Harmonizing People, Processes, and Technology for Robust Cybersecurity

D5.4 Evidence Integrity System v2

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	D5.4 Evidence Integrity System v2		
Work Package	WP5 Cross-Border Cyber Collaboration and Secure Response (CROSS-CORE)		
Contractual due date	31 May 2026	**Actual submission date**	10/07/2026
Type	OTHER	**Dissemination Level**	Public
Lead Beneficiary	Meridian Group srl (MER)		
Responsible Author	Andrea Purificato (MER)		
Contributions from	Andrea Purificato (MER), Vasilis Keleris (MAG), George Karavokiros (BYTE)		

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	01.05.2026	Initial Deliverable structure	Andrea Purificato (MER)
0.2	25/05/2026	Chapter 1 & 2	Andrea Purificato (MER)
0.3	11/06/2026	Chapter 4 & 5	Andrea Purificato (MER)
0.4	15/06/2026	Chapter 6, updating all sections	Andrea Purificato (MER), Vasilis Keleris (MAG), George Karavokiros (BYTE)
0.5	16/06/2026	Updating all sections	Andrea Purificato (MER), Vasilis Keleris (MAG), George Karavokiros (BYTE)
0.6	25/06/2026	Final draft ready for internal review	Andrea Purificato (MER)
0.7	08/07/2026	Final draft ready for QA	Laskarina Mavropoulou (MER)
0.8	09/07/2026	Final quality check	Eleni Keliri (eBOS)
0.9	10/07/2026	Final version ready for submission	Violeta Vasileva

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 this document is believed to be accurate, the author(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

© CYberSynchrony, 2024

Table of Contents

1 Executive Summary 8
2 Introduction 9
2.1 Mapping CYberSynchrony Outputs 9
2.2 Linkage to other project outputs 10
2.3 Deliverable Structure 11
3 CYberSynchrony Technical Evolution of the Evidence Integrity System 13
3.1 Transition from Foundational Framework to M25 Integrated Implementation 14
3.2 Evaluation of Advanced Cryptographic Technologies 14
3.3 Technical Coordination and Platform Integration Leadership 14
3.3.1 Steering the Unified Incident Response Mechanics 14
3.3.2 Enhancing the Evidence Plane 14
3.3.3 Coordinating the Transition to Real-World Pilot Validation 14
4 CYberSynchrony Structured Threat Data and Formats updates since V1 16
4.1 Supported Data Types and Standardized Formats 16
4.2 Application of Monitoring and Intelligence Technologies 16
4.3 Technical Challenges and Practical Solutions 16
4.4 Lessons Learned and Operational Insights 17
5 CYberSynchrony Interoperable Exchange and Integrity Mechanisms updates since V1 18
5.1 RESTful APIs 18
5.2 Apache Kafka 18
5.3 Distributed Ledger Technologies (DLT) 19
5.4 Platform Integration 19
6 KPIs Mapping 20
6.1 KPI 3.6: Risk Scenarios Analysed 20
6.2 KPI 4.5: Incident Collaboration Index 21
6.3 KPI 5.1: Number of Risk Monitoring Services Provided 21
7 Conclusions 23
8 References 24

© CYberSynchrony, 2024

List of Tables

Table 1: Adherence to CYberSynchrony's GA 9
Table 2: Links to other Project Outputs/Work 10
Table 3: Evidence Integrity System v2 13
Table 4: KPI 3.6: Risk Scenarios Analysed. 20
Table 5: KPI 4.5: Incident Collaboration Index. 21
Table 6: KPI 5.1 Number of Risk Monitoring Services Provided. 22

© CYberSynchrony, 2024

Acronyms and abbreviations

Abbreviation / Term	Description
API	Application Programming Interface
CERT	Computer Emergency Response Team
CKKS	Cheon-Kim-Kim-Song
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
DLT	Distributed Ledger Technology
DP	Differential Privacy
EVE	Emulated Virtual Environment
FHE	Fully Homomorphic Encryption
GDPR	General Data Protection Regulation
HE	Homomorphic Encryption
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IoC	Indicator of Compromise
IPS	Intrusion Prevention System
JSON	JavaScript Object Notation
JWT	JSON Web Token
LDP	Local Differential Privacy
KPI	Key Performance Indicator
MISP	Malware Information Sharing Platform
MITRE	MITRE Corporation
MOS	Mean Opinion Score
MS	Member State(s)
PHP	Hypertext Preprocessor
REST	Representational State Transfer
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SOC	Security Operations Center

