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

D2.1. Stakeholders’ analysis & requirements elicitation

Deliverable date: 2024-04-25

Status: Final

Version: 1.0

List of changes

Version	Date	Description	Author(s)
0.1	01.03.2024	First Version	Eva Maia
0.2	29.03.2024	Final Version	Eva Maia
1.0	25.04.2024	Quality Assurance review	Liana Predut, Ioana-Andreea Craciun

Contributors

Role	Contributor's Name	Entity Name - Beneficiary
Deliverable Lead	Eva Maia	ISEP
Contributor	João Vitorino	ISEP
Contributor	Isabel Praça	ISEP
Contributor	Rodrigo Diaz	ATOS SP
Contributor	Hristo Koshutanski	ATOS SP
Contributor	Esteban Alejandro Armas Vega	ATOS SP
Contributor	Alejandro Moreno	ATOS SP
Contributor	Mircea Avram	Eviden
Contributor	Gabriel Petre	Eviden
Contributor	Mihai Belu	Eviden
Contributor	Andrei Chipaila	Eviden
Contributor	Cristian Radu	Eviden
Contributor	Alexandru Rusandu	Eviden
Contributor	Ioana Andreea Craciun	Eviden

Approvers

Entity Name - Beneficiary	Project Manager	Signature
Eviden Technologies SRL	Ovidiu Calancea	X Ovidiu Calancea Digital unterschrieben von Ovidiu Calancea Datum: 2024.04.26 14:05:14 +03'00'
Instituto Superior De Engenharia Do Porto	Isabel Praça	X Assinado por: Isabel Cecília Correia da Silva Praça Gomes Pereira Identificação: BI09480460 Data: 2024-04-25 às 17:56:30
Directoratul National De Securitate Cibernetica	Christine Demeter	X Semnatar: Demeter Christine Data si ora semnarii: 25-04-2024 18:09:33 SERVICIUL DE TELECOMUNICAȚII SPECIALE ROMÂNIA
Atos Spain SA	Rodrigo Diaz Rodriguez	X Rodrigo Diaz Rodriguez Digitally signed by Rodrigo Diaz Rodriguez Date: 2024.04.25 18:38:54 +02'00'

1 Contents

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them

2 Glossary: Acronyms, Terms and Abbreviations

2.1 Acronyms

AI	Artificial Intelligence
API	Application Programming Interface
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CPU	Central Processing Unit
CSV	Comma-Separated Values
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service
DL	Deep Learning
DNS	Domain Name System
DoS	Denial of Service
EU	European Union
FDI	False Data Injection
GDPR	General Data Protection Regulation
HDD	Hard Disk Drive
HID	Human Interface Device
HIDS	Host-based Intrusion Detection System
HTTP(s)	Hypertext Transfer Protocol (Secure)
HW	Hardware
ICMP	Internet Control Message Protocol
ID	Identifier
IoC	Indicator of Compromise
IP	Internet Protocol
ISO	International Organization for Standardization

IT	Information Technology
JSON	JavaScript Object Notation
MAPN	Ministerul Apararii Nationale
MISP	Malware Information Sharing Platform
MitM	Man-in-the-Middle
MITRE	Massachusetts Institute of Technology Research and Engineering
ML	Machine Learning
NIST	National Institute of Standards and Technology
NTA	Network Traffic Analysis
OSINT	Open-Source Intelligence
RAM	Random Access Memory
SIEM	Security Information and Event Management
SOC	Security Operations Center
SRI	Serviciul Roman de Informatii
STIX	Structured Threat Information eXpression
SYN	Synchronize
TAXII	Trusted Automated Exchange of Indicator Information
TCP	Transmission Control Protocol
TIP	Threat Intelligence Platform
TIT	Threat Intelligence Team
TTP	Tactics, Techniques, and Procedures

3 Introduction

CYDERCO (CYber DEtection, Response and COllaboration) project aims to develop, test, and validate a platform that will support and enhance the detection and response capabilities of relevant entities, including private and national SOCs, in their fight against cyber threats affecting networks 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 from different layers with AI. The platform dynamically learns about the changing threat landscape and is composed of 4 main building blocks:

The Data Analytics module will ingest and process data from multiple sources to detect threats. It should provide an intuitive user interface for security teams to have access to essential information and relevant context.

The Network Traffic Analysis module will monitor network activity to detect malware or abnormal network. When the NTA solution detects anomalies, it raises alerts that can be transferred to SOCs for further analysis.

The Host-based Intrusion Detection module will detect malicious activities posing cyber threats - such as malware affecting supported assets (e.g., workstations). It will use different techniques to detect threats, including file integrity monitoring and analysis, and correlation of logs collected from the devices.

