Harmonizing People, Processes, and Technology for Robust Cybersecurity

D5.2 Evidence Integrity System v1

Document Summary Information

Grant Agreement No	101158555	**Acronym**	CYberSynchrony
Full Title	Harmonizing People, Processes, and Technology for Robust Cybersecurity		
Start Date	01/06/2024	**Duration**	36 months
Project URL	https://www.cybersynchrony.eu/		
Deliverable	D5.2 Evidence Integrity System v1		
Work Package	WP5 Cross-Border Cyber Collaboration and Secure Response (CROSS-CORE)		
Contractual due date	31 May 2025	**Actual submission date**	3 June 2025
Type	OTHER	**Dissemination Level**	Public
Lead Beneficiary	Meridian Group srl (MER)		
Responsible Author	Andrea Purificato (MER), George Karavokiros (BYTE)		
Contributions from	Andrea Purificato (MER), George Karavokiros (BYTE), Alexandros Psychas (MAG), Panayiotis Klitou (EBOS)		

Funded by the European Union

ECCC

Funded by the European Union under Grant Agreement no. 101158555 and supported by the European Cybersecurity Competence Centre (ECCC). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Revision history

Version	Issue Date	Changes	Contributor(s)
0.1	19.03.2025	Initial Deliverable structure	Andrea Purificato (MER)
0.2	31.03.2025	Initial Feedback	Andrea Puricicato (MER), George Karavokiros (BYTE)
0.3	29.04.2025	Review	Andrea Purificato (MER), George Karavokiros (BYTE)
0.4	02.05.2025	Review	Andrea Purificato (MER)
0.5	05.05.2025	Final draft ready for internal review	Andrea Purificato (MER)
0.6	29.05.2025	Final draft ready for QA	Andrea Purificato (MER)
0.9	02.06.2025	Final quality check	Panayiotis Klitou (EBOS)
1.0	03.06.2025	Final version ready for submission	Andrea Purificato (MER)

Disclaimer

The content of the document herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the CYberSynchrony consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© CYberSynchrony Consortium This Deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

[1] According to CYberSynchrony's Quality Assurance Process for reports:

- 3 months before Deliverable's Due Date: Table of Contents ready to be reviewed by WP leader/ Technical Manager/ Quality Manager
- 2 months before Deliverable's Due Date: 50% should be complete. Review by the Quality Manager (& Technical Manager for software).
- 1 month before Deliverable's Due Date:100% should be complete. Review by the Quality Manager and Peer Reviewers.
- M: Sent to PC for Submission to the EC after addressing all comments by Quality Manager and Peer Reviewers

Table of Contents

1 Executive Summary 7
2 Introduction 8
2.1 Mapping CYberSynchrony Outputs 8
2.2 Linkage to other project outputs 8
2.3 Deliverable Structure 9
3 Overview of the Evidence Integrity System v1 (Data Management Plan) 11
3.1 Data Management Plan objectives 11
3.2 Key principles adopted 11
4 CYberSynchrony Data Sharing Context and Classification 12
4.1 Purpose of Cyber Threat Intelligence Data Collection and Generation 12
4.2 Relation to project Objectives 12
4.2.1 WP5 Objective 1: “Facilitate secure data exchange during mutual assistance”. 13
4.2.2 Wp5 Objective 2: “Promote standardized data sharing among MS”. 14
4.2.3 WP5 Objective 3: “Strengthen incident response coordination”. 14
4.3 Assessing Current Cyber Threat Intelligence Data Sharing Practices 14
4.3.1 CSIRTs practices 14
4.3.2 ENISA Practices 15
4.3.3 ECN Practices 15
4.3.4 Challenges Across All Entities 15
5 CYberSynchrony Structured Threat Data and Formats 17
5.1 Defining a Common Data Format 17
5.1.1 Incident Reports 17
5.1.2 Cyber Threat Intelligence 18
5.1.3 Logs 19
5.1.4 Others 19
5.2 Adoption of Structured Frameworks and Exchange Formats 19
5.2.1 STIX: structured threat object encoding 20
5.2.2 TAXII: exchange protocol for STIX data 21
5.2.3 OpenC2: action representation for mitigation and automated response 21
5.2.4 Purpose of each within CYberSynchrony. 22
6 CYberSynchrony Interoperable Exchange and Integrity Mechanisms 24
6.1 Establishing Interoperable Data Exchange Mechanisms 24
6.1.1 RESTful APIS 25
6.1.2 MQTT and Apache kafka 25
6.1.3 Distributed Ledger Technologies (DLT) 26
6.1.4 Platform Integration: MISP, ECN, CSIRT Network 27
6.2 Maintaining Data Integrity Across Borders 27
7 Partner Contributions and Data Inventory 30
7.1 Partner Data Input Matrix 30
8 Conclusions 33
9 References 34

© CYberSynchrony, 2024

List of Figures

Figure 1: Example of TAXII-based Cyber Threat Intelligence Sharing [1]. 21
Figure 2: Cyber Threat Intelligence enrichment using data from malware, IPs, and system behaviour. [2]. 25
Figure 3: Blockchain anchoring process for verifying the integrity of Cyber Threat Intelligence [3]. 28

List of Tables

Table 1: Adherence to CYberSynchrony's GA 8
Table 2: Links to other Project Outputs/Work 9
Table 3: Cyber Threat Intelligence Data Sharing Practices - Summary Table 15
Table 4: Example of a Structured Incident Report in JSON format 18
Table 5: Example of a STIX bundle 20
Table 6: Evidence Integrity System Data Types and Formats 22
Table 7: Partner Data Input Matrix 30

© CYberSynchrony, 2024

Acronyms and abbreviations

Abbreviation / Term	Description
API	Application Programming Interface
APT	Advanced Persistent Threat
CSV	Comma-Separated Values
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
DMP	Data Management Plan
DNS	Domain Name System
DPM	Data Preparation Module
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
JSON	JavaScript Object Notation
LAMP	Linux, Apache, MySQL, PHP (web stack)
LDAP	Lightweight Directory Access Protocol
LEMP	Linux, Nginx (Engine-X), MySQL, PHP (web stack)
LLC	Limited Liability Company
MFA	Multi-Factor Authentication
MISP	Malware Information Sharing Platform
MITRE	MITRE Corporation
MS	Member State(s)
PHP	Hypertext Preprocessor
RAW	Raw data format
RBAC	Role-Based Access Control
REST	Representational State Transfer
SAML	Security Assertion Markup Language
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SOC	Security Operations Center

© CYberSynchrony, 2024

STIX	Structured Threat Information Expression
TAXII	Trusted Automated eXchange of Indicator Information
TLP	Traffic Light Protocol
UFT	Unalterable Forensic Techniques
WHOIS	Domain Registry Lookup Protocol
WP	Work Package
XML	eXtensible Markup Language
YAML	YAML Ain't Markup Language

© CYberSynchrony, 2024

1 Executive Summary

This deliverable, D5.2 "Evidence Integrity System v1 (Data Management Plan)", presents the foundational framework and operational guidelines for ensuring the integrity, authenticity, and interoperability of cyber threat intelligence (CTI) exchanged across Member States (MS) within the CYberSynchrony project. As a core output of Work Package 5 (CROSS-CORE), the Evidence Integrity System is designed to address the critical need for secure, standardized, and trustworthy data sharing in support of cross-border cyber incident response and mutual assistance.

The document outlines the objectives, methodologies, and technical mechanisms underpinning the Evidence Integrity System. It details how the Data Management Plan (DMP) acts as a living document, evolving alongside project implementation to reflect changes in data handling, partner contributions, and regulatory requirements. The DMP establishes clear processes to guarantee that digital evidence, ranging from low-level indicators of compromise to complex incident reports, remains secure, unaltered, and legally defensible throughout its lifecycle.

Key achievements of this deliverable include:

- **Adoption of Standardized Data Formats and Protocols:** the system leverages widely recognized standards such as STIX and TAXII for structured CTI representation and automated exchange, ensuring semantic consistency and machine-readability across diverse platforms. Integration with RESTful APIs, MQTT/Kafka messaging, and Distributed Ledger Technologies (DLT) further enhances interoperability and real-time collaboration1.
- **Data Integrity and Validation Mechanisms:** the Evidence Integrity System employs multi-layered validation, including checksums for rapid verification and blockchain anchoring for tamper-evident, time-stamped records. These mechanisms provide robust assurance that shared intelligence remains unaltered, supporting both operational trust and legal admissibility1.
- **Alignment with European Cybersecurity Ecosystem:** the deliverable documents seamless integration with key EU infrastructures such as MISP, the CSIRT Network, and the European Cybersecurity Network (ECN), reinforcing the project's commitment to interoperability and operational continuity. Structured partner contributions and a comprehensive data inventory ensure traceability and accountability throughout the consortium1.
- **Support for Secure, Real-Time, and Automated Incident Response:** by enabling the secure exchange of actionable intelligence and automating mitigation workflows (e.g., via OpenC2), the system empowers Member States to coordinate responses rapidly and effectively, reducing fragmentation and enhancing Europe's collective cyber resilience1.

The main findings highlight persistent challenges in cross-border CTI sharing, such as trust deficits, legal constraints, and standardization gaps, and demonstrate how CYberSynchrony's unified models and protocols address these barriers. The Evidence Integrity System v1 establishes a scalable, legally robust, and operationally efficient foundation for CTI exchange, directly supporting the project's strategic objectives of trust, transparency, and resilience.