© CYberSynchrony, 2024

STIX	Structured Threat Information Expression
TAXII	Trusted Automated eXchange of Indicator Information
TTP	Tactics, Techniques, and Procedures
WP	Work Package
XML	eXtensible Markup Language
YAML	YAML Ain't Markup Language

© CYberSynchrony, 2024

1 Executive Summary

D5.4 “Evidence Integrity System v2”, presents the second version of the Evidence Integrity System, designed to support the non-alteration, authenticity, traceability and verifiability of cyber threat intelligence (CTI) exchanged across Member States within the CYberSynchrony project.

As a core output of Work Package 5 (CROSS-CORE), the system is designed to address the critical need for secure, standardized, and trustworthy data sharing to support cross-border cyber incident response and mutual assistance.

The primary difference between the initial version (D5.2) and this subsequent D5.4 release lies in their technical maturity and position within the project timeline; while D5.2 provided the initial conceptual design at M12, D5.4 represents the technical implementation status up to M25. This iterative development cycle has allowed the consortium to move beyond synthetic test environments towards validation using real pilot datasets provided by the AMC (clinical records), UPRC (academic records), and EGL (municipal incident records) partners.

The Evidence Integrity System v2 is now fully integrated into the CYberSynchrony platform architecture, leveraging performance-efficient blockchain-based protocols (Hyperledger Fabric) to maintain an unalterable chain of custody. This implementation enables the verification of SHA-256 fingerprints and associated metadata throughout their lifecycle, from initial detection by Suricata and Wazuh[1] to enrichment via MISP and distribution through Apache Kafka[2].

The system now supports a diverse range of structured threat data types, including Incident Reports, IoCs, and TTPs mapped to the MITRE ATT&CK[3] framework, utilizing standardized formats such as STIX as a cyber-threat-intelligence data model, JSON as a serialisation format and OpenC2 as a language for cyber-defence commands, to ensure seamless cross-border interoperability.

During this phase, the consortium extensively evaluated advanced cryptographic technologies, including Differential Privacy (DP) and Fully Homomorphic Encryption (FHE).

This consolidated release supports the project’s technical requirements by enabling stakeholders to collaborate through the exchange of unaltered, authentic intelligence data. D5.4 directly supports risk scenario analysis, incident collaboration and proactive risk monitoring services.

© 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, with 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			
D5.4	Evidence Integrity System v2	Chapters 3-5	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 v2" 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			
T5.1	Task 5.1 - Fortifying Cross-Border Data Exchange	Chapters 3, 5, 6	This task focuses on the rollout of robust information-sharing platforms to ensure data is encrypted and remains unaltered during transit. D5.4 provides the technical integrity and interoperability mechanisms (Chapters 3, 5, and 6) necessary for Member States to exchange information with confidence during mutual assistance.
T5.2	Task 5.2 - Advancing Uniform Data Sharing Standards	Chapters 2,3,4,5,6	This task emphasizes the importance of standardized data sharing protocols among MS. A unified approach 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

© CYberSynchrony, 2024

T5.3	Task 5.3 – Unified Incident Response Mechanics	Chapter 6	This task focuses on unifying incident response strategies across MS using advanced coordination tools. These tools enhance real-time communication and collaboration during cyber crises, ensuring unified actions. They also support detailed response planning and magnifying collective effectiveness. The goal is to transform individual responses into harmonized defences against cyber threats.

2.2 Linkage to other project outputs

The D5.4 "Evidence Integrity System v2" deliverable is closely interconnected with other project outputs and specific deliverables within the CYberSynchrony project, particularly WP5.

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

Table 2: Links to other Project Outputs/Work

WP Number	Task Number	Deliverable Number related	Content
WP5	T5.1, T5.2	D5.2 Evidence Integrity System v1	D5.2 is the initial version (v1) of this deliverable, that focuses on ensuring the non-alteration of digital evidence during cyber investigations
	T5.1	D5.3 Secure Data Exchange Platform v2	D5.3 delivers the definitive technical platform for secure, encrypted data exchange between Member States. D5.4 builds on this by specifying the 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 D5.4 ensure that the data exchanged through D5.3 remains trustworthy, traceable, and compliant with legal requirements
WP4	T4.1, T4.2	D4.3 – Integrated Cybersecurity Monitoring Suite v2	D4.3 provides the primary monitoring telemetry and unified alert streams (incorporating Wazuh, Suricata, and Kafka distribution) that constitute the digital evidence requiring protection. D5.4 establishes the integrity layer that prevents the tampering of these logs and alerts, ensuring they remain forensically valid for cross-border sharing and investigation.