And finally, an AI-driven analytics module will intelligently identify patterns and anomalies in threat intelligence data. It performs smart correlations across different data sources within the environment.

The Detection and Response Hub should be fast, flexible, and it should provide SOC engineers with the needed information to efficiently detect, triage, investigate, and respond to threats.

Additionally, CYDERCO will include a threat Intelligence platform that will provide SOCs with critical information about threat actors and their TTPs and IoCs. As a result, it will improve collaboration, efficiency, and proactivity in dealing with cyber-attacks. Threat Intelligence must cover the entire attack surface and vectors, while organizations need to watch and hunt for industry-specific threats. It is an integrated part of the SOC where threat intelligence feeds provide actionable risk scorings and help detect unknown threats before they reach the organization.

3.1 Deliverable Purpose

This deliverable is an output of Task T2.1 “Stakeholders’ analysis & requirements elicitation” which aims to identify and engage stakeholders, understand their needs, and define project requirements in line with their expectations. It begins by conducting a thorough stakeholder analysis to identify and prioritize the most influential and interested parties. The document then outlines the methodology used to gather insights from end-users through questionnaires. By addressing the end-users' perspective, the document ensures alignment with their expectations and preferences. Additionally, the document meticulously describes the functional and non-functional requirements of the platform, delineating specific features and quality attributes necessary for its development and implementation.

Overall, this document serves as a foundational reference for informing strategic decision-making, guiding development efforts, and ultimately achieving stakeholder satisfaction and project success.

4 Methodology

Stakeholder analysis and requirements elicitation are critical processes in the development of new solutions in any project or system. This is particularly true for research and development initiatives.

By systematically identifying stakeholders and eliciting their requirements, organizations can ensure that their projects are aligned with stakeholder needs and expectations, ultimately leading to successful outcomes.

The primary objective of stakeholder analysis is to understand the perspectives, interests, and level of influence of each stakeholder. This allows us to effectively manage their involvement throughout the project lifecycle. To begin this process, we held internal discussions to identify all potential stakeholders who may have an interest in or be impacted by the CYDERCO platform. We included both internal and external stakeholders, such as end-users, regulatory bodies, and community groups.

Once we identified these stakeholders, we categorized them based on their level of influence and interest in the project. This helps prioritize stakeholder engagement and determine the most appropriate communication and engagement strategies for each stakeholder group.

Finally, to actively involve stakeholders into the CYDERCO project and gather their input, address concerns, and build support for the platform’s requirements, we prepared a questionnaire and presented it in an external Focus Group.

The questionnaire results supported the requirements elicitation process, allowing us to understand the needs, preferences, and constraints of CYDERCO stakeholders. This was crucial in ensuring that the CYDERCO platform meets the needs of its intended users and stakeholders.

The consortium then analyzed the answers in an Internal Focus Group and contributed to documenting the requirements for the platform. This documentation process captures functional requirements (defining what the system should do) and non-functional requirements (outlining qualities or constraints the system must meet).

After building a comprehensive list of requirements, the consortium prioritized them based on their importance, feasibility, and impact on the project’s success. This helps focus resources and efforts on addressing the most critical requirements first.

Figure 1 summarizes the different phases of the methodology outlined above, which provides a structured approach for conducting stakeholder analysis and requirements elicitation. This approach helps the consortium effectively manage stakeholder engagement and deliver projects that meet stakeholder expectations.

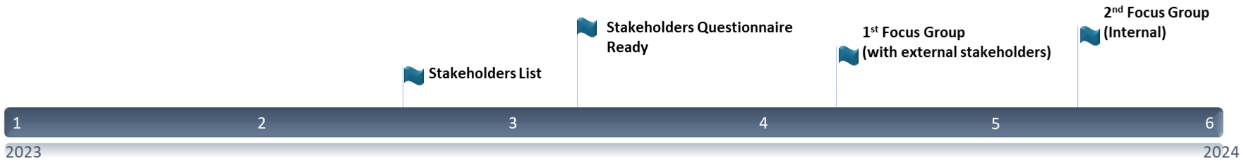
Stakeholders List
Stakeholders Questionnaire Ready
1st Focus Group (with external stakeholders)
2nd Focus Group (Internal)
1
2
3
4
5
6
2023
2024

Figure 1. Phases of Stakeholder Analysis and Requirements Elicitation Methodology

4.1 Stakeholder Groups

CYDERCO platform caters to a wide range of users, from security analysts who will actively utilize it to company board members primarily concerned with its overall impact. Accordingly, the consortium created a comprehensive list of stakeholders representing the diverse spectrum of individuals impacted by CYDERCO.

