available: https://oasis-open.github.io/cti-documentation/stix/intro.

[23] "OASIS Cyber Threat Intelligence (CTI) TC," [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti.

[24] "Introduction to TAXII," [Online]. Available: https://oasis-open.github.io/cti-documentation/taxii/intro.html.

[25] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar and L. Zhang, "Deep Learning with Differential Privacy," *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS),* pp. 308-318, 2016.

[26] A. C. M. Pathum, P. Bertok and I. Khalil, "Local Differential Privacy for Deep Learning," *IEEE Internet of Things Journal,* vol. 7, no. 7, pp. 5827-5842, 2020.

[27] L. T. Phong, Y. Aono, T. Hayashi and L. Wang, "Privacy-Preserving Deep Learning via Additively Homomorphic Encryption," *IEEE Transactions on Information Forensics and Security,* vol. 13, no. 5, pp. 1333-1345, 2017.

[28] N. Papernot, S. Song, I. Mironov and A. Raghunaathan, "Scalable Private Learning with PATE," *arXiv,* p. 1802.08908, 2018.

[29] C. Zhao, S. Zhao, M. Zhao and Z. Chen, "Secure Multi-Party Computation: Theory, practice and applications," *Information Sciences,* vol. 476, pp. 357-372, 2019.

[30] CyberSEAS consortium, "Deliverable D5.7 "Proactive security for energy Operators"," 2023.

[31] K. Psychogyios, A. Papadakis, S. Bourou, N. Nikolaou, A. Maniatis and T. Zahariadis, "Deep Learning for Intrusion Detection Systems (IDSs) in Time Series Data," *MDPI,* 2023.

[32] C. Acciarini, F. Cappa, P. Boccardelli and R. Oriani, "How can organizations leverage big data to innovate their business models? a systematic literature review," Technovation, 2023.

[33] S. Bose, K. S. Dey and S. Bhattacharjee, "Big data, data analytics and artificial intelligence in accounting: An overview.," *Handbook of Big Data Research Methods: 0, page 32,* 2023.

[34] B. Otto, "A federated infrastructure for european data spaces.," *Communications of the ACM,* vol. 65(4):44–45, 2022.

[35] B. Otto,, M. t. Hompel and S. Wrobel, "Designing Data Spaces: The Ecosystem Approach to Competitive Advantage," *Springer Nature,* 2022.

[36] M. Huber,, S. Wessel, G. Brost and N. Menz, "Building trust in data spaces.," *Designing Data Spaces,* p. 147, 2022.

[37] European Parliament, "General Data Protection Regulation, 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.," 2016.

[38] European Commission., "Shaping Europe's digital future. Digital Strategy.," 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/data-spaces.

[39] CyberSEAS consortium, "Deliverable D6.8 "Rules & Tools for Operators Coordination and Reporting to CERTs in Case of Incidents V2"," CyberSEAS consortium, 2024.

[40] "STIX 2.1 Specifications," [Online]. Available: https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.docx.

[41] CyberSEAS consortium, "Deliverable D3.6," CyberSEAS consortium, 2023.

[42] C. Vandeplas, "Galaxies in MISP," 2023.

[43] C. Vandeplas, "MISP Taxonomies," 2023.

[44] CyberSEAS consortium, "Deliverable 3.6" CyberSEAS Data Analytics Infrastructure V2"," CyberSEAS consortium, 2024.