Looking ahead, this deliverable will be regularly updated to keep pace with technological advancements, regulatory developments, and evolving operational requirements. Future versions will integrate feedback from consortium partners and stakeholders, address new and emerging threats, and further improve automation, compliance, and auditability. The final contributions, enhancements, and outcomes will be comprehensively reflected in D5.4, which will serve as the updated version of this deliverable.

© CYberSynchrony, 2024

2 Introduction

2.1 Mapping CYberSynchrony Outputs

This section presents the CYberSynchrony's Grant Agreement (GA) commitments, as extracted from the formal deliverable and task description, in respect to their outputs and work to be performed.

Table 1: Adherence to CYberSynchrony's GA

Component no	Component title	Respective Document Chapter(s)	Justification
DELIVERABLE			
D5.2	Evidence Integrity System v1 (Data Management Plan)	Chapter 4-8	In the context of WP5, which aims to facilitate secure data exchange, promote standardized data sharing, and strengthen incident response coordination among MS, the "Evidence Integrity System v1" directly supports the objective of ensuring the trustworthiness of data exchanged, especially in situations of mutual assistance where the reliability and integrity of digital evidence are paramount.
TASKS			
T5.2	Task 5.2 - Advancing Uniform Data Sharing Standards	Chapter 3,4,5,6,7	This task emphasizes the importance of standardized data sharing protocols among MS. A unified approach (as per Chapters 4,5,6,7) ensures clear understanding and optimal use of shared data (as per Chapters 3,4), eliminating potential ambiguities from diverse formats. Standardization enhances interoperability and maintains data integrity during cross-border exchanges. The ultimate goal is seamless collaboration between MS to strengthen collective cyber defences

2.2 Linkage to other project outputs

The D5.2 "Evidence Integrity System v1 (Data Management Plan)" deliverable is closely interconnected with other project outputs and specific deliverables within the CYberSynchrony project, particularly the WP5.

Its role is both foundational and integrative, providing the data management, integrity, and interoperability framework that underpins secure cyber threat intelligence (CTI) exchange across the consortium and with external stakeholders.

© CYberSynchrony, 2024

Table 2: Links to other Project Outputs/Work

WP Number	Task Number	Deliverable Number related	Content
WP5	T5.1	D5.1 Secure Data Exchange Platform v1	D5.1 delivers the initial technical platform for secure, encrypted data exchange between Member States. D5.2 builds on this by specifying the data management processes, integrity controls, and standardized formats (such as STIX, TAXII, OpenC2) that must be applied to all data handled by the platform. The evidence integrity mechanisms described in D5.2 ensure that the data exchanged through D5.1 remains trustworthy, traceable, and compliant with legal requirements

2.3 Deliverable Structure

The structure of Deliverable D5.2 "Evidence Integrity System v1 (Data Management Plan)" is organized to provide a logical flow from the context and objectives of the work package to the technical and operational details of the evidence integrity system. Below is a summary of the main chapters and their content:

- **Chapter 1: Executive Summary**
  Provides a concise overview of the deliverable, summarizing its purpose, key findings, main conclusions, and its value to the overall project.
- **Chapter 2: Introduction**
  Introduces the scope and context of the deliverable, including:
  - Mapping of CYberSynchrony outputs to project objectives.
  - Linkages to other project deliverables and outputs.
  - A brief description of the deliverable's structure.
- **Chapter 3: Overview of the Evidence Integrity System v1 (Data Management Plan)**
  Outlines the objectives of the Data Management Plan, the key principles adopted, and the rationale behind the evidence integrity system.
- **Chapter 4: CYberSynchrony Data Sharing Context and Classification**
  Explains the purpose and context of cyber threat intelligence (CTI) data collection and generation, its relation to project objectives, and an assessment of current CTI sharing practices across relevant European entities.
- **Chapter 5: CYberSynchrony Structured Threat Data and Formats**
  Describes the approach to defining common data formats for CTI, including the adoption of standards such as STIX, TAXII, and OpenC2, and the rationale for their use within the project.
- **Chapter 6: CYberSynchrony Interoperable Exchange and Integrity Mechanisms**
  Details the mechanisms for establishing interoperable data exchange, including RESTful APIs, MQTT/Kafka, Distributed Ledger Technologies (DLT), and integration with platforms like MISP, ECN, and the CSIRT Network. It also covers methods for maintaining data integrity across borders.
- **Chapter 7: Partner Contributions and Data Inventory**
  Documents the contributions of each project partner, including the types of data provided, their sources, formats, and integration into the overall system.

© CYberSynchrony, 2024

- **Chapter 8: Conclusions**
  Summarizes the main outputs and value added by the deliverable, discusses best practices, potential improvements, and outlines the way forward for future iterations.

This structure ensures that the deliverable is comprehensive, logically organized, and accessible to both technical and non-technical stakeholders, supporting clarity and traceability throughout the document.

© CYberSynchrony, 2024

3 Overview of the Evidence Integrity System v1 (Data Management Plan)

This Evidence Integrity System, as Data Management Plan (DMP), is essentially a set of questions answered at an appropriate level of detail to effectively share cyber threat intelligence across MS.

3.1 Data Management Plan objectives

This DMP is intended to be a **living document** in which information can be made available on a finer level of granularity through updates as the implementation of the project progresses and when significant changes occur.

The deliverable will outline or provide a process, a system or guidelines designed to guarantee that digital data (evidence) remains secure, unchanged and authentic.

In the context of WP5, which aims to facilitate secure data exchange, promote standardized data sharing, and strengthen incident response coordination among MS, the "Evidence Integrity System v1" directly supports the objective of ensuring the trustworthiness of data exchanged, especially in situations of mutual assistance where the reliability and integrity of digital evidence are paramount.

3.2 Key principles adopted

This document provides a comprehensive framework tailored to the specific needs of WP5's *Evidence Integrity System* while ensuring alignment with best practices in data management planning.

© CYberSynchrony, 2024

4 CYberSynchrony Data Sharing Context and Classification

The effective collection and utilization of cyber threat intelligence (CTI) across EU Member States is a cornerstone for coordinated and timely responses to cyber incidents. Structured intelligence sharing allows national authorities to identify cross-border threats early, anticipate evolving attack vectors, and align their response strategies under a unified operational perspective. Beyond its technical value, this process strengthens institutional trust and facilitates mutual support in high-impact scenarios that transcend national boundaries. As threat actors grow more sophisticated, the ability to act upon accurate, contextualized intelligence becomes indispensable for ensuring cyber resilience across Europe.

Despite growing awareness and initiatives at the EU level, several discrepancies still exist in how cybersecurity-related information is interpreted, formatted, and exchanged among Member States. These include divergences in terminologies, threat classification taxonomies, metadata structures, and severity assessment models. Such inconsistencies can obstruct real-time collaboration and may lead to incomplete or misaligned interpretations during critical incident response windows. Addressing these gaps requires a concerted effort to enhance both semantic clarity and technical compatibility across data-sharing systems.

Work Package 5 (WP5) of the CYberSynchrony project is specifically designed to overcome these challenges. Through Task 5.2, the project promotes the adoption of shared data representation models and structured exchange mechanisms, enabling seamless interoperability between national actors. Within this framework, data functions as both an operational asset and a trust vehicle, central to the CROSS-CORE infrastructure. By applying recognized standards (such as STIX, TAXII) and secure exchange protocols, WP5 ensures that cyber threat intelligence and incident-related data are consistently validated, securely transmitted, and operationally meaningful across all participating entities. In doing so, it contributes directly to the broader objectives of trust, transparency, and integrity of evidence envisioned by the project.

4.1 Purpose of Cyber Threat Intelligence Data Collection and Generation

In the context of CYberSynchrony, the collection and generation of cyber threat intelligence (CTI) serves a targeted operational purpose: to enable dynamic, evidence-driven coordination between national actors and cybersecurity platforms. Rather than relying solely on retrospective analysis or manual reporting, cyber threat intelligence produced through the project supports real-time threat detection, risk assessment, and cooperative incident handling.

The project facilitates the generation of cyber threat intelligence at multiple layers: from low-level indicators (such as IP addresses, file hashes, or malicious domains) to behavioural patterns and tactics, techniques, and procedures (TTPs) attributed to threat actors. This intelligence is intended to feed not only human decision-making, but also automated detection systems such as intrusion detection systems (IDS), security information and event management platforms (SIEM), and threat scoring models.

4.2 Relation to project Objectives

The structured generation, categorization, and cross-border sharing of Cyber Threat Intelligence (CTI) lie at the heart of CYberSynchrony's contribution to a resilient European cybersecurity ecosystem. These activities enable consistent, secure, and reliable information exchange that underpins trust, enhances real-time situational awareness, and supports coordinated responses to cyber threats across Member States.

CROSS-CORE, the technical implementation of WP5, integrates CTI into strategic workflows that support prevention, detection, response, recovery, and legal cooperation. It establishes shared protocols and data structures that facilitate interoperability among national actors, empowering them to act in unison even under differing legal or infrastructural constraints.