The table below outlines the various CYDERCO stakeholders identified and categorized into four distinct groups:

- Stakeholder Roles - classify and define the roles of the different stakeholder types.
- Internal Stakeholders - entities that share a common communication process- such as government entities communicating with each other.
- External Stakeholders- entities encompassing for-profit organizations that are publicly, privately, or government-owned and play various roles, such as managing critical infrastructure or operating in sectors such as pharmaceuticals and services.
- Collaborative Partners- companies or organizations providing IT or IT Security services that may offer relevant feedback or information for the project.

It is important to note that a stakeholder may belong to more than one group simultaneously.

Table 1. Stakeholders List

	Name	*Description*
Stakeholder Roles	Chief Information Security Officer (CISO)	Responsible for overall cybersecurity strategy and oversees the SOC's effectiveness.
	Security Analysts	Operational personnel responsible for monitoring, detecting, and responding to security incidents.
	Network Administrators	Collaborate with the SOC to ensure network security and provide necessary insights.
	Incident Response Team	A specialized group within the SOC handling and mitigating security incidents.
	Threat Intelligence Team	A specialized group within Security Operations that collaborates with SOCs.

	IT Operations Team	Works closely with the SOC to implement security measures and maintain system integrity.
	Chief Information Officer (CIO)	Ensures alignment of SOC activities with broader organizational goals.
	Audit and Compliance Teams	Ensure that the SOC adheres to relevant industry standards and regulations.
	Board of Directors	Receives regular updates on cybersecurity posture and risks from the SOC.
Internal Stakeholders	National CERTs	Government organizations that have CERTs/SOCs which interact with SOCs/organizations handling critical infrastructure.
	Government entities	SOCs which fall under government control. E.g.: MAPN SOC, SRI SOC.
	Law Enforcement Agencies	Collaborate with the SOC in case of serious cyber incidents or attacks.
External Stakeholders	Critical Infrastructure Organizations	Organizations that manage EU critical infrastructure. Their SOC teams are directly involved.
	For-profit Organization	Public or privately-owned companies that operate in various domains and have SOC Teams and incident response processes.
	Regulatory Bodies	Authorities overseeing compliance with industry-specific security regulations and standards.
Collaborative Partners	External Security Researchers	Provide insights into emerging threats and vulnerabilities.
	IT Service Providers	Collaborate with the SOC to ensure the security of outsourced services.
	Third-Party Security Vendors	Companies providing tools and solutions for threat intelligence, detection, and prevention.
	Security Service Providers	Organizations that offer security related services.

4.2 Online Questionnaire

A questionnaire was developed to gather the requirements and needs of various stakeholders. It specifically aimed at comprehending the challenges and demands of EU SOCs and collaboration mechanisms at regional, national, and international levels. The primary objective is to explore and outline innovative methods of SOC collaboration and cooperation, facilitate the exchange of best practices, address common issues, and identify avenues for mutual support in responding collectively to cyber crises. Furthermore, the questionnaire seeks to establish effective countermeasures while considering social aspects and economic impacts.

Before pre-testing the questionnaire, the consortium partners discussed the format and wording of the questions. Open-ended questions were preferred over closed-ended ones to encourage respondents to express their views in their own words, revealing the most pressing issues.

Organized into two main sections, the questionnaire begins with a general section aimed at understanding the stakeholders' profiles, gathering information such as position within the organization, sector, organization size, and stakeholder group.

The second section coincides with the main focus and consists of open-ended questions. Here, our objective is to delve into the stakeholders' concerns and challenges regarding the various technologies utilized by SOCs and threat analysts. We aim to identify desired functionalities and features that should be available and automated.

Additionally, through these questions, we seek to ascertain the types of cyber threats and attacks that are of greatest concern to the stakeholders, and whether they are industry-specific. Another crucial aspect addressed in the survey is the method by which stakeholders perform data acquisition and export, aiming to gauge the compatibility and flexibility of the technologies.

Furthermore, the questionnaire explores themes such as information sharing and incident response, aiming to understand the specific types of information stakeholders intend to share and how this can enhance the effectiveness of incident response efforts. Industry standards and communication channels are also discussed. Towards the conclusion, we seek to understand stakeholders' expectations for a collaborative SOC while soliciting feedback and suggestions for improvement in this regard.

The EU Survey tool was selected as the hosting platform for the questionnaire due to its GDPR compliance and the added value of being from an EU domain. It was accessible at this link during January and February 2024.

The survey was initially distributed to all project partners through the CYDERCO mailing list. The recipients were prompted to further distribute the questionnaire within their networks. Additionally, an external focus group was convened and publicized to clarify the survey's objectives and questions. The project partners utilized diverse social media channels to promote the external focus group and the questionnaire.

