Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

CYDERCO - CYber DEtection, Response and COllaboration

D2.2. Pilot design

Deliverable date: 2024-06-26

Status: Final

Version: 1.0

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

List of changes

Version	Date	Description	Author(s)
0.1	18.06.2024	First Version	Christine Demeter
0.2	24.04.2024	Final Version	Christine Demeter
1.0	26.06.2024	Quality Assurance	Liana Predut

Assinado por: Isabel Cecília Correia da Silva Praça Gomes Pereira
Identificação: BI09480460
Data: 2024-06-28 às 11:10:27

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

Contributors

Role	Contributor's Name	Entity Name - Beneficiary
Deliverable Lead	Christine Demeter	DNSC
Contributor	Marius Duță	DNSC
Contributor	Mihaela Dan	DNSC
Contributor	Antonio Radu	DNSC
Contributor	Mihai Nena	DNSC
Contributor	Ștefan Tănase	DNSC
Contributor	Eva Maia	ISEP
Contributor	Isabel Praça	ISEP
Contributor	Rodrigo Diaz Rodriguez	Atos IT
Contributor	Hristo Koshutanski	Atos IT
Contributor	Mircea Avram	Eviden Technologies (Ro)
Contributor	Ioana-Andreea Craciun	Eviden Technologies (Ro)
Contributor	Gabriel Petre	Eviden Technologies (Ro)
Contributor	Mihai Belu	Eviden Technologies (Ro)
Contributor	Andrei Chipaila	Eviden Technologies (Ro)
Contributor	Cristian Radu	Eviden Technologies (Ro)
Contributor	Alexandru Rusandu	Eviden Technologies (Ro)
Contributor	Dan Brasov	Eviden Technologies (Ro)
Contributor	Alexandru Velcea	Eviden Technologies (Ro)

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

Approvers

Entity Name - Beneficiary	Project Manager	Signature
Eviden Technologies SRL	Ovidiu Calancea	X Ovidiu Calancea — Digitally signed by Ovidiu Calancea Date: 2024.06.28 13:35:48 +03'00'
Instituto Superior De Engenharia Do Porto	Isabel Praça	X
Directoratul National De Securitate Cibernetica	Christine Demeter	Semnatar: Demeter Christine Data si ora semnarii: 27-06-2024 13:39:30 X
Atos Spain SA	Rodrigo Diaz Rodriguez	X Rodrigo Diaz Rodriguez — Digitally signed by Rodrigo Diaz Rodriguez Date: 2024.06.27 13:05:04 +02'00'

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

Contents

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

1. Glossary: Acronyms, Terms and Abbreviations

Acronyms

AI	Artificial Intelligence
CMM	Capability Maturity Model
CSO	Critical Service Operators
CTI	Cyber Threat Intelligence
DoS	Denial of Service
ENISA	The European Union Agency for Cybersecurity
EU	European Union
HIDS	Host-based Intrusion Detection System
ID	Identifier
IoC	Indicator of Compromise
IP	Internet Protocol
IT	Information Technology
NIST	National Institute of Standards and Technology
NTA	Network Traffic Analysis
SOC	Security Operations Center
TIP	Threat Intelligence Platform
TTP	Tactics, Techniques, and Procedures

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

2. Introduction

CYDERCO (CYber DEtection, Response and COllaboration) project aims to develop, test, and validate components which will support and enhance the detection and response capabilities of relevant entities, including private and national SOCs, to fight against cyber threats that affect network and information systems across the European Union.

CYDERCO will include a Detection and Response hub which will be aiming to improve the detection capabilities of malicious activities by combining information coming from different layers with AI and dynamical learning about the changing threat landscape. It is composed of 4 main building blocks.

The Data Analytics module will ingest and process data from multiple sources to detect threats. It will provide an intuitive user that allows security teams to access relevant information and context easily.
The Network Traffic Analysis (NTA) module will monitor network traffic to detect malware or abnormal network activities. When the NTA solution detects any anomalies, it will raise alerts that can be transferred for further analysis to SOCs.
The host-based intrusion detection module will detect malicious activities posing cyber threats, including malware affecting supported assets, such as workstations. It will use various techniques to detect threats.
Finally, an AI-driven analytics module will intelligently identify patterns and anomalies. The Detection and Response Hub should be fast and flexible, equipping SOC engineers with the necessary information to efficiently detect, triage, investigate, and respond to threats.

Additionally, CYDERCO will include a Threat Intelligence Platform that will provide SOCs with valuable threat intelligence. This will improve collaboration, efficiency, and proactivity in dealing with cyberattacks.

2.1 Deliverable Purpose

This deliverable is an output of Task T2.2 “Pilot definition”. It aims to provide in-depth information about the Pilot that will be used to demonstrate and validate the solution, use cases, and scenarios that need to be covered. The document will encompass the functional description of use cases and their specific challenges and constraints. The architectural view of the pilot's design will be used in Task T5.2 to guide the implementation and deployment of the platform in the pilot. Thus, this deliverable describes the design of the pilot (including architectural design applied to the scenarios, services, and exploitation paths) and the anticipated evaluation strategy.
The objective of this deliverable is to outline the methodologies, scenarios, and frameworks utilized to evaluate the effectiveness and capabilities of the CYDERCO platform in different cybersecurity contexts.

Building on the foundational purpose mentioned earlier, Table 1 provides a comparative analysis of the current cybersecurity state and the significant enhancements achieved with the implementation of the CYDERCO platform. By evaluating key performance indicators and specific benefits, we demonstrate the transformative impact of CYDERCO on the organization's overall security posture.

Table 1 - CYDERCO Platform benefits

Objectives	Without CYDERCO	With CYDERCO
Develop a platform for advanced detection of malicious activities and security incidents to support and strengthen SOC ecosystems.	Cybersecurity personnel assistance	Intuitive user interface providing most of the information in a single solution
	Environment with limited threat detection solutions	Enhances threat detection capabilities by using AI and consolidating threat data from various sources into a unified platform
Develop a platform for storing and sharing actionable threat intelligence among entities dealing with cyber threats	Limited CTI sharing	Enables automated CTI sharing, facilitating information exchange in standardized formats and ensuring privacy and anonymity
	Difficulty in quick decision-making	Actionable CTI scoring

2.2 Scenarios Highlighting CYDERCO's Operational Impact

To further illustrate the practical benefits and effectiveness of CYDERCO, this section presents detailed scenarios that showcase its capabilities in real-world cybersecurity contexts. These scenarios highlight the platform's ability to strengthen threat intelligence sharing which enhances detection, analysis, and response processes, emphasizing the substantial improvements compared to the current state.

Scenario 1: Data Exfiltration on National CERT

- Situation: Breach at National CERT.
- Services and Paths:
  - National CERT to national subscribers.
  - Sectorial CERT for various sectors.

Created Services: Wartime intelligence, automated enrichment, local awareness

Scenario 2: Ransomware Attack on a Public Hospital

- Situation: Ransomware attack on a public hospital.

- Services and Paths:
  - National CERT to national subscribers
  - Sectorial CERT – Healthcare subscribers
  - Local - Organizations.

Created Services: Wartime intelligence, automated enrichment, local awareness

The above scenarios highlight its critical capabilities and benefits in effectively addressing diverse cybersecurity challenges in different organizations.