CTI is not merely a stream of raw data but a dynamic operational tool that supports CYberSynchrony’s overarching mission: fostering cross-border collaboration, reducing fragmentation, and strengthening Europe’s

© CYberSynchrony, 2024

collective cybersecurity posture. The alignment with project objectives is reflected across three central pillars of WP5.

4.2.1 WP5 Objective 1: "Facilitate secure data exchange during mutual assistance".

Effective mutual assistance in cyber crises relies on the ability to exchange data that is not only timely and relevant but also secure and trustworthy. CTI shared between Member States must maintain its confidentiality and integrity throughout its lifecycle.

CROSS-CORE supports this objective by implementing mechanisms for encrypted transmission, evidence traceability, and chain-of-custody assurance. These guarantees are essential for legal admissibility and institutional trust during coordinated incident response operations. By integrating CTI into secure communication pipelines, the system reinforces a unified operational picture and enables evidence-based support among Member States.

In the context of CYberSynchrony, the collection and generation of cyber threat intelligence (CTI) serves a targeted operational purpose: to enable dynamic, evidence-driven coordination between national actors and cybersecurity platforms. Rather than relying solely on retrospective analysis or manual reporting, CTI produced through the project supports real-time threat detection, risk assessment, and cooperative incident handling.

CYberSynchrony facilitates CTI generation at multiple layers, from low-level indicators (e.g., IP addresses, file hashes, or malicious domains) to behavioural patterns and tactics, techniques, and procedures (TTPs) attributed to threat actors. This intelligence feeds both human-driven analysis and automated detection systems, including Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) platforms, and threat scoring models.

Equally important is the transformation of collected digital evidence into verifiable and shareable intelligence. Within the CROSS-CORE module, CTI supports:

- early collaborative detection of multi-jurisdictional campaigns,
- joint analysis and attribution activities, and
- legal/investigative procedures where evidence integrity and chain of custody are critical.

CYberSynchrony emphasizes an operational framework for structuring, categorizing, and utilizing CTI to maximize its impact. CTI in the project is classified as:

- **Indicators of Compromise (IOCs):** Technical artefacts (e.g., malicious IPs, domains, file hashes) that support immediate threat detection.
- **Tactics, Techniques, and Procedures (TTPs):** Behavioural patterns mapped to frameworks such as MITRE ATT&CK, informing proactive defences.
- **Attribution Elements:** Data linking threats to actor groups, supporting geopolitical response and prioritization.
- **Behavioural Patterns and Anomalies:** Contextual signals of insider threats or novel attack vectors.

CTI also supports:

- **Customized risk analysis**, enabling MS to understand sector-specific exposure and tailor mitigation strategies accordingly.
- **Cybersecurity awareness and training initiatives**, particularly within the CYBERWISE module, where shared CTI informs real-world learning scenarios.
- **Policy harmonization**, by promoting common understanding and standards adoption, in alignment with EU-wide cybersecurity objectives.

© CYberSynchrony, 2024

In short, CTI in CYberSynchrony is not an abstract data stream, but a vital operational asset. Its structured use enhances cross-border cooperation, increases the responsiveness of EU cybersecurity posture, and contributes directly to trust, resilience, and situational awareness across all Member States.

4.2.2 Wp5 Objective 2: "Promote standardized data sharing among MS".

Inconsistent data formats and terminology across Member States have historically hampered effective collaboration. CYberSynchrony addresses this by structuring CTI into interoperable formats, such as Indicators of Compromise (IOCs), Tactics, Techniques, and Procedures (TTPs), attribution data, and behavioural anomalies, aligned with recognized standards such as STIX and TAXII.

This standardization enhances machine-readability, eliminates semantic ambiguities, and enables automated ingestion into tools like SIEM and SOAR platforms. As a result, national cybersecurity agencies can share, interpret, and act upon CTI with greater clarity and consistency, even across heterogeneous infrastructures.

4.2.3 WP5 Objective 3: "Strengthen incident response coordination".

Coordinated incident response requires more than shared data, it requires synchronized understanding, joint planning, and operational alignment. CYberSynchrony supports this by using CTI to power collaborative analysis, strategic attribution, and real-time alerting.

Structured CTI allows participating entities to respond to threats not in isolation, but as a unified European front. It supports detailed planning, forensic investigation, and policy-level decision-making, all grounded in a shared, validated intelligence base. Through CROSS-CORE, CTI becomes the backbone of a harmonized European incident response capability.

4.3 Assessing Current Cyber Threat Intelligence Data Sharing Practices

Practical cyber threat intelligence (CTI) data sharing is essential for enabling coordinated and timely responses to cyber incidents across Member States. While there has been progress in harmonizing CTI exchange practices, critical challenges remain, particularly regarding interoperability, semantic consistency, and technical standardization.

Three key actors in the European cybersecurity landscape, CSIRTs, ENISA, and the European Cybersecurity Network (ECN), play pivotal roles in the design, implementation, and evolution of CTI sharing mechanisms. Each entity brings a distinct scope and methodology, resulting in varying degrees of maturity, adoption, and integration.

Below is a consolidated assessment of their practices.

4.3.1 CSIRTs practices

CSIRTs play a central role in sharing cyber threat intelligence to combat cyber incidents effectively (see [4]).

Their practices include:

- **Standards and Protocols**: Use of formats like Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII) for structured data sharing. However, the lack of universally adopted standards often leads to interoperability challenges.
- **Incident reporting and communication**: Implementation of secure channels (e.g., online portals, encrypted forms) for incident reporting and dissemination of threat intelligence. Frameworks like the Traffic Light Protocol (TLP) are employed to classify information sensitivity.
- **Trust and legal challenges**: Stakeholder reluctance to share sensitive data due to trust issues, legal ambiguity, and data protection constraints limits cross-border collaboration and reduces effectiveness

© CYberSynchrony, 2024

4.3.2 ENISA Practices

ENISA coordinates EU-wide cybersecurity initiatives and provides guidance for standardizing CTI exchange (see [5]). Its efforts include:

- **Cybersecurity Threat Landscape (CTL) methodology**: ENISA developed the CTL methodology to standardize data collection, analysis, and dissemination processes. This framework aims to improve situational awareness and support decision-making with timely, actionable intelligence.
- **Sectoral collaboration**: ENISA supports Information Sharing and Analysis Centers (ISACs), which facilitate collaboration between public and private sectors, particularly in critical infrastructure protection. These efforts aim to build trust within communities and enhance collective cybersecurity resilience.
- **Automation potential**: while ENISA emphasizes systematic processes, it acknowledges that much of the work remains manual. Automation is seen as a future goal to enhance efficiency in CTI sharing.

4.3.3 ECN Practices

The European Cybersecurity Network (ECN) promotes advanced tools and privacy-preserving models for secure CTI sharing (see [6]). These include:

- **Threat Intelligence Platforms (TIPs)**: ECN advocates for TIPs like the Malware Information Sharing Platform (MISP) to enable secure, privacy-preserving data exchange. These platforms incorporate features such as access control, anonymization techniques (e.g., K-anonymity), and blockchain-based auditing to ensure data integrity.
- **Collaboration models**: ECN emphasizes building trust through privacy-enhancing technologies and federated learning models, which allow organizations to share insights without exposing sensitive data. This approach enhances detection capabilities while maintaining confidentiality.
- **Actionable intelligence**: ECN stresses the importance of sharing high-quality, relevant, and actionable intelligence that can be immediately leveraged by organizations to mitigate threats.

4.3.4 Challenges Across All Entities

Despite their specific mandates, CSIRTs, ENISA, and ECN face shared challenges in CTI sharing:

- **Trust issues**: a lack of trust among stakeholders often limits open sharing of sensitive threat intelligence.
- **Legal and Privacy concerns**: Varying national laws and strict data protection regimes obstruct smooth information flow.
- **Standardization gaps**: Fragmented data formats, taxonomies, and severity models reduce semantic alignment and create operational inefficiencies.

CYberSynchrony, through Task 5.2, aims to resolve these issues by developing unified CTI models, interoperable data-sharing protocols, and legally robust exchange mechanisms. These innovations will support faster, more coordinated, and more trusted incident responses across Europe.

Table 3: Cyber Threat Intelligence Data Sharing Practices - Summary Table

Organization	Key Practices	Challenges
CSIRTs	Use of STIX/TAXII; secure incident reporting; TLP tagging	Interoperability; trust deficits

© CYberSynchrony, 2024

ENISA	CTL methodology; ISAC collaboration; automation goals	Manual processes; fostering trust
ECN	TIPs with Privacy-Enhancing Technologies (PETs)/blockchain; federated learning models	Privacy concerns; standardization gaps

© CYberSynchrony, 2024

5 CYberSynchrony Structured Threat Data and Formats

The efficient exchange of cyber threat intelligence (CTI) relies heavily on consistent data structures and standardized formats. CYberSynchrony places a strong emphasis on organizing and structuring CTI to ensure clarity, consistency, and effective communication across diverse cybersecurity platforms and stakeholders.

A common structure for organizing threat data enables interoperability, automation, and seamless integration across national systems. In this context, three core schema types are commonly used:

- **Observables:** Raw data points or artifacts detected in systems, such as IP addresses, file hashes, domain names, or registry keys. Observables represent factual, measurable elements that do not inherently indicate malicious activity.
- **Indicators:** Combinations or patterns of observables that suggest potential malicious activity. For instance, an IP address combined with a known malicious file hash forms an Indicator of Compromise (IOC), helping organizations detect and respond to threats.
- **Incidents:** Document actual security events or breaches. Incidents include detailed information such as attack timelines, affected assets, attacker tactics, and overall organizational impact.