© CYberSynchrony, 2024

WP3	T3.2	D3.3 - Enhanced Threat Intelligence System v2	D3.3 describes the second version of the integration and interoperability of the WP3 threat intelligence components. It outlines the implementation of the Wazuh/Suricata-MISP alert enrichment workflow, the integration of the Kitsune Search user interface, and the redesigned forensic integrity pipeline, which applies HMAC-SHA256 to each alert and anchors the resulting integrity records in Hyperledger Fabric.

2.3 Deliverable Structure

The structure of Deliverable D5.4 "Evidence Integrity System v2" 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**
  This chapter provides a concise overview of the deliverable, summarizing its core purpose, key technical findings and the value that the Evidence Integrity System adds to the overall project. It also highlights the transition from the initial conceptual framework to this consolidated v2 implementation.
- **Chapter 2: Introduction**
  This chapter introduces the scope and context of the deliverable, mapping its outputs to the project's formal Grant Agreement commitments and associated tasks. It also details the linkages and dependencies between D5.4 and other work packages, ensuring a unified understanding of the system's integration.
- **Chapter 3: CYberSynchrony Technical Evolution of the Evidence Integrity System**
  This chapter explains the technical maturation of the system, detailing the shift from synthetic data to real pilot datasets and the refinement of integrity protocols. It also documents the consortium's evaluation of advanced cryptographic technologies, providing the technical verification required for metrics such as risk scenario analysis and incident collaboration.
- **Chapter 4: CYberSynchrony Structured Threat Data and Formats updates since V1**
  This chapter describes the diverse range of structured threat data types now supported by the system. It emphasizes the use of standardized formats to ensure interoperability and seamless data exchange.
- **Chapter 5: CYberSynchrony Interoperable Exchange and Integrity Mechanisms updates since V1**

  This chapter details the updated mechanisms for establishing secure and interoperable data exchange. It explains how these technologies interact to maintain a tamper-evident audit trail and a verifiable chain of custody for digital evidence
- **Chapter 6: KPIs mapping**

  This chapter maps the Evidence Integrity System v2 to the specific project Key Performance Indicators (KPIs) it addresses.
- **Chapter 7: Conclusions**
  Summarizes the main outputs and value added by the deliverable.

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 CYberSynchrony Technical Evolution of the Evidence Integrity System

The Evidence Integrity System v2 (D5.4) provides a verification mechanism for supporting data privacy and security during information exchange among Member States. As a core component of the CYberSynchrony platform, it implements the project's evidence integrity services, supporting secure information exchange and the verification of shared digital evidence.

This implementation adopts performance-efficient blockchain protocols (Hyperledger Fabric) to support real-time evidence preservation while maintaining operational agility and addressing integrity forensic requirements.

As part of the continuous technical refinement and the transition from the initial framework in D5.2 to the M25 implementation of D5.4, the consortium has evaluated the technical merits of advanced cryptographic technologies. By defining the DP → HE → SHA-256 pipeline, D5.4 establishes the mechanisms through which sensitive forensic artifacts are anonymized, encrypted, and anchored to support secure and verifiable data exchange.

The following table summarizes the D5.4 framework components and their role within the implemented Evidence Integrity System:

Table 3: Evidence Integrity System v2

Framework Component	Technical Decision & Guidance	Implementation Reference
Privacy-Preserving Analytics (DP → HE)	Enforces a hybrid deployment model that physically separates on-premise encryption from cloud aggregation to guarantee raw data never leaves the owner's control.	D5.3 (Secure Data Exchange Platform v2)
Unalterable Chain of Custody (Blockchain)	Prioritizes Hyperledger Fabric for the primary evidence plane to meet "real-time" requirements, reserving FHE for specific, less time-sensitive use cases due to computational overhead.	D5.3 (Section 6 & 7)
Standardized Data Formats	Mandates the use of STIX, JSON, and OpenC2 to normalize heterogeneous inputs (e.g., from Wazuh and Suricata) into a unified and verifiable alert stream.	D4.3 (Integrated Cybersecurity Monitoring Suite v2)
Integrity-Aware API Gateway	Employs a Node.js/Express gateway with Keycloak JWT authentication to handle asynchronous ledger transactions via Fabric event listeners.	D5.3 (Section 6.5)
Unified Evidence Plane	Establishes the technical verification required for cross-border collaboration, ensuring that shared indicators and playbooks are cryptographically anchored for global trust.	D4.3, D5.3 (KPI Mapping)