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

3. Methodology

In this chapter, we present the systematic approach and procedures employed in this study, detailing the research design, data collection methods, and analytical techniques used to investigate proposed scenarios. By providing a clear and comprehensive overview of the methodology, we ensure the reproducibility and reliability of the study's findings. This chapter serves as a guide to understanding how the research was conducted and the rationale behind the chosen methods.
The goal of this document is to provide a thorough description of the pilot project designed to demonstrate and validate the CYDERCO platform. It encompasses scenarios, architectural design, integration, services, and exploitation paths.
To define the pilot's functional aspects, address challenges, and establish the foundation for implementation and deployment, the following actions will be taken:

1. **Developing Pilot Scenarios**
2. **Creating a Logical Layout**
3. **Adapting Incident Response Phases**
4. **Evaluating the Pilot**

3.1 Developing Pilot Scenarios

Scenario 1: Data exfiltration on National CERT
This scenario will highlight the response to a cyber incident affecting a national-level cybersecurity organization.
Scenario 2: Ransomware attack on a public hospital
This scenario will demonstrate the response to a cyber incident in a healthcare setting, emphasizing the impact on critical infrastructure.
Both scenarios were chosen to illustrate the wide applicability of the project's components, demonstrating their utility in creating services across various sectors and organizations, from local entities to national institutions.

3.2 Creating a Logical Layout for the infrastructure architecture

The current section focuses on developing a logical layout for the pilot components to effectively showcase the services created and their potential exploitation paths. This layout will provide a clear visual representation of how the components interact and integrate within the scenarios.

The infrastructure for the pilot tests will be built to reflect a realistic organizational environment. This includes the necessary components such as an IT&C network, network users, and managed IT data, all within an organization with established procedures.

3.2.1 IT data required for the scenarios

To achieve the project's functional objectives, the following high-level data will be aiming to be collected from the assets affected by security incidents in the scenarios:

Network related data, such as:

- IP addresses, ports, protocols

Network related data, such as:

- System data from endpoints and servers to check for any signs of unauthorized access or suspicious activities
- Process executions, process terminations, parent process, child process (e.g.: execution tree)

Threat Intelligence, such as:

- Hash values of malicious files
- Behavioral signatures
- URLs of known malicious domains, if applicable
- IP addresses of C2 servers

3.2.2 Virtualized Infrastructure

1. Physical Servers:

Physical servers will form the backbone of the virtualized environment. These servers will provide the necessary computing power and resources to support the virtualization layer and the various virtual machines required for the scenarios.

2. Virtualization Platform:

Proxmox (or other similar software): This open-source server management platform will likely be used to create and manage the virtualized environment. Proxmox allows for efficient resource allocation and management, enabling the creation of multiple virtual machines on physical servers.

3. Operating Systems:

Windows Operating Systems: Provided by Microsoft for development purposes, these systems will be valid for three months. They will be used to simulate the typical operating environments found in organizations.

Linux Operating Systems: These will also be part of the virtualized infrastructure, offering a diverse range of environments to test the CYDERCO platform's capabilities. Linux systems are often used in server environments and for specific applications that require robust security and stability.

3.3 Applying Incident Response Strategies in Scenarios

The incident response phases—Preparation, Detection, Containment, Eradication, Recovery, and Post-Incident Activities—will be adapted from the NIST 800-61 Computer Security Incident

Handling Guide. This adaptation ensures alignment with both EU Detection Triage Analysis Incident Response (ENISA recommendations) and the SANS Incident Response lifecycle and phases. Furthermore, it will provide a robust framework for handling incidents in the pilot scenarios, while also meeting all requirements for demonstrating the components, from detection features to threat intelligence processing and distribution.
The technical components of each organization highlighted in the scenarios will be emphasized to simulate compromised infrastructures.

Scenario 1: Data exfiltration on National CERT:

- The infrastructure will simulate a full-scale National CERT environment, with a virtualized IT&C network and the necessary procedural frameworks.
- Various virtual machines will be set up to represent different components of the CERT, such as servers, workstations, and networking devices.

Scenario 2: Ransomware Attack on a Public Hospital:

- A virtual hospital IT environment will be created, including networked medical devices (except for OT and IOT devices), servers, and user workstations.
- The virtual infrastructure will mimic the constraints and challenges that hospital IT departments face in the real world, such as limited resources and the need for rapid recovery.

By leveraging this virtualized infrastructure, the pilot tests can accurately simulate real-world conditions and demonstrate the effectiveness of the CYDERCO platform in diverse and dynamic environments.

3.4 Evaluating the Pilot

The evaluation of the pilot will be done using the **Capability Maturity Model (CMM)** methodology.

The Capability Maturity Model (CMM) plays a crucial role in the pilot definition by providing a structured framework for evaluating and improving the maturity of cybersecurity processes across different scenarios. By leveraging the CMM methodology in each scenario, the pilot systematically assesses and enhances several phases of the incident management lifecycle, such as detection, containment, or post-incident activities such as threat intelligence sharing. This approach showcases areas where the security posture is strengthened and aligns with the project's Key Performance Indicators (KPIs).

Each scenario will be evaluated through an initial measurement phase and a post-implementation phase.
The initial measurement which this deliverable is executing the baseline maturity of cybersecurity processes before using CYDERCO, while the post-implementation estimation highlights the targeted improvements achieved through CYDERCO's capabilities. This comprehensive approach underscores the specific benefits of the CYDERCO platform, demonstrating how its advanced capabilities contribute to enhanced threat detection, efficient incident management, and continuous improvement in cybersecurity practices.

The final measurement will be performed in WP5, and it will validate the accuracy of the estimations currently described in the post-implementation sections of *Table 2: Capability Maturity Model - Data Exfiltration Scenario* and *Table 3: Capability Maturity Model - Ransomware attack on a public hospital.*

The CMM consists of five maturity levels, each depicting a different degree of process sophistication and capability:

Level 1 - *Initial*

Processes at this level are often undocumented and subject to frequent changes, driven in an ad hoc, reactive manner by users or events and subject to change in an undocumented way. This can create a chaotic and unstable environment for the processes.

Level 2 - *Repeatable*

It is characteristic of this level of maturity that some processes be repeatable, possibly with consistent results. While process discipline is unlikely to be rigorous, its presence (where applicable) may help to ensure that existing processes are maintained during times of stress.

Level 3 - *Defined*

It is characteristic of processes at this level to be defined, documented, and subject to some degree of improvement over time. While these standard processes are established, they may not have been systematically or repeatedly used enough for users to become proficient or for the process to be validated in a range of situations. This stage can be seen as a developmental phase, with the potential for the process to mature as it is used more widely, and users become more skilled.

Level 4 - *Managed (Capable)*

It is characteristic of processes at this level to utilize metrics to demonstrate their effectiveness in achieving process objectives under different operational conditions. The process has been tested, refined, and adapted to ensure its suitability in multiple environments.

Process users have experienced the process in multiple and varied conditions and can demonstrate competence. The maturity of the process allows for adaptations to projects without notable loss of quality or deviations from specifications. Process Capability is established from this level.

Level 5 - *Optimizing (Efficient)*

It is characteristic of processes at this level to focus on continually improving process performance through incremental and innovative technological changes.

Maturity level 5 focuses on addressing statistically common causes of process variation and changing the process to improve performance. This is achieved while maintaining the likelihood of meeting the established quantitative process improvement objectives.

Automation of manual tasks is pursued at this level.