5.1 Defining a Common Data Format

In the context of CYberSynchrony, defining a standard data format is crucial to enhancing the efficiency and reliability of cyber threat intelligence (CTI) exchange among Member States and organizations. By standardizing the structure and content of CTI data, we ensure that cyber threats can be detected, analysed, and mitigated with precision and speed. The ability to exchange structured, standardized data is a foundational principle for cross-border collaboration in cybersecurity.

The following schema types form the basis of CYberSynchrony's data structuring strategy.

5.1.1 Incident Reports

Incident reports are a core element of any cybersecurity response, documenting the full details of an event to ensure proper follow-up and resolution. A well-structured incident report makes it easier to share actionable data across organizations and ensures that critical information is captured systematically. This enables faster decision-making, improved incident handling, and better preparedness for future events.

Key elements in a typical incident report include:

- Event type: The type of incident helps categorize the threat and determines the response needed. For example, identifying a ransomware attack as the event type allows security teams to implement specific response procedures that are different from those used for a data breach. A standardized classification of event types ensures that security teams can act appropriately, without confusion or delays.
- Vector: The attack vector describes the path through which the attacker gained access to the system. Common attack vectors include email phishing, exploiting vulnerabilities in web applications, or social engineering tactics. By clearly identifying the vector, organizations can implement more targeted defenses to block similar types of attacks in the future. A standardized format for recording attack vectors helps ensure that responses are tailored to the method of the attack.
- Asset: The affected asset refers to the specific system or resource that was targeted in the attack, such as a server, database, or endpoint device. Identifying the affected asset helps organizations assess the level of risk and prioritize responses based on the asset's criticality. For instance, a compromised database containing personal data may require more urgent remediation than a workstation that was affected by a lesser-known exploit.
- Impact: The impact of the incident refers to the consequences the attack had on the organization, including data loss, financial damage, or service disruption. A standardized description of impact helps

© CYberSynchrony, 2024

determine the severity of the incident and guides the allocation of resources for response and recovery. It also ensures that organizations can assess the long-term effects of the incident on business operations, customer trust, and regulatory compliance.

Threat intelligence provides actionable insights into ongoing or future cyber threats. For threat intelligence to be valuable and practical, it must be organized in a standardized format so that it can be easily shared, processed by different security tools, and acted upon quickly.

To further illustrate the importance of standardized data formats, consider the following example of a structured cyber incident report using JSON. Such a format ensures that incident data can be easily parsed, analysed, and acted upon by both automated systems and human operators.

Table 4: Example of a Structured Incident Report in JSON format

JSON

```
{
  "incident_id": "INC-2025-0456",
  "timestamp": "2025-04-26T14:32:00Z",
  "event_type": "Phishing Attempt",
  "vector": "Email",
  "affected_asset": "Employee Email Account",
  "impact": "Credential Theft Risk",
  "iocs": [
    { "type": "url", "value": "http://malicious-example.com" },
    { "type": "ip", "value": "198.51.100.23" }
  ],
  "ttype": "T1566.001",
  "description": "Spearphishing via email with a malicious link redirecting to a fake login page."
}
```

In this example, the incident report captures critical elements such as the type of attack, the method of compromise, the affected asset, the impact assessment, and the relevant Indicators of Compromise (IOCs). Utilizing a standardized JSON structure not only facilitates faster integration across cybersecurity tools but also improves the accuracy and speed of incident triage, analysis, and response.

5.1.2 Cyber Threat Intelligence

CTI includes several core elements that must be standardized for effective sharing:

- Indicators of Compromise (IOCs): IOCs are specific data points or artifacts that suggest a system has been compromised. These can include IP addresses, file hashes, domains, or URLs associated with malicious activity. For example, a malicious IP address identified as part of a botnet can be added to a blocklist to prevent further access. The standardization of IOCs ensures that they can be used by security teams worldwide to identify and block threats quickly.
- Tactics, Techniques, and Procedures (TTPs): TTPs describe the methods and strategies employed by threat actors during an attack. For instance, a common TTP might involve using phishing emails as the initial tactic, malicious attachments as the technique, and payload delivery as the procedure. By understanding these patterns, organizations can anticipate future attacks and develop defence mechanisms accordingly. Standardizing the description of TTPs enables security professionals to recognize attack patterns and respond more effectively.
- Attribution: Attribution is the process of identifying the threat actor behind an attack. This could involve linking the attack to a known cybercriminal group or a state-sponsored threat actor. Understanding the

© CYberSynchrony, 2024

motivations, capabilities, and strategies of the threat actor allows organizations to tailor their defences accordingly. Standardized attribution data enables a shared understanding of the threat landscape and improves global collaboration in countering threats.

Using shared formats like STIX/TAXII ensures CTI is machine-readable, shareable, and actionable across platforms.

5.1.3 Logs

Logs are a fundamental component of any cybersecurity infrastructure. They provide detailed event traces that are crucial for detecting and validating security incidents in real time. CYberSynchrony emphasizes the structured handling of logs to support interoperability, automation, compliance, and cross-platform analysis.

Key aspects include:

- **Content and Sources:** Logs are generated by systems, applications, and security tools within an organization's infrastructure. They record critical activity such as user authentication, system events, application errors, file access, and network traffic. This information allows security professionals to track what occurred before, during, and after an incident.
- **Security Utility:** Logs serve as the first line of defence in detecting suspicious or malicious activity. For example:
  - A failed login attempt followed by multiple retries may signal a brute-force attack.
  - Access to sensitive files at unusual hours can indicate potential insider threats or account compromise.
  - Correlating logs from multiple systems provides a more complete forensic picture during investigations.
- **Standardized Formats:** To maximize their effectiveness and interoperability, logs must be structured in machine-readable, consistent formats. The two most common are:
  - **JSON (JavaScript Object Notation):** Lightweight, human-readable, ideal for SIEM integration and widely used in web applications. Its structure allows fast parsing and processing by automated tools.
  - **XML (eXtensible Markup Language):** Suitable for complex or hierarchical logging needs, with metadata support. While more verbose than JSON, it offers greater flexibility for nested relationships.
- **Automation and Real-Time Response:** When logs follow consistent schemas, automation tools (e.g., SIEM, SOAR) can parse them efficiently and trigger real-time alerts. This supports early detection, correlation of threat signals, and immediate mitigation actions.
- **Compliance and Auditability:** Structured logs help meet regulatory and cybersecurity framework requirements (e.g., NIS2, ISO 27001, GDPR). They facilitate reliable log retention, retrieval, and reporting during audits or incident post-mortems.

This structured approach to logging aligns with CYberSynchrony's goal of enabling consistent, secure, and actionable event traceability using standardized formats such as JSON and XML across Member States.

5.1.4 Others

Other formats may include vulnerability reports, policy configurations, or machine learning outputs for anomaly detection. These may also be standardized using schema extensions compatible with CTI pipelines.

5.2 Adoption of Structured Frameworks and Exchange Formats

For cyber threat intelligence (CTI) to be shared effectively across different systems and organizations, it is critical to adopt structured frameworks and standardized data formats. These frameworks provide essential rules and protocols that ensure consistent, secure, and interoperable exchange of data between various cybersecurity

© CYberSynchrony, 2024

platforms. By adopting these standardized formats, organizations can not only share information more effectively but also use it to respond to threats with greater speed and accuracy.

In practical operational environments, structured frameworks and standardized protocols play a crucial role in ensuring the timely and effective exchange of threat information. For instance, when a national CSIRT identifies a new phishing campaign targeting critical infrastructure, it can create a detailed STIX object that captures all relevant Indicators of Compromise (IOCs), such as malicious email addresses, URLs, and payload hashes.

This structured data is then uploaded to a MISP (Malware Information Sharing Platform and Threat Sharing) instance, a widely adopted open-source threat intelligence platform that supports STIX/TAXII formats. Through MISP's TAXII server capabilities, authorized Member States or trusted partners can automatically pull the newly shared intelligence using TAXII clients.

This real-time, machine-readable CTI dissemination enables rapid updates to local SIEM systems, intrusion detection tools, and security orchestration workflows. By embedding structured CTI exchanges through frameworks like STIX and TAXII, CYberSynchrony enhances the ability of Member States to coordinate proactive defences, quickly adapt to evolving threats, and maintain a cohesive cybersecurity posture across borders.

5.2.1 STIX: structured threat object encoding

STIX is one of the most widely adopted standardized formats for representing and exchanging CTI. Developed by MITRE and managed by OASIS, STIX provides a structured language that enables organizations to describe cyber threats, threat actors, incidents, and attack patterns in a uniform and machine-readable way (see [1]).

The format allows for the detailed representation of threat data, such as TTPs, indicators of compromise (IOCs), vulnerabilities, and attack vectors. This enables the full lifecycle of a threat to be described, from detection to response. For instance, a STIX bundle can capture all phases of a ransomware campaign, from phishing delivery to payload execution and ransom demand, enabling better situational awareness.

STIX also facilitates automation in detection and response. Security systems can ingest STIX objects and trigger predefined responses, such as updating firewalls or raising alerts.