4.3 External Focus Group

The objective of the external focus group was to engage various CYDERCO stakeholders, acquaint them with the project, and emphasize the importance of responding to the CYDERCO stakeholder questionnaire. An online session was organized via the Microsoft Teams platform to facilitate this. The session brought together not only consortium partners, but also external stakeholders invited via email and through the partners' social networks.

During the session, we commenced with a presentation of the project and its partners, followed by a detailed discussion on the primary objectives of the CYDERCO project. We highlighted our approach to gathering and analyzing requirements from diverse stakeholders to fully comprehend the needs and functionalities to be incorporated into the CYDERCO platform. We also provided an overview of the different sections of the questionnaire and how each stakeholder could utilize the platform.

A total of 20 individuals attended the event, on January 19th,2024, including internal and external participants from the project.

4.4 Internal Focus Group

The internal focus group took place on February 22nd and 23rd, 2024, in person in Porto, Portugal. Its purpose was to analyze the responses to the questionnaire and collaboratively establish the functional and non-functional requirements of the CYDERCO platform. However, at the time of the focus group session, we had received only one response to the questionnaire. While we analyzed this response, we also conducted a brainstorming session to gain insights from the stakeholders' perspective on how they would interact with the system and to identify key requirements for the system's design. The participation of a stakeholder from the consortium, DNCS, added significant value to this discussion by helping us maintain a focus on the stakeholders' needs and aspirations.

In this manner, we established an initial set of functional and non-functional requirements. These were subsequently reviewed and elaborated to attain the first stable version of requirements elicitation.

5 End-users’ Perspective

The consortium's expectations for the questionnaire were not met as only 7 responses were received. We had hoped for a larger number of participants considering the interest shown by stakeholders during the external focus group and our efforts to distribute the questionnaire.

Since at the time of the internal focus group we had received only one response, we decided to make additional efforts to gather more responses. At the same time, we realized the need to involve DNCS, an important stakeholder, in defining the requirements within the consortium. We also acknowledged the importance of analyzing the responses to ensure alignment with the defined requirements.

In this chapter, we delve into an analysis of the received inputs, shedding light on the types of stakeholders and the sectors they represent. This analysis aims to provide valuable insights into the stakeholders' perspectives and their potential impact on the CYDERCO platform requirements.

5.1 Stakeholders and Cyber Threats

The 7 participants represent various positions within the cybersecurity field, offering valuable insights into the requirements of security personnel at different stages of the detection and mitigation of cyber threats. Among the participants are 2 **malware analysts** and 2 **security directors** with similar responsibilities, while the other participants hold unique roles across different organizations. Table 2 provides an overview of the general information of the participants.

Table 2. Overview of participants

Participant ID	Current Role	Team Size	Organization Size
QP1	Director of Security Operations	10-20	-
QP2	System Administrator	-	100-150
QP3	Director of Managed Security Services	-	50-100
QP4	Malware Analyst	10-20	-
QP5	Digital Forensics Expert	10-20	-
QP6	Malware Analyst	-	100-150
QP7	Open-Source Intelligence Expert	-	150-200

Even though the 2 directors solely identified the **Security Service Providers** group, the remaining 5 participants representing security personnel were affiliated with multiple stakeholder groups, which included **National CERTs**, other **Government Entities**, and **Regulatory Bodies**. This enabled them to provide their view on the distinct requirements of different stakeholders.

Figure 2 provides an overview of the overall proportion of responses from each stakeholder group.

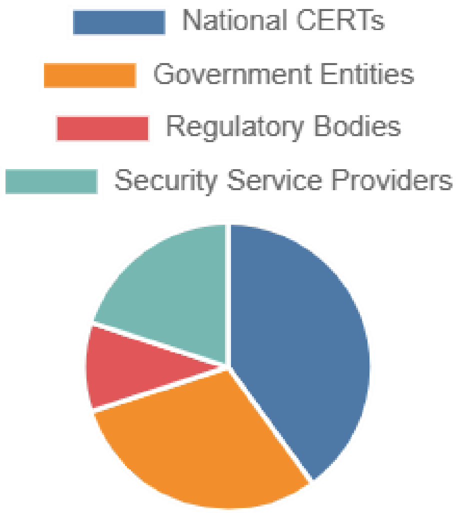

Figure 2. Overview of stakeholder groups

All participants identified **ransomware** and **phishing** as the biggest cyber threats their organizations face, associated with **social engineering** to trick personnel into making mistakes and giving away sensitive and confidential information. However, for other common threats, there was a clear difference between the security personnel that are responsible for directly dealing with threat information and the security directors that oversee the work and take accountability for it.

The responses of the security personnel prioritized detecting and mitigating **malware**, **unauthorized access**, and **data leaks**, as well as addressing **software vulnerabilities**. They also expressed that National CERTs and Government Entities face state-sponsored cyber-attacks that can strain their resources.