© CYberSynchrony, 2024

3.1 Transition from Foundational Framework to M25 Integrated Implementation

This technical evolution is characterized by a shift from synthetic test data to M25 implementation fully integrated within the CYberSynchrony platform, preparing the system for subsequent validation using real pilot datasets from AMC (clinical records), UPRC (academic records), and EGL (municipal incident records).

During this phase, the consortium evaluated advanced cryptographic technologies, specifically Differential Privacy (DP) and Fully Homomorphic Encryption (FHE) to enhance cross-border security.

3.2 Evaluation of Advanced Cryptographic Technologies

While D5.3 (Secure Data Exchange Platform v2) provides the foundational benchmarks for these technologies, including the DP → HE → SHA-256 pipeline, D5.4 applies these findings to maintain an unalterable chain of custody.

Specifically, D5.3 details how the computational overhead of FHE (CKKS scheme) was measured across pilot scenarios, leading to the decision in D5.4 to **prioritize performance-efficient blockchain-based protocols** (Hyperledger Fabric) to satisfy real-time monitoring requirements.

Consequently, D5.4 prioritizes the use of Hyperledger Fabric to maintain an **unalterable chain of custody**, ensuring that digital evidence remains trustworthy and forensic validity is preserved throughout its lifecycle.

Differential Privacy (DP) was assessed for its potential to enhance the anonymization of sensitive forensic artifacts shared between Member States, ensuring that the information sharing frequency can increase, while strictly adhering to GDPR principles and data privacy related objectives.

Simultaneously, the consortium investigated Fully Homomorphic Encryption (FHE) to determine if performing threat analysis on encrypted data, without the need for decryption, could further bolster the confidentiality of data shared during mutual assistance efforts.

While DP was confirmed as a vital tool for the anonymization of sensitive forensic artifacts to increase information sharing frequency (KPI 5.2), it was determined that the current computational overhead of FHE challenges the real-time requirements of the CYBRITE and CROSS-CORE modules.

3.3 Technical Coordination and Platform Integration Leadership

As the lead beneficiary and responsible author for D5.4, MER serves as a technical and coordinative pillar, guiding the Evidence Integrity System v2 from its initial conceptual framework toward a v2 implementation fully embedded in the CYberSynchrony architecture.

3.3.1 Steering the Unified Incident Response Mechanics

MER facilitates the unification of incident response strategies across Member States. This role ensures that cross-border coordination tools utilize unalterable forensic techniques and verifiable chains of custody to support secure mutual assistance, transforming individual responses into a harmonized defence front.

3.3.2 Enhancing the Evidence Plane

MER's technical leadership is further demonstrated through the integration of the Kitsune Monitoring platform into the system's monitoring pipeline. This contribution provides the proactive surveillance and high-fidelity evidence collection necessary to satisfy project benchmarks, specifically enabling the documentation of realistic "what if" risk scenarios (KPI 3.6) and the activation of 25 risk monitoring services (KPI 5.1).

3.3.3 Coordinating the Transition to Real-World Pilot Validation

MER has actively coordinated the transition from the synthetic testing environments of D5.2 v1 to a M25 integrated implementation within the CYberSynchrony platform. The resulting prototype is fully integrated and

© CYberSynchrony, 2024

awaits validation using pilot datasets provided by AMC, UPRC, and EGL with the objective of establishing trustworthy and tamper-evident evidence to support cross-border collaboration within the project.

© CYberSynchrony, 2024

4 CYberSynchrony Structured Threat Data and Formats updates since V1

Diverse range of structured threat data types is now supported. These data types are stored and exchanged using standardized formats.