Below is an example of a STIX bundle containing two domain objects: an indicator for a SHA256 file hash and a malware object describing CryptoLocker ransomware:

Table 5: Example of a STIX bundle

STIX

```
json
{
 "type": "bundle",
 "id": "bundle--12345678-1234-5678-1234-567812345678",
 "objects": [
  {
   "type": "indicator",
   "id": "indicator--87654321-4321-8765-4321-876543218765",
   "created": "2025-04-01T10:50:00.000Z",
   "modified": "2025-04-01T10:50:00.000Z",
   "pattern": "[file:hashes.'SHA256' =
'abcdef1234567890abcdef1234567890abcdef1234567890abcdef1234567890']",
   "valid_from": "2025-04-01T10:50:00.000Z"
  },
  {
   "type": "malware",
   "id": "malware--23456789-2345-6789-2345-678923456789",
   "created": "2025-04-01T10:50:00.000Z",
```

© CYberSynchrony, 2024

```
    "modified": "2025-04-01T10:50:00.000Z",
    "name": "CryptoLocker",
    "malware_types": ["ransomware"],
    "description": "CryptoLocker ransomware encrypts files and demands payment for decryption."
  }
 ]
}
```


STIX objects can be used to describe cyber threats in a structured manner, facilitating automated analysis and sharing.

5.2.2 TAXII: exchange protocol for STIX data

TAXII is a protocol designed to facilitate the secure, automated exchange of STIX data between systems. Working alongside STIX, TAXII ensures that CTI can be pushed, pulled, or subscribed to between trusted partners using HTTPS and JSON-based APIs (see [2]).

This capability supports real-time collaboration and automation. For example, when a national CSIRT uploads STIX-formatted IOCs into a MISP platform, authorized TAXII clients across Member States can automatically retrieve the latest threat data and integrate it into local SIEM or EDR systems for immediate action.

TAXII also enhances international cybersecurity coordination. If a participating organization detects a malicious IP address targeting critical infrastructure, that IOC can be shared in real time via TAXII with trusted partners, allowing them to proactively block the threat and prevent broader impact. This mechanism accelerates information flow and empowers collective response.

The protocol supports multiple exchange models, such as hub-and-spoke, source/subscriber, and peer-to-peer, offering flexibility in deployment and governance. It ensures confidentiality and integrity of shared data through secure transport mechanisms and authentication protocols.

The following figure demonstrates how TAXII facilitates the secure and automated exchange of threat intelligence data, such as STIX, between various organizations. This mechanism plays a key role in enabling rapid detection and response to cyber threats.

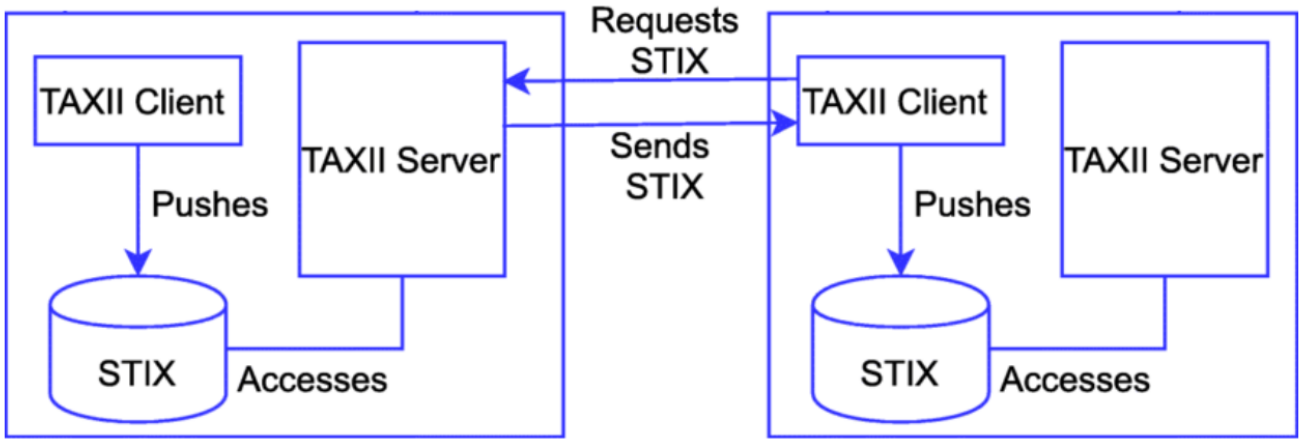

Figure 1: Example of TAXII-based Cyber Threat Intelligence Sharing [1].

5.2.3 OpenC2: action representation for mitigation and automated response

OpenC2 is a standardized, open-source language designed to enable automated, machine-to-machine communication for cyber defence. It allows security systems to issue and respond to commands for mitigating threats without manual intervention, improving both speed and coordination across cybersecurity infrastructures (see [3]).

© CYberSynchrony, 2024

The OpenC2 framework uses a **producer-consumer model**, where a managing system (Producer) sends standardized action commands to a responding system (Consumer), such as a firewall, EDR, or network controller. The Consumer executes the requested action and may provide feedback.

Key advantages of OpenC2 include:

- **Automated Response Coordination:** OpenC2 enables pre-defined, real-time responses to detected threats.
  For example:
  - A SIEM detects abnormal network traffic.
  - It triggers OpenC2 commands to:
    - Block a suspicious IP at the firewall,
    - Isolate an endpoint via the EDR,
    - Notify the SOC team for further investigation.
- **Reduced Reaction Time:** By automating threat mitigation workflows, OpenC2 minimizes delays between detection and action, dramatically increasing the effectiveness of cyber response operations.
- **Interoperability and Vendor Neutrality:** As an open and extensible language, OpenC2 works across diverse security tools and platforms, eliminating reliance on proprietary protocols.
- **Adaptability:** The language is designed to support multiple cyber defence functions, from basic containment to advanced orchestration tasks across SOAR ecosystems.

5.2.4 Purpose of each within CYberSynchrony.

The following table shows the origin of the data, the related WP number and the format, in which the data will be presumably stored.

The following table shows the data type, the origin of the data, the related WP number and the format, in which the data will be presumably stored.

Table 6: Evidence Integrity System Data Types and Formats

#	Data Type	Type	Origin	WP#	Format
1	Incident Report	Document/Structured	CSIRTs, SOCs, National Platforms	WP5	JSON, PDF
2	Indicator of Compromise (IOC)	Structured Data	Security Sensors, MISP, TIPs	WP5, WP3	STIX, JSON
3	Tactics, Techniques & Procedures (TTPs)	Structured Data	Threat Analysis, MITRE Framework, MISP	WP5, WP3	STIX, JSON
4	Attribution Data	Structured Data	Law Enforcement, CERTs, Analysts	WP5	STIX, JSON
5	Behavioural Anomalies	Structured Data	SIEM, EDR, ML Systems	WP5	JSON, CSV
6	Logs	Raw/Parsed Data	IT/OT Systems, Sensors	WP5	JSON, XML, CSV

© CYberSynchrony, 2024

7	Vulnerability Reports	Document/Structured	Security Teams, Vulnerability Scanners	WP5	PDF, JSON
8	Policy Configurations	Document	IT Admins, GRC Tools	WP5	YAML, JSON
9	OpenC2 Action Commands	Structured Data	SOAR, SIEM, Automated Response Systems	WP5	JSON (OpenC2 schema

© CYberSynchrony, 2024

6 CYberSynchrony Interoperable Exchange and Integrity Mechanisms

The effectiveness of cyber threat intelligence sharing depends on ensuring interoperability and data integrity across different platforms. This is especially important for CYberSynchrony, which aims to create a seamless and secure ecosystem where Member States and cybersecurity platforms can easily exchange information and collaborate in real-time. The adoption of standardized frameworks and protocols ensures that data can be shared consistently and securely, helping organizations across Europe to respond swiftly and decisively to emerging threats.

CYberSynchrony aims to ensure that the exchange of cyber threat intelligence is secure and compatible with the various cybersecurity platforms used across the European Union. This is achieved through the use of standardized data formats, encryption techniques, and secure data-sharing protocols that allow for the safe transfer of sensitive information.

In practice, this means that organizations will be able to integrate their internal security systems with EU platforms such as MISP (Malware Information Sharing Platform), CSIRT networks, and national CERT systems. By adhering to open standards such as STIX and TAXII, and implementing automated data exchange protocols, CYberSynchrony ensures that threat intelligence can be shared seamlessly between different systems, increasing the speed and effectiveness of collaborative defence efforts.

Moreover, the secure exchange ensures that data shared between organizations is protected against unauthorized access, ensuring that sensitive threat intelligence is exchanged in a way that complies with EU data protection regulations.

A key element is validating data as it is shared across borders. The integrity and accuracy of the cyber threat intelligence being exchanged are essential for ensuring practical response actions. The project focuses on implementing data validation mechanisms that ensure that CTI remains accurate and unaltered during the exchange process, even when shared between different jurisdictions.

To ensure the accuracy of the shared data, checksum mechanisms and blockchain anchors are used. These techniques allow organizations to verify that the data has not been altered during transmission. For instance, before sharing critical threat data, a checksum value is generated for that data, and the exact value is recalculated upon receipt. If the values match, it ensures the data's integrity.