On the other hand, Security Service Providers directors indicated that many attacks exploit **compromised accounts** and **misconfigurations** in computer networks, leading to reputational damage for organizations. One response highlighted that internal phishing within an organization should not be overlooked, in addition to external phishing threats.

5.2 Concerns and Challenges

The main focus for all participants was enhancing and streamlining their organization's SIEM systems and processes. The responses revealed challenges with handling **large volumes of data** from **multiple data sources** and limited **data correlation** and **analysis** capabilities within their systems. These issues result in **slow search and lookup times**, hindering the ability of security teams to effectively investigate a security incident and consolidate the relevant information of a cyber threat.

Another important concern for multiple participants is the lack of **accessibility** of SIEMs and TIPs, as there is a need to provide other teams with **easily understandable data access**. In a larger organization, different security teams may require access to data for various investigations, while non-security teams may need certain information for their debugging processes. One of the responses also mentioned that **tracking changes** in data source formats is needed to guarantee data accuracy and compatibility for a complex nested correlation.

Regarding network-based and host-based intrusion detection and prevention, there is a major challenge that all participants identified: the systems used by their organizations produce a relatively **large quantity of false positives** and an even greater number of **unfiltered logs**. This issue is primarily attributed to **insufficient storage capacity** and **lack of automation**. The responses outlined the absence of in-depth analysis of network packet capture files. This makes it difficult to detect anomalies, particularly for smaller teams. Furthermore, some participants' organizations are beginning to merge host-based detection with endpoint solutions due to overlapping functionalities. As a result, endpoint detection and response solutions are being implemented.

Out of 7 participants, 2 were unaware of **Artificial Intelligence** (AI) being used in their systems. However, the remaining 5 indicated that their organizations started to use AI and identified pertinent challenges. The utilized **Machine Learning** (ML) models lack **explainability**, which makes it difficult for security teams to understand the **reasoning behind the predictions** they produce. Additionally, there are concerns regarding the **insufficient data quality** of the datasets used to train these models. When coupled with the reliance on a single data source, this can lead to **false positives** and false alarms.

Overall, for a collaborative platform, the responses highlight the need to **share TTPs and IoCs** among multiple security teams, while **analyzing and correlating** them based on the sectors of activity of the organizations. The feedback also mentions the **integration with MITRE** and the enhancement of the **platform with AI** to tackle novel cyber threats and help automate the analysis. Table 3 provides an overview of the current challenges faced by participants and their expectations for a new platform, organized by technology types.

Table 3. Overview of challenges and expectations

Technology	Current Challenges	Platform Expectations
TIP	Lack of accessibility Lack of analysis automation	Need for sharing of TTPs and IoCs Need for MITRE integration
SIEM	High execution time for queries Lack of data processing capacity Lack of data source integration	Need for data correlation mechanisms Need for data source tracking

NIDS	High number of false positives Insufficient storage capacity Lack of detection automation	Need for in-depth analysis mechanisms Need for a combined detection
HIDS	High number of false positives Insufficient storage capacity Lack of detection automation	Need for in-depth analysis mechanisms Need for a combined detection
AI	Lack of prediction explanations Lack of good-quality data Lack of data source integration	Need for explainable mechanisms Need for minimal false positives

5.3 Technologies and Automations

When asked to detail their expectations regarding the considered technologies, the participants highlighted the importance of an intuitive and easy-to-use **graphical user interface** for the successful adoption of a new platform. A collaborative platform should present complex information about security events in a digestible form, enabling users to quickly understand and act on threat intelligence. Some responses mentioned that more technical users should be given access to **complete system statistics** and detailed **descriptions of threats and anomalies**. It was also noted that users without in-depth expertise should be able to visualize the **current state of system security** and obtain an **overview of security incidents**.

A key functionality highlighted in many responses is the incorporation of AI and ML models to increase the ability to respond to security incidents and improve the quality of incident investigations. By automating parts of the analysis with **continuous integration** from multiple sources, **data enrichment** with **contextual knowledge** from various systems and technologies, and complex nested **data correlation** with meaningful insights and **clearly explained results**, participants anticipate that AI will enable security teams to access powerful analytics.

Another very important functionality for all participants is the ability to perform automated and **customizable searches and lookups**. The security teams in all organizations should be able to apply **advanced filtering** and execute queries on **floating time windows**, using a **simple data query language**. Some participants mentioned that accessing **raw data** from multiple technologies in addition to pre-processed data would facilitate in-depth expert analysis. One response highlighted that the ability to perform **retro hunting** would be useful for analyzing past logs and validating correlation rules.