This evolution will be primarily defined by the transition from simulated data to the utilization of real pilot datasets provided by the AMC (clinical records), UPRC (academic records), and EGL (municipal incident records) partners.

4.1 Supported Data Types and Standardized Formats

To ensure cross-border interoperability and legal validity, the system now supports a diverse range of **structured threat data types** beyond simple indicators.

The technical application of these formats is explored in depth in D4.3 (Integrated Cybersecurity Monitoring Suite v2), which describes the following core pipelines:

- **Unified Alert Normalization:** D4.3 details how Wazuh acts as the central normalization layer, converting heterogeneous inputs from Suricata network events (in EVE JSON format) and host-level telemetry into the unified alert stream verified by D5.4.
- **Behavioural Anomaly Detection:** the Anomaly Detector IDS utilizes a transformer-based autoencoder to identify behavioural deviations. D4.3 provides the specific 34-dimensional feature vector schema used to process these anomalies before they are anchored on the blockchain.
- **Monitoring Configuration:** technical hurdles, such as container isolation affecting Suricata's visibility, were resolved by binding the IDS to the real host interface and expanding the HOME_NET definition, as documented in the deployment settings of D4.3.

These data types are exchanged using standardized formats to eliminate ambiguities and ensure that shared intelligence remains actionable across different Member State security operations centers.

4.2 Application of Monitoring and Intelligence Technologies

Several core technologies have been operationally applied within the platform:

- **Suricata and Wazuh Integration:** Suricata IDS has been deployed to provide granular network traffic inspection, generating structured events in EVE JSON format. These events are ingested by the Wazuh SIEM, which acts as a central normalization layer, merging network-level detections with host-level telemetry into a unified alert stream.
- **Anomaly Detection via Kafka:** the Anomaly Detector IDS utilizes an asynchronous pipeline via Apache Kafka to consume flow-level features from Suricata. This setup allows the system to identify behavioural deviations using a transformer-based autoencoder without requiring direct, heavy-lifting connections to the raw telemetry sources.
- **Privacy-Preserving Analytics:** the platform now utilizes Local Differential Privacy (LDP) and Homomorphic Encryption (PyFHEL/CKKS) to enable collaborative analytics. This ensures that organizations can compute shared statistics, such as average response times or risk scores, while their raw records never leave their local perimeter in a readable form.

The Evidence Integrity System v2 operationalizes the monitoring and analytics pipeline by integrating heterogeneous detection engines and privacy-preserving protocols into a single, verifiable environment.

4.3 Technical Challenges and Practical Solutions

During the integration phase, the consortium encountered several technical hurdles that required iterative refinement:

© CYberSynchrony, 2024

- **Container Isolation and Visibility:** initially, the Suricata deployment was restricted by Kubernetes pod isolation, preventing it from seeing host-level network traffic. This was overcome by reconfiguring the deployment to use *hostNetwork: true* and binding the IDS to the real host interface. The detailed Kubernetes configuration files and the shell scripts used to resolve this interface binding issue are documented in Chapter 3 of D4.3 (Integrated Cybersecurity Monitoring Suite v2).
- **Network Classification Ambiguities:** early configurations of the IDS used an incomplete definition of the internal network (HOME_NET), leading to missed alerts. The team resolved this by expanding the configuration to cover the full project address range, including Tailscale and private IP segments. D4.3 provides the comprehensive list of private IP ranges and the specific updates required to ensure Suricata correctly distinguishes between internal and external traffic.
- **Cryptographic Overhead:** evaluations of **Fully Homomorphic Encryption (FHE)** revealed that its computational overhead could challenge real-time monitoring requirements. To maintain **operational agility**, the project prioritized performance-efficient **blockchain-based protocols** (Hyperledger Fabric) for the primary integrity chain, while reserving FHE for specific, less time-sensitive data exchange use cases. The performance metrics and scaling benchmarks that justified this architectural shift, specifically comparing per-record encryption costs to pre-aggregated anchoring, are explored in depth in Chapter 7 of D5.3 (Secure Data Exchange Platform v2).