Additionally, cross-border data validation ensures that different organizations, regardless of their location, can rely on the shared intelligence. By leveraging standardized formats and shared validation protocols, CYberSynchrony ensures that threat intelligence remains reliable and trustworthy, even when it is exchanged across different countries and platforms.

6.1 Establishing Interoperable Data Exchange Mechanisms

In the context of CYberSynchrony, establishing interoperable data exchange mechanisms is essential to ensure that cyber threat intelligence (CTI) can be shared seamlessly across different systems and organizations. These mechanisms allow cybersecurity teams to exchange critical threat data quickly, securely, and efficiently, without the limitations posed by incompatible platforms or conflicting data formats. Their implementation relies on widely accepted technologies and protocols within the cybersecurity community.

To support a smooth and reliable exchange, CYberSynchrony employs a combination of modern protocols, including RESTful APIs, MQTT/Kafka, and Distributed Ledger Technologies (DLT). Together, these technologies ensure scalable, standardized, and trustworthy exchange of information in both real-time and asynchronous environments.

The following figure illustrates how Cyber Threat Intelligence (CTI) data is enriched with various threat data categories, enabling more complete threat analysis. This process is crucial for the effective exchange and categorization of CTI, allowing for faster detection and response to cyber threats.

© CYberSynchrony, 2024

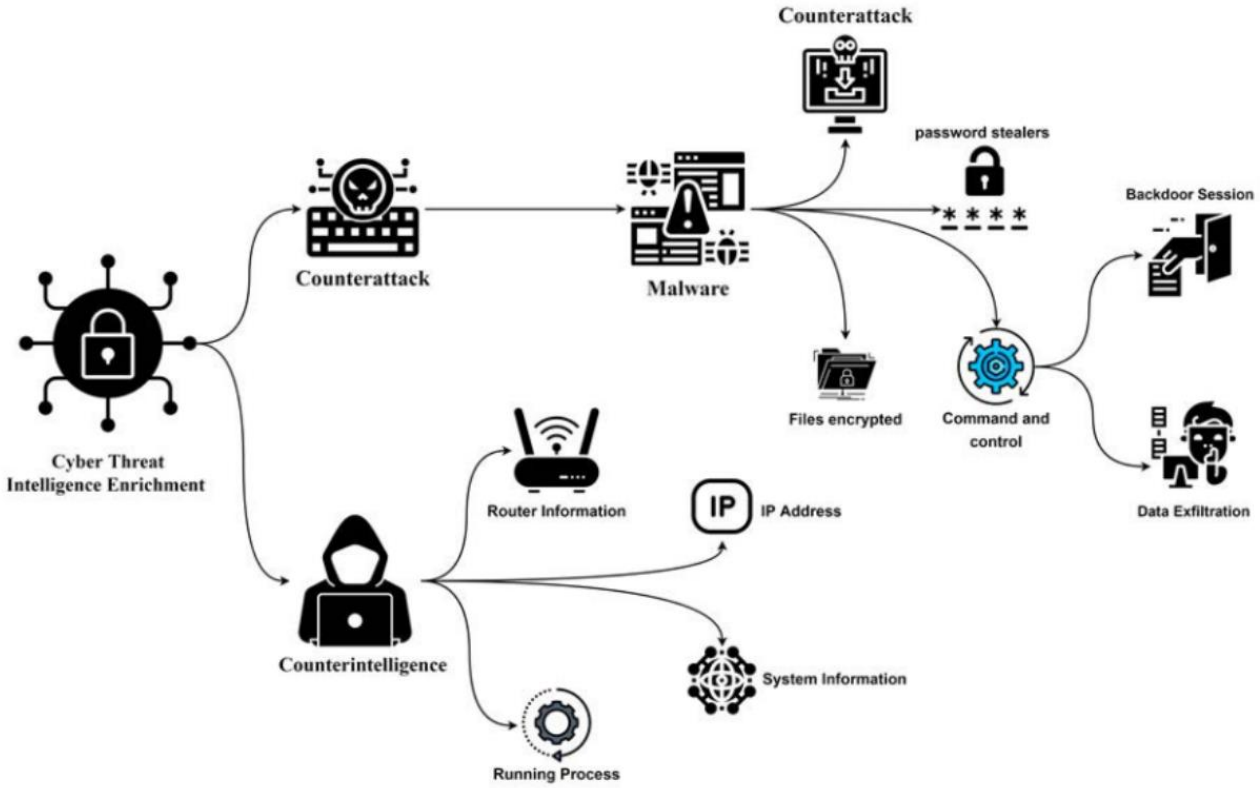

Figure 2: Cyber Threat Intelligence enrichment using data from malware, IPs, and system behaviour. [2].

6.1.1 RESTful APIS

RESTful APIs (Representational State Transfer Application Programming Interfaces) serve as the backbone for structured and secure data integration within the CYberSynchrony ecosystem. This technology enables machine-to-machine communication using well-defined HTTP methods, allowing systems to exchange CTI, such as incident data, IOCs, and mitigation actions in a highly standardized and flexible format.

The key characteristics of RESTful APIs include:

- **Platform-agnostic design**, making them suitable for integration with both **legacy infrastructures** and **modern cloud-native systems**.
- **Support for token-based authentication**, ensuring secure access control and enhancing automation.
- **Compatibility with standardized schemas**, such as **STIX 2.1**, ensuring consistency and reducing the risk of data misinterpretation across different platforms.
- **Widely adopted for structured data integration**, used in systems like **MISP** for threat intelligence publishing and retrieval in a structured manner by authorized actors.
- **Scalability and simplicity**, which are crucial for real-time data exchange and automation across systems.

These advantages make RESTful APIs a critical enabler of both automation and interoperability within CYberSynchrony's framework, ensuring that threat intelligence can be securely and efficiently shared across diverse cybersecurity platforms.

6.1.2 MQTT and Apache kafka

MQTT (Message Queuing Telemetry Transport) and Apache Kafka are messaging protocols and streaming platforms optimized for the continuous flow of high-frequency data, often used in scenarios requiring near real-time situational awareness.

© CYberSynchrony, 2024

MQTT is lightweight, making it ideal for **IoT security** use cases, such as monitoring distributed sensors and edge devices. It transmits alerts or status updates with minimal overhead, ensuring that systems with limited bandwidth can still communicate effectively.

Apache Kafka, on the other hand, is designed for **high-throughput**, fault-tolerant data streaming, making it well-suited for aggregating logs, network events, and telemetry from multiple distributed cybersecurity tools. Kafka is optimized for scenarios where large volumes of data need to be processed quickly and reliably.

The key benefits of **MQTT and Kafka** include:

- **Decoupling data producers from consumers**, enabling flexible, scalable architectures.
- **High resilience and responsiveness**, ensuring that data can be exchanged with minimal latency across systems.
- **Event-driven architectures** that support real-time threat detection, correlation, and response, without the bottlenecks caused by synchronous data exchange.
- **MQTT** for lightweight, low-overhead communication in **IoT and edge security**.
- **Kafka** for handling **massive throughput** in **log aggregation and telemetry**, and for triggering automated responses via platforms like **OpenC2**.

Together, **MQTT and Kafka** form an essential part of CYberSynchrony's ability to orchestrate large-scale, real-time information exchange between systems, ensuring continuous situational awareness and fast incident response.

6.1.3 Distributed Ledger Technologies (DLT)

Distributed Ledger Technologies (DLT) provide a robust mechanism for ensuring the **integrity**, **authenticity**, and **traceability** of cyber threat intelligence (CTI) as it is exchanged between systems and stakeholders. Unlike traditional centralized repositories, DLT-based systems enable the creation of **tamper-evident records** that are distributed across multiple participants, removing single points of failure and fostering trust, even in environments with limited pre-existing relationships.

One of the most common uses of DLT in CYberSynchrony is **blockchain anchoring**, where a **cryptographic hash** of a CTI artifact, such as an IOC or an incident report, is registered on a **permissioned ledger**. This hash functions as a **unique digital fingerprint**, allowing stakeholders to detect any future modifications to the data. Importantly, the **data itself remains off-chain**, ensuring privacy and compliance with data protection laws such as the **General Data Protection Regulation (GDPR)**.

The key advantages of DLTs include:

- **Tamper-evident** records that ensure the data's integrity is preserved during transmission across multiple entities.
- **Privacy-preserving mechanisms**, where sensitive data remains off-chain while still enabling verification via cryptographic hashes.
- **Auditability** and **non-repudiation**: allowing each party to independently verify the data's authenticity.
- **Distributed governance**, enabling trust in decentralized environments by ensuring that no single party has control over the data.

Platforms such as **Hyperledger Fabric** or **Quorum** offer the necessary **access control** and **governance** for regulated environments like CYberSynchrony. By providing a transparent, verifiable, and immutable record, DLT enhances **trust** in the integrity of the intelligence being shared, especially in multi-party environments where digital evidence must be **verifiable**, **resilient**, and **legally defensible**.

© CYberSynchrony, 2024

6.1.4 Platform Integration: MISP, ECN, CSIRT Network

To ensure alignment with existing European cybersecurity infrastructures, CYberSynchrony establishes standardized interfaces with three key platforms: **MISP**, **ECN**, and the **CSIRT Network**. Each of these actors plays a distinct but complementary role in the broader EU cyber threat intelligence ecosystem, and effective integration with them is essential for ensuring both technical compatibility and operational relevance.