With the methodological foundation established, we now move to the first scenario, which will illustrate the practical application and impact of CYDERCO's capabilities in enhancing cybersecurity processes within a specific context.

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

4. Data exfiltration on National CERT

4.1 Situation and Problem statement

The following scenario describes the events taking place when a cybersecurity incident affects National CERT 1.

NATIONAL CERT (1) was the target of a spear phishing attack. The attackers sent a malicious email to two NATIONAL CERT employees' private email addresses, promoting a free PDF file editing application. The attackers targeted the infrastructure of the NATIONAL CERT, namely the exploitation of vulnerabilities in the IT infrastructure to gain access and exfiltrate data from the IT systems as part of a sustained, long-term espionage campaign. The incident poses significant risks to critical service operators and data security, requiring an immediate and skilled response to contain and eradicate the threat.

The CSO database contains sensitive data integral to national security operations. This includes detailed records of cybersecurity incidents, vulnerabilities in critical infrastructure, and contact information of key personnel, making it a potentially attractive target for attackers. The database is stored as a .xls file on a virtual machine running Ubuntu Server with a file transfer server function. Access to the National CERT 1 FTP server is secured by unique credentials assigned to each authorized user. In the event of a cyberattack, attackers would target this database to gain a strategic advantage and potentially exploit vulnerabilities detailed within the records. The attack vector involves the attacker gaining remote access to a victim's computer through a deceptive email, which leads to the unauthorized upload of the .xls document to a malicious external address.

Considering this situation, the following pain points will be addressed during the pilot execution:

Tying Incident Response with Threat Intelligence lifecycles to maximize output:

This scenario is based on the assumption that the targeted National CERT is a well-established organization with complex cybersecurity measures in place, including cyber incident response mechanisms.
The underlying activities align with consecrated incident management phases: preparation, detection/analysis, containment, eradication, recovery, and post-incident activities or lessons learned. Furthermore, the National CERT is part of EU-wide organized cyber incident response mechanisms and has access to threat intelligence platforms and a network of cybersecurity experts.
However, the mere existence of these measures does not guarantee that the National CERT can integrate incident response standard phases with the threat intelligence lifecycle. EU National CERTs share information in a fragmented manner, subject to approval at the management level. This fragmentation, among other challenges, hinders efforts to streamline processes and makes it difficult to align incident response phases with the NIST-focused threat intelligence lifecycle,

which includes stages such as planning and direction, collection, processing, analysis and production, and dissemination and feedback.

High-confidence intelligence:

As an integral component of a comprehensive European framework dedicated to responding to cyber incidents, the national CERT has access to cyber-threat intelligence from multiple sources. Nevertheless, the existing collaboration protocols are far from optimal. Communication is disjointed, and there is a recognized deficiency in automated detection and integration of data sources. The current situation hinders the enrichment process, making it challenging to transform existing intelligence into actionable insights.
To enhance confidence levels, it is imperative to establish holistic procedures and tools that enable efficient sighting support and swift identification of high-priority incidents.

Threat Intelligence generation:

To generate superior and adequately comprehensive threat intelligence, the National CERT must enhance its detection mechanisms and data processing capabilities, among other aspects.
The subsequent phase involves refining the accessibility to a centralized platform exclusively designed to exchange CTI.
The repertoire of generated information must encompass technical artifacts that indicate the existence or predict the likelihood of an attack, such as IoCs, valuable insights into threat actors and their *modus operandi* (TTPs), alerts, and reports.

Scalable detection mechanisms:

The current detection capabilities are inadequate in promptly identifying and prioritizing high-severity incidents, resulting in delayed responses to malicious activities.
Discrepancies between the existing detection devices and the tools utilized for reporting and analysis exacerbate this gap, hindering the scalability of the detection mechanism.

Addressing privacy sharing issues in threat intelligence sharing:

Amidst various challenges, privacy issues significantly impact the global hesitancy towards sharing threat intelligence.
Safeguarding classified or sensitive data and enabling anonymous reporting are crucial elements that must be carefully considered to establish an authentic collaboration framework built on trust.

Inter-nation Threat Intelligence Sharing:

Cross-nation threat information exchange facilitates access to valuable insights that might otherwise be unavailable to a National CERT.
Nevertheless, information sharing - especially between different countries - implies adherence to strict protocols to be effective and mutually beneficial. In this case, reporting time is slow as there is virtually no event synchronization between the targeted national CERT and other national CERT and SOC teams.

Leveraging partners' knowledge and experience is only helpful if it is timely obtained and sufficiently detailed to allow all entities to gain comprehensive situational awareness.
Issues such as privacy controls, and format incompatibility, to name a few, make it challenging to cultivate inter-nation threat intelligence sharing.

4.2 Assumptions

- NATIONAL CERT 1 organization has complex cyber security measures in place but requires assistance from the internal SOC to effectively respond to and recover from cyberattacks.
- EU national CERTs share information in a fragmented way, approved at the level of their management.
- EU national CERTs support private organizations facing malicious activities and vice versa.
- EU National CERTs have established protocols for sharing information and responding to cyber incidents affecting critical infrastructure. The said protocols are mutually beneficial for CERTs and essential service operators.
- The attack involves malware capable of performing activities such as exfiltration, utilizing a sophisticated C2 server infrastructure to manage stolen data.

4.3 Phases and activities

4.3.1 Preparation

This section describes the preparation phase of the incident response process.

As a national cyber incident response body, the NATIONAL CERT 1 organization is prepared for an incident. It is also part of EU-wide organized cyber incident response mechanisms, where it has access to threat intelligence platforms as well as a network of experts in cyber security.
Following industry-accepted incident response lifecycle the National CERT 1 engages when required.

Prerequisites:

- NATIONAL CERT 1 infrastructure includes Windows workstations and Linux-based servers;
- NATIONAL CERT 1 has a database not accessible from the internet, only internal, which holds highly sensitive information.
- NATIONAL CERT 1 personnel frequently use email in their activities;
- NATIONAL CERT 1 policies do not prohibit the use of employee personal email addresses;

Sequence of events:

1. Some server-type systems are accessible only from within the internal infrastructure, such as a server running a Linux operating system and hosting the database of essential service operators; since it cannot be accessed from outside the network, it has no additional security measures applied;
2. Cybersecurity awareness programs are implemented throughout the organization. However, employees occasionally overlook the content of certain email communications due to high work volumes or overconfidence in their knowledge. Consequently, they click on links and open attachments.

4.3.2 Detection

This phase is focused on the detection side of the incident response process, where the initial detection occurs.

Prerequisites:

- Functional Detection and Response hub components;
- Users performing day-to-day activities and usable organization assets
- End-User 1 has access to personal webmail
- Threat actor sends phishing email messages

Sequence of events:

1. Two National CERT employees (End-User 1, End-User 2) regularly access their personal email addresses using webmail on their work laptops. One of the two employees (End-User 1) accessed an email from an apparent internal source (later proved as spoofing) and downloaded the attachment which included a free PDF editing tool. The attachment was a ZIP file with .zip extension.
2. After the download was finished, the employee de-archived the ZIP file and clicked the installer .exe. From this point, the malware file started the process of infecting the machine.
3. The HIDS detects unusual activities on the system on the end-user device;
4. After obtaining the initial foothold, the threat actor moves laterally to the file server which holds sensitive information;
5. The threat actor performs other discovery-related activities on the file server;
6. Data exfiltration begins on the file server asset leveraging low footprint protocols;
7. During this phase Detection and Response components alert on the potentially malicious activities.