4.4 Lessons Learned and Operational Insights

The development of version 2 has provided critical insights for the final validation phase:

- **The Value of a Unified Evidence Plane:** Proving that host-based and network-based events can be correlated within a single SIEM layer is fundamental for efficient incident response. Chapter 4 of D4.3 provides extensive documentation and dashboard evidence showing how these heterogeneous inputs are normalized into a unified structure, enabling more efficient cross-layer auditing and investigation. This unified approach ensures that forensic evidence is consistent and ready for integrity validation by the blockchain layer.
- **Optimization through Local Pre-aggregation:** a major breakthrough in performance was achieved by shifting from encrypting individual records to encrypting only differentially private partial results at the data source. This approach resulted in a 40x reduction in cryptographic work, allowing end-to-end cross-border requests to complete faster. The detailed record-level benchmarks and the scaling comparisons that justify this "local pre-aggregation" strategy are explored in Chapter 7 of D5.3 (Secure Data Exchange Platform v2).
- **Physical Separation as a Privacy Pillar:** enforcing a topology that physically separates the on-premise encryption stage from cloud-side aggregation services is the only way to guarantee that raw data truly never leaves the data owner's control. D5.3 provides the complete hardware specification and virtual machine mapping for the Cross-CORE deployment, illustrating how this physical isolation of the data protection layer is maintained in practice.

© CYberSynchrony, 2024

5 CYberSynchrony Interoperable Exchange and Integrity Mechanisms updates since V1

Since the initial release of the Evidence Integrity System, the platform's exchange and integrity mechanisms have transitioned from standalone proofs of concept to a **coordinated micro-services architecture**. This evolution is underpinned by a hybrid deployment model that physically separates local data protection from cloud-side aggregation and auditing.

The primary achievement in this version is the operationalization of a **DP → HE → SHA-256 pipeline**, where privacy-preserving analytics and blockchain-based audit trails function in parallel to ensure that cross-border information sharing is both legally compliant and technically verifiable.

5.1 RESTful APIs

Interoperability is primarily facilitated through RESTful APIs that exchange data in JSON format, enabling machine-to-machine communication between the modular components. Secure access to these services is enforced through Keycloak Identity Manager, which issues JWT (JSON Web Tokens) that must be presented in the authorization header of every API call.

Interoperability across the modular framework is now enforced through a **centralized API gateway** based on Node.js and Express. While version 1 used ad-hoc communication, version 2 implements a thin REST surface that translates high-level platform requests into specific ledger operations.

- **Security and Standardization:** access is strictly managed via Keycloak Identity Manager, requiring the presentation of JSON Web Tokens (JWT) for every call. The system utilizes JSON as the standard exchange format, ensuring that metadata, threat indicators, and cryptographic anchors are parsed consistently.
- **Challenges and overcoming them:** a significant challenge was ensuring that the gateway could handle the asynchronous nature of blockchain transactions without blocking the user interface. This was overcome by implementing Fabric event listeners (e.g., *RequestOpened*, *PartialAnchored*), allowing the dashboard to update live as transactions are committed.

The comprehensive list of RESTful lifecycle and verification endpoints, along with the detailed authentication flow using Keycloak-issued tokens, is documented in Chapter 6 of D5.3 (Secure Data Exchange Platform v2).

5.2 Apache Kafka

Apache Kafka serves as the central message bus for the platform. Security events from the Wazuh Server logs are streamed into Kafka topics, allowing components like the Anomaly Detector IDS to consume network flow features asynchronously without requiring direct connections to the telemetry source.

Apache Kafka has now been integrated, enabling near real-time data distribution across the detection and analytics layers.

- **Operational Application:** the system now streams Suricata EVE JSON records directly to the on-premise Kafka topic as they are generated. This serves as the primary input for the Anomaly Detector IDS, which asynchronously consumes flow-level features to identify behavioural deviations without taxing the primary SIEM performance.
- **Lessons Learned:** a critical lesson learned during deployment concerned network visibility within Kubernetes. Initially, container isolation prevented the message bus from seeing the host-level network traffic needed for accurate monitoring. The consortium resolved this by adopting a host-networking topology (*hostNetwork: true*), allowing the monitoring agents to bind directly to the physical host interfaces

© CYberSynchrony, 2024

The specific Kafka topic configurations, the asynchronous inference pipeline for the anomaly detector, and the host-networking topology used to ensure container visibility are explored in detail in Chapters 3 and 5 of D4.3 (Integrated Cybersecurity Monitoring Suite v2).

5.3 Distributed Ledger Technologies (DLT)

The integrity layer utilizes a Hyperledger Fabric permissioned network for anchoring cryptographic evidence.