Regarding TIPs, SIEMs, and specific network-based and host-based detection technologies, the responses indicated that organizations do not expect particular tools but rather require assurance that a new platform can meet their **accuracy and response time** requirements. Security personnel also expressed the need for visual aids such as graphics and threat maps covering the threat actors and techniques outlined in the **MITRE ATT&CK** framework to complement the information.

5.4 Collaboration and Information Sharing

The participants indicated that the **Threat Intelligence Team** (TIT) and the **SOC** collaborate by following the specific sharing processes and workflows established by their organizations. However, these processes can be adjusted to integrate information from other organizations. The TIT shares threat briefings, incident triage and escalation, and threat campaign tracking with the SOC. Conversely, the SOC provides the TIT with threat intelligence feeds integration, SIEM integration, threat-hunting tools and techniques, and incident response playbooks.

The communication within an organization is currently assured via **MISP threat sharing** and **encrypted direct chats**. The participants prefer **notifications and emails** for low-severity security incidents, while **alarms and phone calls** are prioritized for crisis and urgent threats. Additionally, security teams must record and preserve **security incident artifacts** and **cyber forensics reports** and provide them to law enforcement agencies as needed. They also share these artifacts and reports with National CERTs through MISP, ticketing platforms, or direct communication in standard formats when necessary.

The security personnel (including - malware analysists) require direct communication with their colleagues, team members, directors, and executives. They would benefit from a streamlined and efficient collaboration with other incident response teams and SOCs from other organizations in the same sector of activity. Their responses expressed the expectation of sharing **TTPs and IoCs in near real-time** to enhance detection capabilities. Additionally, they prefer to receive **daily reports** on threat intelligence, security events, log data, system and endpoint information, access control details, and external threat feeds.

The directors, who are part of the Security Service Providers stakeholder group, require their internal security teams to share information and have **two-way communication** with National CERTs and private organizations. They prefer to receive **weekly progress reports** on SOC alerts, current cyber threats, security incident investigations, and red, and purple team activities.

Overall, a collaborative platform is expected to provide **24/7 availability** for information-sharing tools, fast and effective mechanisms for **incident response** and containment, and **technical and non-technical reports**. The integration of **AI and ML models** is expected to simplify incident response workflows, automate analysis tasks for security personnel, and provide easily understandable information and relevant alerts for further investigation.

5.5 Compatibility and Compliance

None of the participants expressed concerns about the compatibility of a collaborative platform with the systems used in their organizations. Therefore, they did not specify any required technologies or processes for integration purposes. Their primary expectations for a collaborative

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them

platform were **scalability**, **adaptability**, utilization of **standard data formats** in cybersecurity, and the ability to effectively **handle novel cyber threats** as their organization's cybersecurity needs evolve.

Regarding authentication and authorization, most participants indicated that their organizations utilize **multi-factor authentication** and **virtual private networks**, which are becoming standard security measures for organizations of all sizes. The access to data and its exchange between teams and systems is done through **role-based access** or **privileged access** management mechanisms. This allows for a clear distinction between technical users and other users with less in-depth expertise and lower security clearance.

In terms of compliance, all responses outline the importance of adhering to **GDPR** when utilizing sensitive data on a collaborative platform. Several responses also mention the **ISO 27001** international standard to improve information security management systems and the **NIST cybersecurity framework** with guidelines to manage and reduce cybersecurity risks. Additionally, some responses suggested that a new platform should provide **detailed and compliant documentation** for all application programming interfaces, query languages, and integration processes to ensure compliance and ease of use.

6 CYDERCO Requirements

This section describes the different requirements of CYDERCO Platform. Since the platform has different components, we present the requirements per component. Nevertheless, all the requirements should have the same fields namely:

- Requirement ID, a unique string to identify each requirement.
- Requirement Type, that indicates if the requirement is functional or non-functional.
- Requirement Title, a brief title of the requirement.
- Requirement Description, a short description of the requirement.
- Requirement Priority that indicates how important it is to satisfy a given requirement in the CYDERCO solution. This field is used to separate critical requirements from not-so-critical ones, and even the optional ones. We can differentiate between three priority levels, stated below according to decreasing criticality:
    - MUST – denotes high-priority requirements that are critical for the successful realization of CYDERCO project. These requirements cover key aspects of the Platform and its building blocks and must be implemented in the final solution at the end of the project.
    - SHOULD – denotes medium priority requirements that should ideally be implemented in the final solution but are not as critical for the success of the project as MUST requirements. Although failure to implement a SHOULD requirement would hinder the project, the impact would not be as severe as with MUST requirements.
    - COULD – denotes low-priority requirements that cover optional features that would be nice to have in the final solution, but do not affect the overall success of the project.
- Requirement Dependency, ID of other related requirements, if they exist.