4.3.3 Containment

This phase focuses on the initial containment, stopping actions-on-objectives for the threat actor, scoping, and initial development of the intelligence.

Prerequisites:

- Functional access to the Detection and Response hub to analyze the alerts and data;
- Containment mechanisms available and ready to be used.

Sequence of events:

- The alerts and/or events are analyzed and corroborated;
- The indicators of compromise are created, as well as a new signature to be shared;
- According to the action defined in the created rule, NTA is able to block the malicious action;
- Data exfiltration is stopped before the full database of operators of essential services data is uploaded to malicious server.

4.3.4 Eradication

This phase is focused on removing all artifacts left by the threat actor and eradicating its foothold from within the organization.

Prerequisites:

- Eradication procedures for infected systems in accordance with NIST 800-61 such as reimagining End-User Workstation 1 and File Server

Sequence of events:

- Reimage End-User 1 device;
- Reimage file server;
- End-User 2 accesses the malicious email. However, the infection does not occur due to the blocking rules previously set in place.

4.3.5 Recovery

In the recovery phase, affected systems and services are restored and returned to normal operations. This includes repairing or rebuilding impacted systems, restoring data from backups, and removing any temporary containment measures put in place. Recovery efforts are carefully planned and executed to ensure that no remnants of the threat are left behind and that systems are fully functional and secure.

Prerequisites:

- Restoring reimaged assets from backups.

Sequence of events:

- Clean backups are used to restore data and systems

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

4.3.6 Post Incident Activities

This section captures the lessons learned, highlighting potential measures to improve the security posture of the organization when faced with a similar threat. This includes threat intelligence distribution.

Prerequisites:

- Functional Threat Intelligence Platform
- Compatible technical sharing mechanisms for processing intelligence, developing lessons learned, and sharing threat intelligence with Sectorial CERTs, National CERT 1, as well as other EU National CERTs (e.g., NATIONAL CERT 2)
- Sharing agreements and processes are in place between the Sectorial CERT, and the National CERT, EU National CERT.

Sequence of events:

1. The National CERT 1 shares intelligence with Sectorial CERTs;
2. The National CERT 1 shares intelligence with National CERT 2.

4.4 Systems, actors, and roles

4.4.1 Human actor and roles

This section describes the actors and roles within the scenario.

The diagram below showcases the generic layout of the project components, information flow, actors, services, and exploitation paths.

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

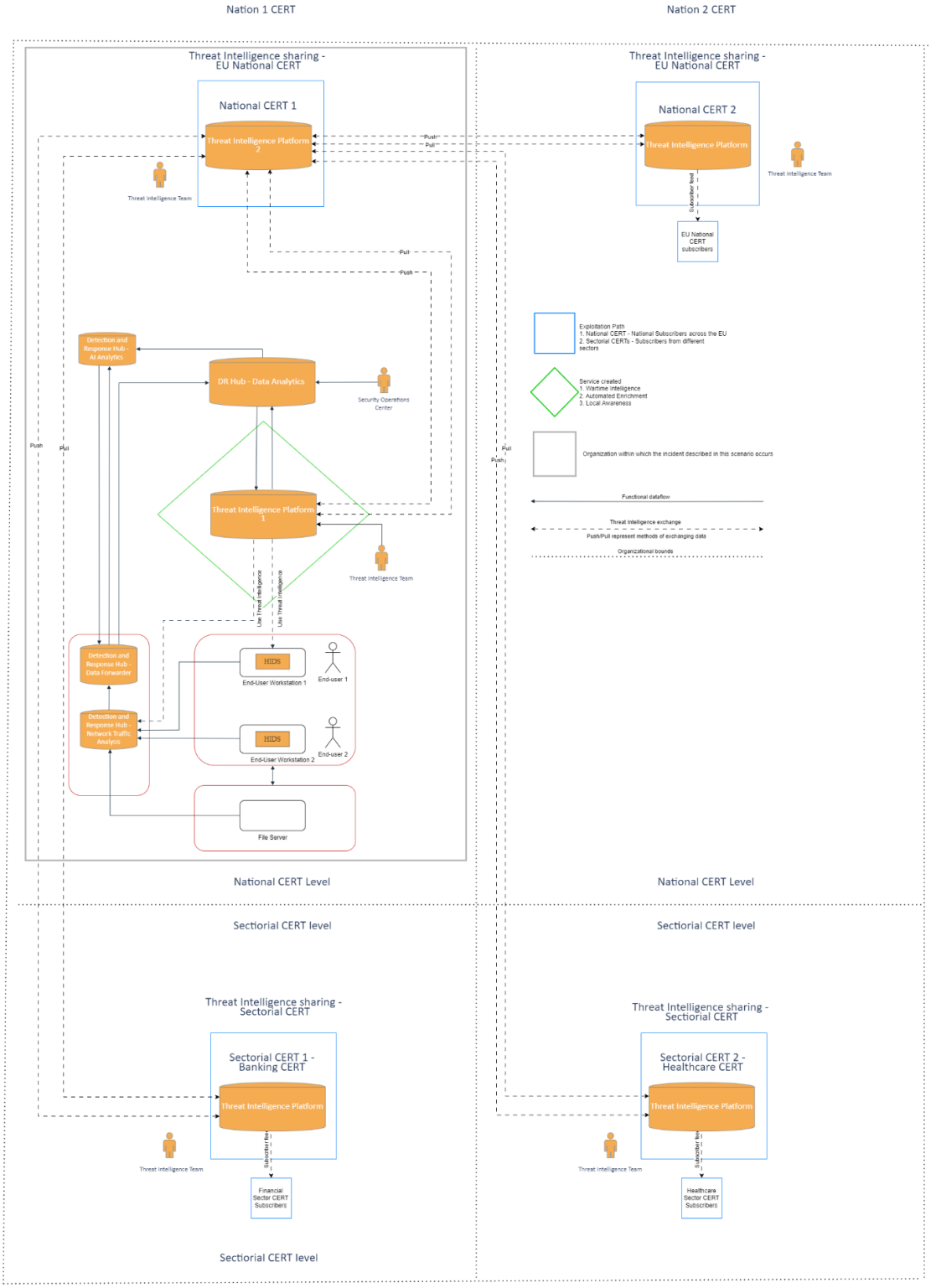

Figure 1 - Systems, actors, services, and exploitation paths representation - Data exfiltration Scenario

- National CERT 1:
  - Business purpose – provides incident response assistance to organizations guided by ENISA recommendations, laws, and regulations such as NIS2;
  - Scenario purpose – is affected by a cybersecurity incident in which a threat actor attempts to exfiltrate information.
  - Human actors:
    - Security Operations Center (SOC analysts) – monitor and analyze security alerts, coordinate with EU CERTs
    - Threat Intelligence (CTI) Team – collect, disseminate and share threat intelligence with other entities and EU partners;
    - End-User 1 - employee which receives the spear phishing email and triggers the incident;
    - End-User 2 - employee which receives the spear phishing email.

- National CERT 2:
  - Business purpose - provides incident response assistance to organizations guided by laws and regulations such as NIS2 and other laws, regulations governing the entity;
  - Scenario purpose - receives intelligence from National CERT 1;
  - Human Actors - Threat Intelligence (CTI) team which processes intelligence.