MISP (Malware Information Sharing Platform & Threat Sharing) is an open-source platform used by CERTs, CSIRTs, SOCs, and government agencies for structuring and disseminating threat intelligence. It natively supports structured formats such as **STIX 2.1** and data exchange via **TAXII 2.0**, providing an ideal foundation for interoperability with CYberSynchrony's CTI modules. Through **RESTful APIs**, MISP instances can push and pull threat data, including **indicators of compromise**, **attack patterns**, and **malware signatures**, to and from CYberSynchrony in real time. MISP offers **access control** and **tagging** features that allow shared data to be contextualized, prioritized, and classified according to **national** or **sectoral requirements**, which is particularly important when coordinating data exchange across Member States with varying sensitivity levels and response protocols.

ECN (European Cybersecurity Network), operating under **Europol**, supports cross-border cybersecurity collaboration among EU Member States. While **MISP** focuses on **technical indicators**, **ECN** handles **broader operational intelligence** related to cybersecurity coordination and crisis management. By interfacing with **ECN's intelligence processing workflows**, CYberSynchrony ensures that threat intelligence gathered from national platforms or automated detection systems can be escalated to EU-wide cybersecurity efforts when necessary. This **bi-directional interface** enables the mutual enrichment of both **technical CTI** and **operational intelligence**, enhancing the overall situational picture and enabling coordinated action against transnational cyber threats.

The **CSIRT Network**, established under the **NIS Directive**, provides a secure and structured channel for coordination between national incident response teams. Interfacing with the CSIRT Network requires both **technical standardization**, ensuring compatibility of **incident reports**, **severity ratings**, and **response recommendations**, and **procedural alignment** to ensure that CYberSynchrony's outputs (e.g., incident summaries, risk alerts) can be integrated directly into national workflows. For example, alerts generated through CYberSynchrony's analytics modules can be ingested by national CSIRT systems via **TAXII endpoints** or message brokers like **Kafka**, facilitating real-time awareness and harmonized responses. This interface also supports **federated collaboration**, allowing multiple CSIRTs to correlate similar incidents across borders and coordinate response actions with greater confidence.

By integrating with MISP, ECN, and the CSIRT Network, CYberSynchrony does not replace existing infrastructures, but instead acts as an **enabler and amplifier**, extending their capabilities through **automation**, **standardization**, and **secure data handling**. This ensures that the project's outputs are not siloed but directly contribute to the operational continuity and strategic preparedness of the European cybersecurity architecture.

6.2 Maintaining Data Integrity Across Borders

As cyber threat intelligence (CTI) circulates across multiple organizations and jurisdictions, ensuring the integrity of shared data becomes critical, not only for technical consistency but also for legal, operational, and evidentiary purposes. In the context of CYberSynchrony, maintaining data integrity across borders requires a multi-layered approach that combines lightweight validation techniques with cryptographic assurances and systematic traceability.

At the foundational level, CYberSynchrony employs checksums to verify that data has not been altered during transit. A checksum is a computed hash value that represents the contents of a dataset at the moment of transmission. Upon receipt, the checksum is recalculated and compared to the original value. If the values match, the data is verified as unchanged; if they do not, tampering or corruption is assumed. This simple but effective mechanism enables CYberSynchrony to detect unauthorized modifications or errors rapidly, making it ideal for use in automated data pipelines and real-time streaming environments.

© CYberSynchrony, 2024

Complementing these lightweight techniques, CYberSynchrony utilizes blockchain anchoring via Distributed Ledger Technologies (DLT) to add an additional layer of cryptographic verification. When a CTI artifact, such as an IOC or an incident report, is shared, a cryptographic hash of the content is registered on a permissioned ledger, creating a tamper-evident, time-stamped record. This allows all stakeholders, including national authorities and incident response teams, to independently verify that a specific version of data existed at a given point in time and has not been altered. Unlike full blockchain storage, this method does not involve recording the data itself on the chain, thereby preserving confidentiality and reducing storage overhead.

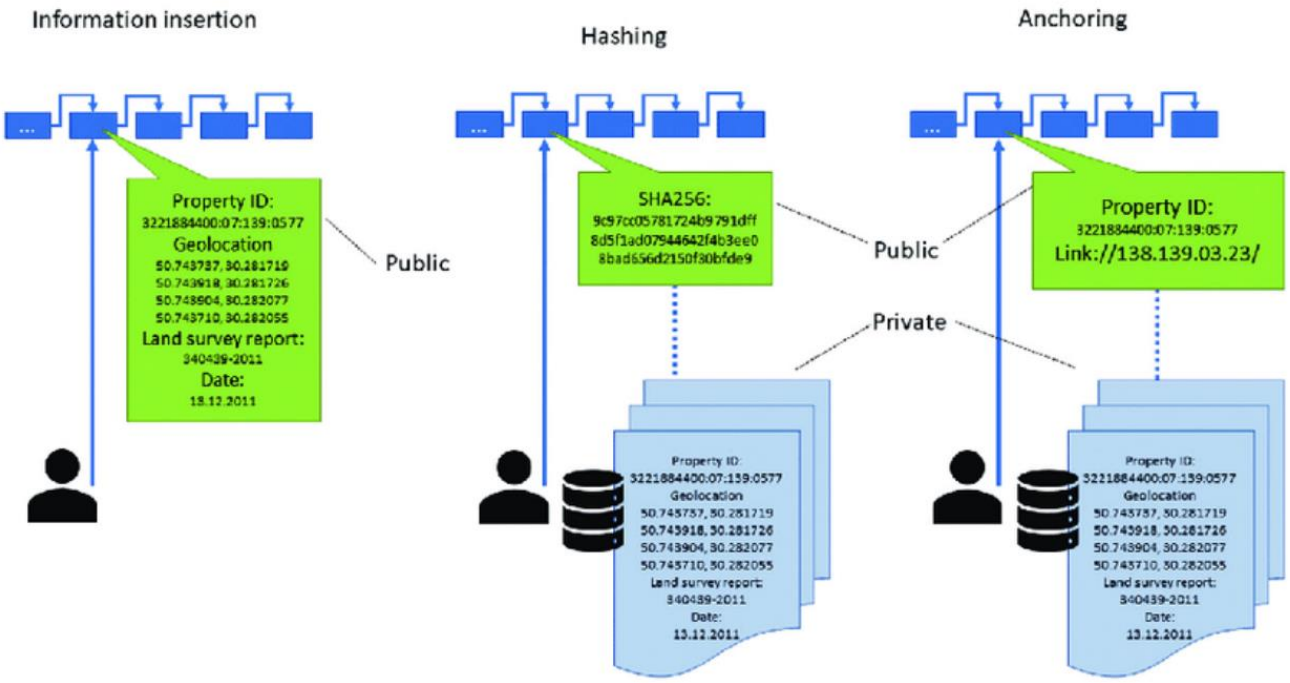

Figure 3: Blockchain anchoring process for verifying the integrity of Cyber Threat Intelligence [3].

As shown in the figure, using blockchain anchoring provides a tamper-evident mechanism that allows stakeholders to verify the integrity of CTI data independently. This approach ensures that CTI artifacts cannot be modified without detection, thereby preserving their authenticity and integrity during cross-border exchanges.

By registering the hash of a CTI artifact on a permissioned ledger, CYberSynchrony creates a tamper-evident, time-stamped record that can later be used to prove the authenticity of the data. Unlike whole blockchain storage, anchoring does not involve recording the data itself on the chain, which preserves confidentiality and reduces storage overhead. This method ensures that all stakeholders, including national authorities and incident response teams, can independently verify that a specific version of data existed at a certain point in time and has not been subsequently altered.

In addition to integrity verification, CYberSynchrony introduces robust error-handling and traceability mechanisms. If a data inconsistency or synchronization failure is detected, whether due to transmission errors, schema mismatches, or unauthorized intervention, the system triggers a defined response workflow, which may involve automatic rollback procedures, re-synchronization attempts, or manual investigation. Every relevant exchange event is logged in a verifiable and chronological manner, creating a full audit trail. These logs are enriched with metadata such as timestamp, origin, system ID, and verification status, providing comprehensive tracking and enabling post-event forensics.

CYberSynchrony also implements a **layered approach to data validation**, with checksums like CRC32 used for rapid verification of payloads, and cryptographic hashes like SHA-256 or BLAKE2 employed in high-trust, inter-organizational contexts. While CRC32 is optimized for low-overhead environments like sensor-level streaming,

© CYberSynchrony, 2024

SHA-256 and BLAKE2 provide stronger guarantees, essential when tampering must be detectable beyond doubt. This **layered hashing mechanism** ensures that each CTI transaction, whether exchanged via REST, Kafka, or direct peer-to-peer protocols, can be validated at multiple levels depending on the sensitivity of the data and the regulatory context.

From an operational perspective, **DLT-based anchoring** plays a crucial role in maintaining legal admissibility and institutional trust. By anchoring IOCs or incident fingerprints on a permissioned ledger, CYberSynchrony not only prevents tampering but also generates a third-party-verifiable record. In cases involving cross-border incidents, such as an Advanced Persistent Threat (APT) attack spanning multiple Member States, this anchoring mechanism serves as digital evidence, timestamped and cryptographically sealed. This process improves the credibility of threat reporting and ensures alignment with frameworks such as **eIDAS** and the **NIS2 Directive**.