The table below provides a template that was followed for the description of the different requirements.

Table 4. Requirement Structure

ID	**<unique string to identify each requirement>**
Type	indicates if the requirement is functional or non-functional
Title	a brief title of the requirement
Description	a short description of the requirement
Priority	indicates how important it is to satisfy a given requirement in the CYDERCO solution
Dependency	ID of other related requirements if they exist

6.1 Detection and Response Hub

6.1.1 Data Analytics

Table 5. Functional Requirement 1 – Data Analytics

ID	FUNC-DA-1
Type	Functional
Title	Data Correlation
Description	The Data Analytics module must be able to correlate data based on specific defined criteria.
Priority	Must
Dependency	N/A

Table 6. Functional Requirement 2 – Data Analytics

ID	FUNC-DA-2
Type	Functional
Title	Data Visualization
Description	The Data Analytics module must be able to provide at least 10 different methods to showcase data that may assist the SOC’s investigation.
Priority	Must
Dependency	N/A

Table 7. Functional Requirement 3 – Data Analytics

ID	FUNC-DA-3
Type	Functional
Title	Graphical User Interface
Description	The Data Analytics module must have an intuitive graphical user interface that will be used in the incident response process.
Priority	Must
Dependency	N/A

Table 8. Functional Requirement 4 – Data Analytics

ID	FUNC-DA-4
Type	Functional
Title	Alert Forwarding
Description	The Detection and Response Hub - Data Analytics component must be able to forward alerts to the Detection and Response Hub - AI-driven component.
Priority	Must
Dependency	N/A

Table 9. Functional Requirement 5 – Data Analytics

ID	FUNC-DA-5
Type	Functional
Title	Role-Based Access Control
Description	The Data Analytics module must be able to provide a multi-tier RBAC (Role-Based Access Control) system which enables a multi-tier SOC to perform investigations.
Priority	Must
Dependency	N/A

Table 10. Functional Requirement 6 – Data Analytics

ID	FUNC-DA-6
Type	Functional
Title	Technology support
Description	The Detection and Response Hub - Data Analytics module must support major data formats for ingestion, which may be used for SOC investigation purposes. The module will accommodate a minimum of 10 different IT vendors, cybersecurity technologies, or products that will be supported.
Priority	Must
Dependency	N/A

Table 11. Functional Requirement 7 – Data Analytics

ID	FUNC-DA-7
Type	Functional
Title	Threat Intelligence - Data Analytics - Sightings support
Description	The Detection and Response Hub – Data Analytics component needs to support data enrichment with threat intelligence from the Threat Intelligence Platform and/or other external sources.
Priority	Must
Dependency	N/A

Table 12. Functional Requirement 8 – Data Analytics

ID	FUNC-DA-8
Type	Functional
Title	Threat Intelligence – Data Analytics - Enrichment
Description	Data of interest processed by the Detection and Response Hub – Data Analytics component needs to be sent to the Threat Intelligence component for enrichment purposes.
Priority	Must
Dependency	N/A

Table 13. Non-Functional Requirement 1 – Data Analytics

ID	NFUNC-DA-1
Type	Non-Functional
Title	Data ingestion
Description	The Detection and Response Hub – Data Analytics component must have the capability to ingest and map data fields required for the incident response process.
Priority	Must
Dependency	N/A

Table 14. Non-Functional Requirement 2 – Data Analytics

ID	NFUNC-DA-2
Type	Non-Functional
Title	Scalability
Description	The Detection and Response Hub – Data Analytics component must have the scalability required from the data ingestion pipeline to the upper technology stacks needed to accommodate functional purposes.
Priority	Must
Dependency	N/A

Table 15. Non-Functional Requirement 3 – Data Analytics

ID	FUNC-DA-2
Type	Functional
Title	Human in the middle
Description	The SOC Analyst must determine the indicators of compromise during an investigation by leveraging the Detection and Response Hub – Data Analytics component.
Priority	Should
Dependency	N/A

6.1.2 Network Traffic Analysis (NTA)

Table 16. Functional Requirement 1 – Network Traffic Analysis

ID	FUNC-NTA-1
Type	Functional
Title	Traffic Monitoring
Description	The NTA module must be capable of monitoring network traffic.
Priority	Must
Dependency	N/A

Table 17. Functional Requirement 2 – Network Traffic Analysis

ID	FUNC-NTA-2
Type	Functional
Title	Anomaly Detection
Description	The NTA module must be able to detect abnormal network activities using, for example, IoC information.
Priority	Must
Dependency	N/A