- Sectorial CERT 1 - Banking Sector CERT:
  - Business purpose - acts as a liaison for all banking service providers or organizations. In this scenario, the Sectorial CERT is intermediating threat intelligence sharing between national, sectorial, and local organizations (banking service providers);
  - Scenario purpose – receives and provides threat intelligence to and from banking entities;
  - Human Actors - Threat Intelligence (CTI) team receives, processes, and shares threat intelligence with other local organizations.

- Sectorial CERT 2 - Healthcare CERT:
  - Business purpose - acts as a liaison for all healthcare providers or organizations. In this scenario, the Sectorial CERT is intermediating threat intelligence sharing between national, sectorial, and local organizations;
  - Scenario purpose – receives and provides threat intelligence to and from healthcare entities;
  - Human actors - Threat Intelligence (CTI) Team receives, processes, and shares threat intelligence with other local (healthcare) organizations.

4.4.2 Computer actor and roles

National CERT 1:

End-user Workstation 1:
- The End-User 1 Workstation is used by a National CERT employee to perform day-to-day actions, including updating the CSO database;
- On this host will run the HIDS Agent;
- The OS being used is a Windows-based machine.

End-user Workstation 2:
- The End-User 2 Workstation is being used by National CERT employee to perform day-to-day actions, including updating the CSO database;
- The HIDS Agent will run on this host;
- The OS used is a Windows-based machine.

File Server:
- Business purpose - This server stores data about Essential Service Operators; the server has access to the Internet, but cannot be accessed from the Internet; it can only be accessed by National CERT 1 employees from the internal network;
- Scenario purpose - is compromised during the incident and the threat actors exfiltrate data;
- The OS used is a Linux machine.

Detection and Response Hub - Host Intrusion Detection System:
- Business purpose - not applicable;
- Scenario purpose:
    - Installed on the End-User Workstation 1 and End-User Workstation 2. The component monitors for cyberthreats;
    - Generates alerts based on monitored actions on the end-user workstations;
    - Uses Threat Intelligence.

Detection and Response Hub - Network Traffic Analytics:
- Business purpose - not applicable;
- Scenario purpose:
    - Monitors via network traffic inspection;
    - Alerts based on detected threats;
    - Blocks known-malicious network traffic;
    - Uses Threat Intelligence.

Data forwarder:
- Business purpose - not applicable
- Scenario purpose:

- Receives and forwards data received from various data sources to upper layers

Detection and Response Hub - Data Analytics:
- Business purpose - not applicable
- Scenario purpose:
  - Acts as a data lake and is used by the SOC for alert investigation;
  - Correlates data of interest and generates alerts

Detection and Response Hub - AI-Analytics:
- Business purpose - not applicable
- Scenario purpose: Leveraging AI algorithms, it acts as a scalable method of generating alerts;

Threat Intelligence Platform 1:
- Business purpose - not applicable
- Scenario purpose:
  - Is leveraged in order to store, process, disseminate, receive, and send threat intelligence within the National CERT organization;

Threat Intelligence Platform 2:
- Business purpose - not applicable
- Scenario purpose:
  - Is leveraged in order to store, process, receive, and send threat intelligence to other entities;

National CERT 2:
- Threat Intelligence Platform:
  - Business purpose - not applicable
  - Scenario purpose:
    - Is leveraged by National CERT 2 to store, process, receive and send threat intelligence;

- Sectorial CERT - Banking Sector CERT:
  - Threat Intelligence Platform:
    - Business purpose - not applicable
    - Scenario purpose:
      - Is leveraged by the Banking CERT to store, process, receive, and send threat intelligence;

- Sectorial CERT - Healthcare CERT:
  - Threat Intelligence Platform:
    - Business purpose - not applicable
    - Scenario purpose:
    - Is leveraged by Healthcare Sector CERT to store, process, receive, and send threat intelligence;

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

4.5 Exploitation paths and Services

4.5.1 Exploitation paths

1*. National CERT Subscribers to National EU CERTs, generally sectorial CERTs, and other organizations of interest.
2*. Sectorial CERT Subscribers to the Sectorial CERT, generally local organizations with business operations focusing on a particular industry (e.g.: Banking CERT subscribers are organizations offering banking services)

*The exploitation paths may be modified and detailed in later Work Packages and dedicated deliverables.

4.5.2 Services

1. Wartime Intelligence - This service represents the intelligence generated during incident response lifecycle. It provides the core intelligence that must be distributed to achieve a stronger, more uniform defense. The role is to distribute critical intelligence during active incidents, enabling rapid and coordinated defensive actions.

2. Automated Enrichment - This service represents the process of automating the threat intelligence contextualization, or enrichment. By streamlining threat analysis, it improves the efficiency and accuracy of threat detection and response.

3. Local awareness - This service showcases the potential of Open-Source Intelligence when utilized in daily operations. Although OSINT may not always provide high-confidence information for preventive measures (e.g.: Wartime Intelligence), it is valuable in the incident response process.

4.6 Capability Maturity Model

Current Capability Maturity Model for the activities and sequences

The Capability Maturity Model (Table 2) is adopted to assess and quantify the performance improvements required to evaluate the project's success. By systematically rating the capabilities of the beneficiary(ies) before and after the project implementation, this framework allows us to measure the positive changes in their capacity and maturity brought about by the project's interventions.

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

Table 2 - Capability Maturity Model - Data Exfiltration Scenario

Scenario phases	Initial measurement	Post implementation (end of project scenario execution)
Preparation	**Repeatable** - The scenario mentions that NATIONAL CERT 1 has complex cybersecurity measures and incident response mechanisms in place and is part of EU-wide organized cyber incident response mechanisms. This suggests that some processes are repeatable, characteristic of the "Repeatable" level.	**Repeatable to Defined –** The scenario specifies that National CERT 1 is part of EU-wide organized cyber incident response mechanisms and has access to threat intelligence platforms as well as a network of cybersecurity experts. This indicates that processes are documented and repeatable. The platform's capabilities, such as the centralized threat intelligence sharing and collaboration features, enable the organization to refine and adapt its processes based on metrics and experiences from multiple environments.
Detection	**Repeatable** - The scenario implies that basic detection mechanisms are in place at National CERTs, but they are reactive and rudimentary, situating them at the Repeatable level, where success can be repeated across similar situations.	**Managed** - CYDERCO's advanced detection capabilities, including AI-driven analytics and network traffic analysis, enable effective threat detection across a range of operational conditions. This aligns with the "Managed" level, where processes are refined and adapted based on metrics and experiences. CYDERCO combines high-confidence signature-based detections with scalable AI-based detections, enhancing the organization's ability to detect both known and emerging threats.
Containment	**Defined** - Initial containment efforts were guided by existing protocols but lacked comprehensive execution,	**Defined to Managed** - Provides the security teams with the means to apply