The anchoring process follows a DP → HE → SHA-256 flow, where only SHA-256 hashes are written to the ledger, rather than raw records. This ensures a tamper-evident audit trail that is independently verifiable through Hyperledger Explorer.

The integrity layer has matured from a simple test network into a permissioned Hyperledger Fabric network with dedicated peer organizations and an ordering service.

- **Evolution of the Data Model:** unlike the generic key-value store of version 1, version 2 introduces three purpose-built record types, *RequestAnchor*, *PartialAnchor*, and *ResultAnchor*, to track the complete lifecycle of a cross-border exchange. This allows auditors to reconstruct a request's history while ensuring that no raw records or plaintext values ever touch the ledger.
- **Optimization Success:** a significant optimization was achieved through the implementation of local pre-aggregation. By anchoring only a single fingerprint of a differentially private partial sum per dataset, the project achieved a 40x reduction in cryptographic work, enabling end-to-end requests to complete faster.

The formal specification of these purpose-built record types, the chaincode function surface, and the production-path performance scaling benchmarks are detailed in Sections 6 and 7 of D5.3.

5.4 Platform Integration

The Evidence Integrity System is designed to integrate with external threat intelligence repositories like MISP and collaborative networks such as the CSIRT Network. This integration enriches local alerts with global context and ensures that shared intelligence artifacts, such as hardening playbooks or vulnerability advisories, are anchored on the blockchain to attest to their authenticity and origin.

The Evidence Integrity System is now a fundamental pillar for cross-border threat-intelligence sharing, facilitating the exchange of cyber defence artifacts between Member States.

- **Collaborative Workflows:** the platform enriches local alerts by correlating them with MISP Indicator of Compromise (IoC) repositories. When a shared artifact (such as a phishing indicator or a hardening playbook) is exchanged, its SHA-256 fingerprint and structural metadata are anchored on the blockchain to attest to its authenticity and origin.
- **Impact on KPIs:** this integration directly supports the goal of establishing a cohesive European defence front, providing the technical trust necessary to meet the benchmark of sharing information in 75% of cyber incidents and crises. Through Hyperledger Explorer, auditors can independently verify the frequency and authenticity of these exchanges, moving from self-reporting to evidence-based performance tracking.

The operational correlation between local alerts and MISP indicators, including their visualization within the SIEM environment, is demonstrated in Chapter 4 of D4.3, while the specific anchoring sequence for shared intelligence artifacts is provided in Section 8 of D5.3.

© CYberSynchrony, 2024

6 KPIs Mapping

This chapter maps the **Evidence Integrity System v2** to the specific project Key Performance Indicators (KPIs) it addresses. The system provides the technical verification and unalterable audit trails necessary to validate the following performance metrics.

6.1 KPI 3.6: Risk Scenarios Analysed

This KPI tracks the quantity of customized risk scenarios analysed to evaluate the potential impact of cyber threats on critical sectors. The Evidence Integrity System v2 (**D5.4**) provides the technical verification necessary to move beyond simple alert counting toward documenting realistic "what if" situations for each pilot.

By recording affected assets, potential outcomes, and risk severity in an unalterable format, the project aims to **increase analysed risk scenarios by 15%**, achieving a target of at least **12 customized scenarios.**

Table 4: KPI 3.6: Risk Scenarios Analysed.

KPI ID	**KPI Name**	**//**	**Owner**
KPI3.6	**Risk Scenarios Analysed**	//	MER
Increase analysed risk scenarios by 15% (≥12 customised scenarios)			
Participating partners & Role in KPI Measurement		**Components involved**	**Evidence collection process & validation approach**
MER and Pilots: collaborate to define and analyze realistic "what if" situations for each pilot.		CYBERRA, CYBRITE	Review each scenario analysis and compare year-over-year changes to ensure threat models remain synchronized with current landscapes.
Current Value/Target	**Date of Measurement**	//	**Next Actions** (if required)
Pilot-specific scenarios are being defined.	At D5.4 v1.0 submission (M24)	//	Finalize the scenario analysis register for M36 reporting

© CYberSynchrony, 2024

6.2 KPI 4.5: Incident Collaboration Index

This metric evaluates the effectiveness of cross-border incident response coordination based on successful collaborative efforts. The project utilizes data from unified response mechanics in Task 5.3 to calculate an Incident Collaboration Index with a target of 70%.