Additionally, **robust error-handling logic** is integrated into CYberSynchrony's architecture at multiple levels. On the application side, asynchronous data reception is supported by mechanisms like message queuing, retry policies, acknowledgment systems, and schema negotiation layers to reconcile conflicting versions of data. These mechanisms help minimize data loss and prevent malformed threat intelligence from propagating through the system. On the governance layer, CYberSynchrony incorporates **escalation workflows** for incidents that involve critical integrity failures, such as data mismatches that cannot be automatically resolved. These incidents are logged, timestamped, and escalated to human analysts for further review, ensuring that human oversight is maintained in complex scenarios.

Finally, CYberSynchrony emphasizes **traceability** not just for individual transactions but for entire chains of custody. Every CTI record processed through the platform is associated with a **digital provenance trail** that includes metadata such as submission identity, transmission route, applied transformations, and verification outcomes. This metadata is essential for post-incident forensics and enables **selective trust models**, where higher credibility is assigned to indicators provided by trusted sources like national CERTs or organizations with known validation histories. Over time, these mechanisms support the emergence of a **reputation-based trust layer**, enhancing the quality of intelligence and enabling better-informed automated responses.

In a cross-border cybersecurity environment, maintaining data integrity is not just a matter of technical reliability, it also underpins regulatory compliance and strategic coordination. For example, when incident reporting is required under frameworks such as the **NIS2 Directive** or sectoral **CSIRT mandates**, the ability to prove that CTI was received and acted upon without modification is critical. Integrity mechanisms integrated with compliance workflows automatically generate evidence for post-incident disclosures or security audits. Additionally, in scenarios involving state-level or coordinated cyber operations, the traceability and integrity features safeguard against malicious data injection, a tactic often used to obscure attribution or derail response. By treating integrity not merely as a passive property but as an active security signal, CYberSynchrony not only contributes to information sharing but also fosters **trust-based cyber diplomacy** and legal robustness across the Union.

© CYberSynchrony, 2024

7 Partner Contributions and Data Inventory

Effective collaboration across the CYberSynchrony consortium requires not only common formats and exchange mechanisms, but also a clear understanding of how each partner contributes to the shared cyber threat intelligence (CTI) landscape. In this context, the current chapter documents the origin, type, structure, and integration of CTI data handled by each contributor.

This collective inventory serves multiple purposes: it enables traceability of data flows, ensures consistency across work packages, and supports compliance with the technical and governance models defined in the project. By clearly identifying roles, responsibilities, and technical components, CYberSynchrony reinforces its commitment to structured, verifiable, and interoperable CTI exchange.

7.1 Partner Data Input Matrix

To ensure full transparency and alignment in how cyber threat intelligence (CTI) is handled within the CYberSynchrony framework, the following matrix collects structured input from all project partners. Each contributor is invited to specify which tools or components they operate, what types of CTI are shared or processed, the data formats used, and how this information integrates into the broader interoperability and structured sharing frameworks described in previous chapters (e.g., STIX, TAXII, JSON/XML schemas).

The matrix not only clarifies each partner's technical footprint, but also facilitates mapping between data sources and interoperability mechanisms, laying the groundwork for effective cross-platform integration and compliance tracking. By populating this matrix, the consortium builds a shared view of the data ecosystem, identifying convergence points and potential gaps for further harmonization.

The following table shows the data type, the origin of the data, the related WP number and the format, in which the data will be presumably stored.

Table 7: Partner Data Input Matrix

Component	Data Type	Data Format	Framework Adaptation
MISP	MISP is an open-source tool for collecting and sharing threat information. It predicts potential threats. In the project, MISP will improve how threats are detected and shared, helping organizations address them before they become serious problems.	JSON	ECS (Elastic Common Schema), EVE-compatible log format
Wazuh	Wazuh is an open-source platform used to monitor systems for security threats and respond to incidents (SIEM protection). It can protect computers, networks, and even cloud environments. In CYberSynchrony, it will help detect and respond to security issues in real-time and monitor potential risks proactively.	JSON	ECS (Elastic Common Schema), EVE-like log structure

© CYberSynchrony, 2024

Suricata	Open-source intrusion detection system (IDS) for monitoring network traffic and identifying threats	JSON (EVE format)	EVE JSON schema, compatible with SIEM (Wazuh), MISP enrichment
WEKA	WEKA is an open source ML tool that can be used for classification purposes (https://ml.cms.waikato.ac.nz/weka/). For CYberSynchrony purposes it can be used as an external component for classifying network (or log) data and identifying possible attacks. This tool was not part of the GA purposes it can be used as an external component for classifying network (or log) data and identifying possible attacks. This tool was not part of the GA	CSV	Custom structured CSV for labelled post-analysis
SNYK	Snyk scans an organization's software code to find vulnerabilities that hackers could exploit. It does this before the software is even deployed, ensuring it is secure. In the project, Snyk will help identify security gaps in the software and ensure applications meet cybersecurity standards.	JSON	CVE/CWE-based vulnerability data, JSON
Human RM (HRM)	This is a tool focused on the human side of cybersecurity. It assesses the risks associated with human behaviour, such as mistakes or lack of awareness, and creates strategies to improve security culture. In the project, it will help train people and develop security policies.		TBD
Keycloak Identity Manager	Identity management and access control for Services and API	JSON (as per Keycloak docs)	N/A
Anomaly Detector IDS	The AI-Based Intrusion Detection System (IDS) leverages advanced machine learning techniques to detect anomalies in network traffic. By processing raw log data with Zeek and combining temporal patterns (via Multi-Head Self-Attention) with raw network features, it identifies unusual behaviours and cross-feature inconsistencies. This ensures real-time monitoring and robust anomaly	JSON	Internal vectorized format, potential alignment with MITRE ATT&CK (TBD)

© CYberSynchrony, 2024

	detection across various environments.		
Blockchain Integrity Validator	Ensures the data required for the IDS systems are not altered or tampered with using native hash functions.	JSON	Custom SHA-256 + metadata schema
Kitsune Monitoring	After setting the appropriate keywords to monitor, the service will start the monitoring process and provide evidence by creating an alert when the specific event is detected. The service will check for BOTNET infections of users and new data LEAK of specific mail domains, MENTIONS of specific keywords inside dark web and darknet perimeter.	JSON	TBD
Kitsune Search	Functionalities used to SEARCH for: specific Information about Threat Actors and Threat Landscape, returning info related to IOCs (Indicator Of Compromise); specific Information about data LEAK exposition related to a domain/keyword; BOTNET (infostealer) infections related to users of a specific mail domain; MENTIONS of specific keywords inside dark web and darknet perimeter.	JSON	TBD
Attack Surface Assessment (ASA)	N/A	N/A	N/A
Purple Team Assessment (PTA)	N/A	N/A	N/A
SecurityBreachSimulation (SBS)	Perform manual penetration testing conducted by skilled offensive security analysts to identify vulnerabilities	N/A	N/A
Defensive Cyber Operations (DCO)	TBD	JSON (events, triggers)	OpenC2 (TBD)

© CYberSynchrony, 2024

8 Conclusions

The D5.2 “Evidence Integrity System v1 (Data Management Plan)” deliverable establishes a robust, standardized foundation for the secure management and exchange of CTI across Member States within the CYberSynchrony project. By defining interoperable data formats, adopting widely recognized standards such as STIX and TAXII, and integrating advanced validation mechanisms, including checksums and blockchain anchoring, the deliverable directly addresses persistent challenges in cross-border CTI sharing, such as semantic inconsistencies, trust deficits, and legal constraints.

The system’s alignment with key European cybersecurity infrastructures (MISP, ECN, CSIRT Network) and its support for both automated and real-time incident response workflows significantly enhance operational efficiency, trust, and situational awareness. The structured approach to evidence integrity ensures that digital evidence remains authentic, unaltered, and legally defensible throughout its lifecycle, which is essential for both technical and regulatory compliance.

As the Data Management Plan is designed to be a living document, it will evolve to incorporate feedback from consortium partners, adapt to emerging threats, and integrate new technological and regulatory developments. Future iterations will further refine automation, compliance, and auditability, ensuring that the Evidence Integrity System remains at the forefront of best practices in European cybersecurity collaboration.

© CYberSynchrony, 2024

9 References

[1] OASIS, "STIX (Structured Threat Information Expression)," [Online]. Available: https://www.oasis-open.org/2021/06/23/stix-v2-1-and-taxii-v2-1-oasis-standards-are-published/

[2] OASIS, "TAXII (Trusted Automated Exchange of Intelligence Information)," [Online]. Available: https://docs.oasis-open.org/cti/taxii/v2.0/taxii-v2.0.html

[3] OpenC2 Forum, "Open Command and Control (OpenC2)," [Online]. Available: https://openc2.org/news.html

[4] ENISA, "CSIRT Services," [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe

[5] ENISA, "European Union Agency for Cybersecurity," [Online]. Available: https://www.enisa.europa.eu/

[6] NCPC, "European Cybersecurity Network," National Cybersecurity Preparedness Consortium, [Online]. Available: https://www.nationalcpc.org/

© CYberSynchrony, 2024