	placing National CERT in the Defined stage.	structured and consistently documented processes for containing threats. **Managed to Optimizing -** CYDERCO offers automated containment capabilities that enable immediate isolation of infected systems, significantly reducing manual intervention. CYDERCO's actionable CTI scoring allows the organization to prioritize containment efforts based on the relevance and severity of detected threats. This empowers the security team to take preemptive actions to manage and isolate threats effectively.
Eradication	**Repeatable** - Eradication efforts before the scenario were likely inconsistent, lacking a systematic approach, indicative of the Repeatable level.	**Repeatable** - Eradication efforts remain likely inconsistent, lacking a systematic approach, indicative of the Repeatable level. Even if CYDERCO does not have direct capabilities for eradication, the platform provides indirect support through detailed threat intelligence and analytics, which help enable eradication via previous phases.
Recovery	**Repeatable** - Recovery processes before the scenario were implemented as needed but were not systematically managed or optimized, reflective of the Repeatable level.	**Repeatable** - Recovery processes remain implemented as needed and are not systematically managed or optimized, reflective of the Repeatable level. Even if CYDERCO may not directly facilitate recovery through specific tools, it enhances the overall cybersecurity posture of the organization. This helps the organization to be better prepared for recovery processes. CYDERCO improves threat detection, which can

		lead to quicker containment and eradication of threats.
Post-Incident Activities	**Defined -** The initial steps towards reviewing incidents and documenting lessons learned suggest National CERT 's processes were already at a Defined level, with standardized procedures for post-incident analysis.	**Optimizing** - CYDERCO's capabilities, such as privacy-preserving threat intelligence sharing and intelligence distribution and collaboration with other EU and sectorial CERTs, enable the organization to continuously improve its security posture and adapt to emerging threats. This aligns with the "Optimizing" level, where the focus is on continuous improvement and innovation. Benefits: CYDERCO provides enhanced situational awareness by monitoring indicator evolution. It offers meaningful insights that help the organization optimize its post-incident activities and continuously improve its cybersecurity posture.

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

5. Ransomware attack on a public hospital

5.1 Situation and Problem Statement

The following scenario describes the events taking place when a cybersecurity incident affects Hospital 1.

A hospital's (Hospital 1) critical systems and patient data have been encrypted by ransomware, disrupting medical services and compromising patient privacy. The attack requires a coordinated response to mitigate damages, restore services, and prevent future incidents, highlighting the necessity for effective collaboration to prevent other hospitals from being affected.

The National CERT, typically referring to a national cybersecurity center or authority (although the exact acronym might vary by country), plays a critical role in managing cybersecurity threats and incidents. In the context of healthcare and hospitals, a healthcare cybersecurity incident will be reported to a body like NATIONAL CERT. In this scenario, the National CERT receives and shares intelligence with the hospital via the Sectorial CERT for Healthcare.

Considering this, the pain points described below will be addressed during the pilot execution.

Tardy threat intelligence sharing
The level of information exchange between the hospital, national and sectorial CERT does not exist. Communication is limited to email exchanges, which hinders the hospital's ability to receive and potentially act on intelligence.

Challenges in data sharing and event synchronization among entities
The existing mechanisms for sharing and synchronizing intelligence between the hospitals and the organizations which assist these entities during cyber crisis need improvement to ensure effective and timely information exchange.

Limited cyber threat intelligence and situational awareness
There is a gap in the hospital's access to comprehensive cyber threat intelligence (CTI) that affects its situational awareness and ability to preemptively defend against emerging threats.

Limited resources and knowledge
Hospitals typically do not prioritize cybersecurity due to their focus on patient care. They often have limited staff and lack the expertise to address cyber threats.

Inadequate analytic and data showcase capabilities
The hospital's security operations center (SOC) faces challenges in showcasing and performing analytics on ingested data, which hampers its ability to investigate and understand security incidents thoroughly.

Ineffective use of AI for threat detection
The utilization of AI techniques in the hospital's platform is not optimal, limiting its capacity to detect various types of threats and network anomalies crucial for proactive threat mitigation.

Standardized intelligence sharing mechanisms
The hospital should leverage industry-accepted mechanisms to effectively engage in the threat intelligence-sharing process. It is crucial to prioritize addressing standardized mechanisms for data exchange, secure data-sharing protocols, and compatibility with various file extensions or formats.

Privacy concerns when threat intelligence is shared
Privacy-related issues are among the top concerns that hinder the fruition of threat intelligence sharing among entities. The hospital has yet to cultivate trust by implementing advanced encryption and anonymization techniques and displaying adherence to standard and elevated collaboration protocols.

5.2 Assumptions

A threat actor has targeted a hospital and has accessed its IT infrastructure to encrypt systems and demand ransom. The incident poses significant risks to patient care and data security, requiring an immediate and skilled response to contain and eradicate the threat.

- The hospital has basic cybersecurity measures in place
- National EU CERTs share intelligence in a structured, process-approved manner
- Sectorial CERT supports private or government healthcare organizations facing malicious activities
- National CERT has established protocols for sharing intelligence and responding to cyber incidents affecting critical healthcare infrastructure
- The affected entity lacks proper cybersecurity hygiene due to the nature of its business

5.3 Phases and activities

5.3.1 Preparation

This section describes the preparation phase of the incident response process.

The Hospital (1) employs limited IT and security personnel and has basic security measures in place. They operate on a best-effort basis when preparing and responding to cyber threats.
This scenario will demonstrate the effectiveness of our solutions in addressing frequent and potentially severe ransomware attacks.

Prerequisites:

- Hospital 1 IT infrastructure includes Linux servers and Windows end-user devices;
- Legacy workstations running with outdated software packages;
- Lack of cybersecurity training for hospital staff.

Sequence of events:

1. Cybersecurity awareness programs are not implemented;
2. Hospital employees frequently receive suspicious emails, click on links, and open attachments;
3. Hospital policy does not prohibit usage of personal email on organization-owned assets.

5.3.2 Detection

This phase is focused on the detection side of the incident response process, where the initial detection occurs.

Prerequisites:

- Functional Detection and Response hub components;
- Hospital employees sometimes use personal email inbox for work-related tasks. In this case, a personal mailbox accessed by webmail interface is used (e.g.: Yahoo Mail, Proton Mail).
- Threat actor sends phishing email messages

Sequence of events:

- Attacker sends a spear phishing email to the targeted employee;
- An employee accesses their personal email box through a browser-based interface.
- The employee unknowingly opens the email and accesses the attachment or link, which triggers the download and execution of malicious code on their workstation;
- The executed malicious code establishes a backdoor communication with the attacker's server, allowing the attacker to command the infected machine and potentially discover and spread to other systems.
- Attacker uses the credentials found on the infected workstation to gain unauthorized access to a server within the network, potentially housing sensitive information or critical operations;
- The threat actor performs other discovery-related activities on the file server;
- Attacker attempts to exfiltrate data from both the infected workstation and the compromised server. This step involves identifying valuable data, packaging it, and transferring it out of the network to a location controlled by the attacker;

- During the investigation of the alerts, the activities are identified as being malicious;
- The threat actor begins to perform data exfiltration;
- Afterwards the attacker deploys ransomware on both the employee's workstation and the server, encrypting files and demanding a ransom for the decryption keys. The deployment of ransomware can serve as both a final attempt to extract value and a means to cover their tracks;
- During the phase the Detection and Response components alert on the potentially malicious activities.

5.3.3 Containment

This phase focuses on the initial containment, stopping actions-on-objectives for the threat actor, scoping, and initial development of the intelligence.

Prerequisites:

- Functional access to the Detection and Response hub to analyze the alerts and data;
- Containment mechanisms available and ready to be used.

Sequence of events:

1. The alerts and/or events are analyzed and corroborated;
2. The indicators of compromise are created;
3. According to the action defined in the created rule, NTA is able to block the malicious action;
4. Data exfiltration is stopped before the full database of patients' data is uploaded to the malicious server;

5.3.4 Eradication

This phase is focused on removing all artifacts left by the threat actor and eradicating its foothold from within the organization.