As the consolidated version of the integrity suite, D5.4 provides the unalterable forensic techniques and verifiable chain of custody required to prove that shared information was complete, clear, and timely during joint exercises.

Table 5: KPI 4.5: Incident Collaboration Index.

KPI ID	**KPI Name**	**//**	**Owner**
KPI4.5	Incident Collaboration Index	//	BYTE
Target			
Participating partners & Role in KPI Measurement		**Components involved**	**Evidence collection process & validation approach**
BYTE (Lead) with MER: utilize data from unified incident response mechanics (T5.3)		CYRESCUE, CROSS-CORE	Track and analyse cross-border incident response collaborations via participant surveys.
Current Value/Target	**Date of Measurement**	//	**Next Actions** (if required)
Initial collaboration exercises have been initiated.	Early pilot runs	//	Aggregate survey results from the upcoming cross-border pilot exercises.

6.3 KPI 5.1: Number of Risk Monitoring Services Provided

This KPI measures the quantity of risk monitoring services offered as part of the project's secure communication and information sharing infrastructure. D5.4 acts as a foundational component by ensuring the integrity of evidence collected by 25 risk monitoring services, which include active setups for Wazuh endpoint groups, Suricata network segments, and Kitsune monitoring profiles. Success is further validated through user surveys

© CYberSynchrony, 2024

aimed at achieving a 95% satisfaction rating regarding alert accuracy and maintaining a false positive rate below 5%.

Table 6: KPI 5.1 Number of Risk Monitoring Services Provided.

KPI ID	**KPI Name**	**//**	**Owner**
KPI5.1	Number of Risk Monitoring Services Provided	//	MER
Participating Partners & Role in KPI Measurement		**Components involved**	**Evidence collection process & validation approach**
MER and Pilots: deploy and monitor active service groups across pilot infrastructures		CYRESCUE, CROSS-CORE	Conduct user surveys to assess the accuracy of detections and the timeliness of alerts.
Current Value/Target	**Date of Measurement**	//	**Next Actions** (if required)
Deployment of modular services (CYRESCUE, CROSS-CORE) is ongoing.	Early pilot runs	//	Finalize performance testing and user satisfaction benchmarks for version 2 of the services.

© CYberSynchrony, 2024

7 Conclusions

The Evidence Integrity System v2 (D5.4) represents a significant evolution of the project's evidence-preservation framework, transitioning from an initial conceptual design into a prototype fully integrated within the CYberSynchrony platform and ready for validation using real pilot datasets provided by AMC, UPRC and EGL.

By operationalizing a robust pipeline centred on performance-efficient blockchain-based protocols, specifically a permissioned Hyperledger Fabric network, the system provides the foundations for maintaining an unalterable chain of custody for digital forensic artifacts exchanged across Member State borders. This implementation is designed to preserve the integrity of digital evidence and support the maintenance of its forensic validity throughout its lifecycle, which is a critical prerequisite for secure cross-border incident response and mutual assistance.

The system’s technical maturity is further reflected in its support for a diverse range of structured threat data types, including STIX-formatted IoCs, incident reports, and MITRE-mapped TTPs, as well as its capability to normalize heterogeneous inputs from SIEM tools such as Wazuh and network IDS such as Suricata into a unified, verifiable format.

Through the evaluation of advanced cryptographic techniques such as Differential Privacy (DP) and Fully Homomorphic Encryption (FHE), the consortium has investigated approaches to balance strong privacy guarantees with the project's real-time performance requirements.

D5.4 delivers a prototype fully integrated into the CYberSynchrony platform, ready for testing and validation with the aim of supporting the project’s Key Performance Indicators, including targets such as increasing information sharing frequency to 75% and achieving a 20% reduction in identified risks.

This consolidated release provides the basis for a dependable evidence plan designed to foster cross-border collaboration, enabling hospitals, universities, and municipalities to share security insights with increased confidence in the authenticity and integrity of exchanged data.

© CYberSynchrony, 2024

8 References

[1] Wazuh – Open Source Security Platform. [Online]. Available: https://wazuh.com/
[2] Apache Kafka – Open Source. [Online]. Available: https://kafka.apache.org/
[3] MITRE ATT&CK. [Online]. Available: https://attack.mitre.org/

© CYberSynchrony, 2024