Prerequisites:

- Eradication procedures for infected systems in accordance with NIST 800-61, such as reimagining End-User Workstation and File Server

Sequence of events:

- Reimaging affected systems;
- All access points created or exploited by the attacker are identified and revoked.

5.3.5 Recovery

In the recovery phase, affected systems and services are restored and returned to normal operations. This includes repairing or rebuilding impacted systems, restoring data from backups, and removing any temporary containment measures put in place. Recovery efforts are carefully planned and executed to ensure that no remnants of the threat are left behind and that systems are fully functional and secure.

Prerequisites:

- Up-to-date and secure backups for all critical data and systems exist

Sequence of events:

- Secure backups are used to restore encrypted data and systems

5.3.6 Post incident activities

This section captures the lessons learned, highlighting potential measures to improve the security posture of the organization when faced with a similar threat. This includes threat intelligence distribution.

Prerequisites:

- Functional Threat Intelligence Platform
- Mechanisms and procedures for reporting and analyzing incidents, developing lessons learned, and sharing threat intelligence with Sectorial CERT, National CERT;
- Sharing agreements and processes are in place between the Hospitals, Sectorial CERT, and the National CERT.

Sequence of events:

3. The Security Team of the hospital needs to share intelligence with the Sectorial CERT;
4. The Sectorial CERT shares intelligence with other hospitals (Hospital 2);
5. Sectorial CERT shares intelligence with National CERT.

5.4 Systems, actors, and roles

The diagram below showcases the generic layout of the project components, information flow, actors, services, and exploitation paths.

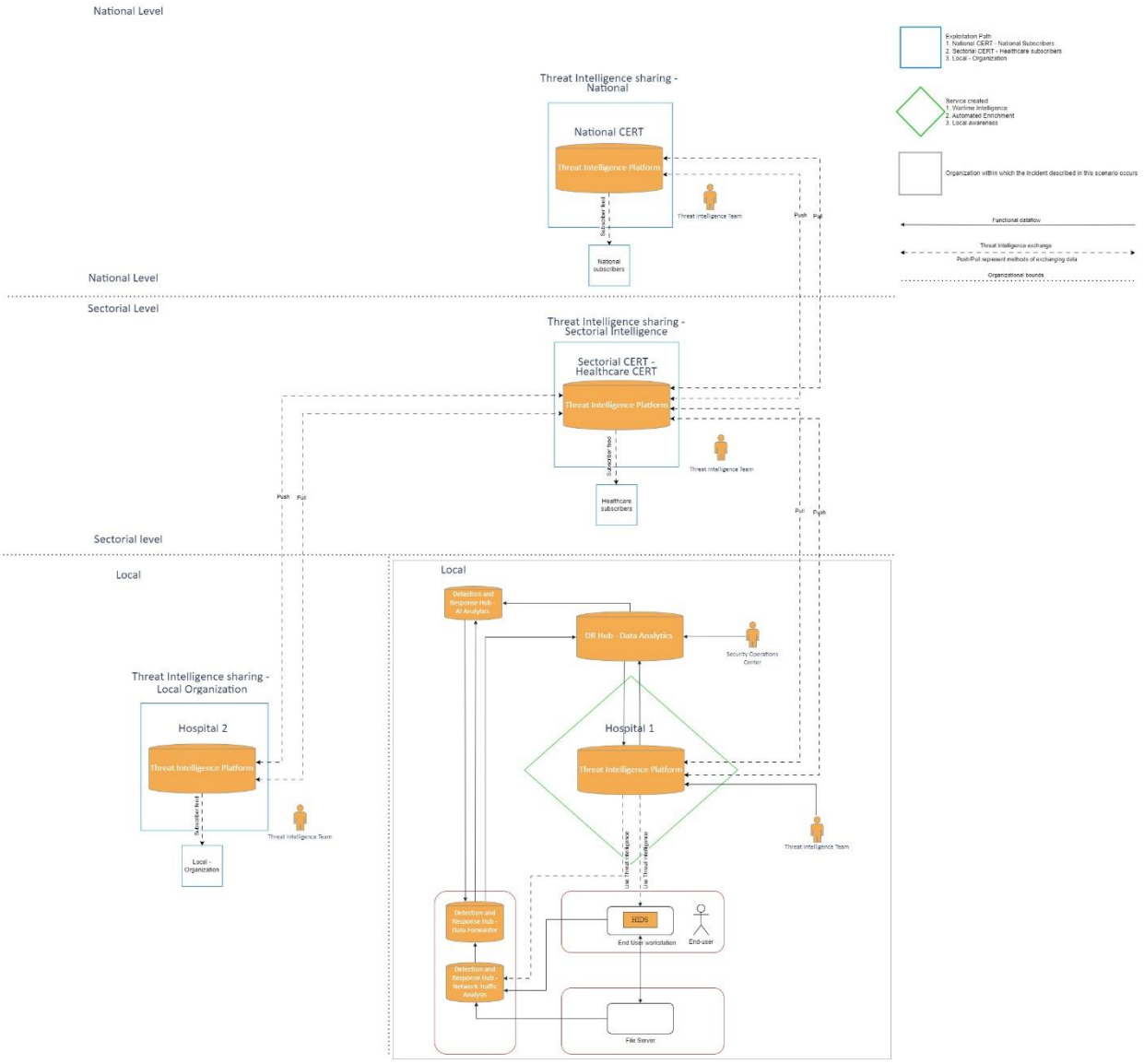

Figure 2 - Systems, actors, services, and exploitation paths representation – Ransomware attack on a public hospital

Ransomware attack on public hospital

The project funded under Grant Agreement No. 101128052 is supported by the European Cybersecurity Competence Centre

5.4.1 Human actors and roles

This section describes the actors and roles within the scenario.

- Hospital 1:
  - Business purpose - provides healthcare services to citizens;
  - Scenario purpose - is affected by a ransomware attack;
  - Human actors involved:
    - SOC responding to Security Incidents;
    - Employee who triggers the incident.
- Hospital 2:
  - Business purpose - provides healthcare services to citizens;
  - Scenario purpose - receives intelligence from Sectorial CERT;
  - Human Actors - SOC analysts who process intelligence.

- National CERT:
  - Business purpose - acts according to legislations such as NIS 2 and provides SME assistance to organizations guided by NIS2 and other laws and regulations;
  - Scenario purpose - the National CERT receives intelligence from the Sectorial CERT;
  - Human actors - Threat Intelligence (CTI) Team.

- Sectorial CERT - Healthcare CERT:
  - Business purpose - acts as a liaison for all healthcare providers or organizations. In this scenario, the Sectorial CERT is intermediating threat intelligence sharing between national, sectorial (healthcare), and local organizations (healthcare providers);
  - Scenario purpose – receives and provides threat intelligence to and from healthcare entities;
  - Threat Intelligence Team: receives, processes, and shares threat intelligence with other local (healthcare) organizations.

5.4.2 Computer actor and roles

Hospital 1:

End-user workstation:

- Business purpose - the end-user workstation is used by hospital employee to perform day-to-day actions;
- Scenario purpose - the end-user workstation is infected due to opening a malicious file sent via e-mail and credentials are stolen;
- The OS used is Windows machine;

File Server:

- Business purpose - File share which users leverage to access internal documents for day-to-day hospital activities;
- Scenario purpose - is compromised during the incident and the threat actor exfiltrates data;

HIDS:

- Business purpose - not applicable;
- Scenario purpose:
    - Installed on the End-user workstation, monitors for cyberthreats;
    - Generates alerts based on monitored actions on the end-user workstation;
    - Uses Threat Intelligence

NTA:

- Business purpose - not applicable
- Scenario purpose:
    - monitors via network traffic inspection;
    - Alerts based on detected threats;
    - Blocks known-malicious network traffic;
    - Uses Threat Intelligence;

Data forwarder:

- Business purpose - not applicable
- Scenario purpose:
    - Receives and forwards data received from various data sources to upper layers.

Detection and Response Hub - Data Analytics:

- Business purpose - not applicable
- Scenario purpose:
    - Acts as a data lake and is used by the SOC for alert investigation;
    - Correlates data of interest and outputs alerts

Detection and Response Hub - AI-Analytics:

- Business purpose - not applicable
- Scenario purpose: Leveraging AI algorithms, it acts as a scalable method of generating alerts;

Threat Intelligence Platform:

- Business purpose - not applicable
- Scenario purpose:
    - Is leveraged by Hospital 1 SOC to store, process, disseminate, receive, and send threat intelligence;

Hospital 2:

Threat Intelligence Platform:

- Business purpose - not applicable
- Scenario purpose:
  - Is leveraged by Hospital 2 SOC to store, process, receive, and send threat intelligence;

Sectorial CERT:

- Threat Intelligence Platform:
  - Business purpose - not applicable
  - Scenario purpose:
    - Is leveraged by Sectorial CERT to store, process, receive, and send threat intelligence;

National CERT:

Threat Intelligence Platform:

- Business purpose - not applicable
- Scenario purpose:
  - Is leveraged by National CERT to store, process, receive, and send threat intelligence;

5.5 Exploitation paths and Services

5.5.1 Exploitation paths

- *National CERT Subscribers to National EU CERTs, generally sectorial CERTs, and other organizations of interest. These organizations handle cybersecurity incidents at the national level and include sectorial CERTs, government agencies, and other organizations of national importance. Their main function is to provide threat intelligence, guidance, and support to enhance national cybersecurity posture.

- *Sectorial CERT Subscribers to the Sectorial CERT, generally local organizations with business operations focused on a particular industry (e.g.: Healthcare CERT subscribers are organizations offering healthcare services). Their main role is to offer industry-specific threat intelligence and support, helping organizations in that sector defend against relevant threats.

- *Local – Organization – Local entities, such as individual hospitals or healthcare providers, which engage directly with Sectorial CERTs. The healthcare organizations have the possibility to exchange, not only subscribe, intelligence with the Sectorial CERT and have capabilities generated by a threat intelligence platform. Their main function is to utilize capabilities generated by a Threat Intelligence Platform (TIP) to enhance their cybersecurity defenses through shared intelligence and insights.

*The exploitation paths may be modified and detailed in later Work Packages and dedicated deliverables.

5.5.2 Services

1. Wartime Intelligence - This service represents the intelligence generated during the incident response lifecycle. It provides the core intelligence that must be distributed to achieve a stronger, more uniform defense. The role is to distribute critical intelligence during active incidents, enabling rapid and coordinated defensive actions.

2. Automated Enrichment - This service represents the process of automating the threat intelligence contextualization, or enrichment. By streamlining threat analysis, it improves the efficiency and accuracy of threat detection and response.

3. Local awareness - This service showcases the potential of Open-Source Intelligence when utilized in daily operations. Although OSINT may not always provide high-confidence information for preventive measures (e.g.: Wartime Intelligence), it is valuable in the incident response process.

5.6 Capability Maturity Model

Current Capability Maturity Model for the activities and sequences

The Capability Maturity Model (Table 3) is adopted to assess and quantify the performance improvements required to evaluate the project's success. By systematically rating the capabilities of the beneficiary(ies) before and after the project implementation, this framework allows us to measure the positive changes in their capacity and maturity brought about by the project's interventions.

Table 3 - Capability Maturity Model - Ransomware attack on a public hospital

Scenario phases	Initial measurement	Post implementation (end of project scenario execution)
Preparation	**Initial** – The hospital's detection capabilities were limited due to workstations running outdated software packages and the low level of preparedness among the cybersecurity staff. These factors resulted in a reactive posture with insufficient monitoring and delayed threat	**Repeatable** - With CYDERCO, the hospital can establish repeatable processes and procedures for responding to incidents, elevating the maturity level to "Repeatable". CYDERCO enhances the hospital's preparedness for sophisticated cyber threats and can be used effectively in environments with less specialized

	identification, reflecting the "Initial" level.	technical staff, thus improving the cybersecurity posture with less reliance on highly trained personnel.
Detection	**Initial** - The hospital had limited detection capabilities, relying on basic tools without a systematic approach.	**Defined** - CYDERCO's detection capabilities enable effective threat detection across a range of operational conditions. This aligns with the "Defined" level, where processes are refined and adapted.
Containment	**Repeatable**: The hospital's initial containment efforts are reactionary and lack fully structured approach, placing it the "Repeatable" level.	**Defined to Managed** - CYDERCO's timely and accurate detection aids the security team in performing efficient manual containment, making the processes structured and consistently applied. **Managed to Optimizing -** CYDERCO offers automated containment capabilities that enable immediate isolation of infected systems, significantly reducing manual intervention. Benefits: CYDERCO enables rapid deployment of signatures and countermeasures, addressing the pain point in data sharing and event synchronization among entities.
Eradication	**Repeatable** - The scenario mentions that the hospital has eradication procedures for infected systems in accordance with NIST 800-61. This suggests that the hospital has documented and standardized procedures for eradicating infected systems, which aligns with the "Repeatable" level of maturity.	**Repeatable** – The hospital has documented and standardized procedures for eradicating infected systems, which aligns with the "Defined" level of maturity. Eradication efforts remain likely inconsistent, lacking a systematic approach, indicative of the Repeatable level. Even if CYDERCO does not have direct capabilities for eradication, the platform provides indirect support through detailed threat intelligence and analytics, which help structure and execute eradication procedures.

Recovery	**Repeatable** - The scenario states that up-to-date and secure backups of all critical data and systems exist. This indicates that the hospital has some level of recovery processes in place. These are likely repeatable but may not be fully documented or consistently applied, characteristic of the "Repeatable" level.	**Repeatable** - The hospital has some recovery processes in place. These are likely repeatable but may not be fully documented or consistently applied, characteristic of the "Repeatable" level. Even if CYDERCO may not directly facilitate recovery through specific tools, it enhances the overall cybersecurity posture of the organization. This helps the organization to be better prepared for recovery processes. CYDERCO improves threat detection which can lead to quicker containment and eradication of threats.
Post-Incident Activities	**Initial** - The hospital's post-incident activities are largely undocumented, reactive, and driven by ad hoc decisions. The insufficient threat intelligence sharing, challenges in data synchronization, and limited resources contribute to a chaotic and unstable environment, characteristic of the "Initial" level in the CMM.	**Managed to Optimizing** - CYDERCO's capabilities, such as mechanisms for analyzing incidents and sharing threat intelligence, enable the hospital to refine and continuously improve its processes. This aligns with the "Managed" to "Optimizing" levels, where the focus is on continuous improvement.