Table 18. Functional Requirement 2 – Network Traffic Analysis

ID	FUNC-NTA-3
Type	Functional
Title	Alert Generation
Description	The NTA module must be able to generate alerts and provide detailed information about the event.
Priority	Must
Dependency	N/A

Table 19. Functional Requirement 3 – Network Traffic Analysis

ID	FUNC-NTA-4
Type	Functional
Title	Alerts - format
Description	The NTA module must be able to send the generated alerts to the Data Analytics module in supported formats such as Syslog, JSON, or others.
Priority	Must
Dependency	N/A

Table 20. Functional Requirement 4 – Network Traffic Analysis

ID	FUNC-NTA-5
Type	Functional
Title	Generate signature-based alerts based on Indicators of Compromise
Description	The NTA module must be able to generate alerts manually (leveraging human effort) or automatically based on indicators of compromise provided, for example, by the threat intelligence component.
Priority	Must
Dependency	N/A

Table 21. Non-Functional Requirement 1 – Network Traffic Analysis

ID	NFUNC-NTA-1
Type	Non-Functional
Title	Performance
Description	The NTA module should have minimal impact on network performance and latency, ensuring efficient and timely analysis of network traffic.
Priority	Should
Dependency	N/A

Table 22. Non-Functional Requirement 2 – Network Traffic Analysis

ID	NFUNC-NTA-2
Type	Non-Functional
Title	Accuracy
Description	The NTA module should demonstrate good accuracy in detecting anomalies.
Priority	Should
Dependency	N/A

Table 23. Non-Functional Requirement 3 – Network Traffic Analysis

ID	NFUNC-NTA-3
Type	Non-Functional
Title	Accuracy
Description	The NTA module should demonstrate a low false positive rate in detecting anomalies.
Priority	Should
Dependency	N/A

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

Table 24. Non-Functional Requirement 4 – Network Traffic Analysis

ID	NFUNC-NTA-4
Type	Non- Functional
Title	User Interface
Description	The NTA module could provide an intuitive interface for monitoring the network.
Priority	Could
Dependency	N/A

6.1.3 Host Intrusion Detection Service

Table 25. Functional Requirement 1 – Host Intrusion Detection Service

ID	FUNC-HIDS-1
Type	Functional
Title	Anomaly-based HID
Description	Provide Anomaly-based HIDS for detection of deviations (anomalies) from a baseline of host behavioral patterns.
Priority	Must
Dependency	N/A

Table 26. Functional Requirement 2 – Host Intrusion Detection Service

ID	FUNC-HIDS-2
Type	Functional
Title	Alert forwarding
Description	The HIDS module must forward alerts with sufficient information to the Detection and Response Hub.
Priority	Must
Dependency	N/A

Table 27. Functional Requirement 3 – Host Intrusion Detection Service

ID	FUNC-HIDS-3
Type	Functional
Title	AI-based anomaly detection
Description	The HIDS shall adopt a machine learning/deep learning algorithm suitable for learning high-dimensional behavioral features extracted from legitimate host activities.
Priority	Must
Dependency	N/A

Table 28. Functional Requirement 4 – Host Intrusion Detection Service

ID	FUNC-HIDS-4
Type	Functional
Title	Outgoing network activity modelling
Description	The HIDS shall detect anomalous behavioral patterns in outgoing network connections from a monitored host environment to external servers, devices, and domains.
Priority	Must
Dependency	N/A

Table 29. Functional Requirement 5 – Host Intrusion Detection Service

ID	FUNC-HIDS-5
Type	Functional
Title	Incoming network activity modelling
Description	The HIDS shall detect anomalous behavioral patterns in incoming network connections to a monitored host environment from external servers, devices, and domains.
Priority	Must
Dependency	N/A

Table 30. Functional Requirement 6 – Host Intrusion Detection Service

ID	FUNC-HIDS-6
Type	Functional
Title	Resource consumption
Description	The HIDS shall detect anomalous behavioral patterns in consumption of hardware resources in a monitored host environment. Define and extract suitable metrics of CPU utilization, RAM utilization, HDD utilization, and Network utilization.
Priority	Must
Dependency	N/A

Table 31. Functional Requirement 7 – Host Intrusion Detection Service

ID	FUNC-HIDS-7
Type	Functional
Title	Correlation of patterns
Description	The HIDS shall correlate network behavioral patterns with the host hardware utilization patterns through its ML/DL module for an extended detection of anomalies.
Priority	Must
Dependency	N/A

Table 32. Functional Requirement 8 – Host Intrusion Detection Service

ID	FUNC-HIDS-8
Type	Non-Functional
Title	OS Support
Description	The HIDS shall make use of open-source technologies and cross platform programming languages for supporting multiple OSs such as Linux, Windows, or Mac.
Priority	Must
Dependency	N/A

Table 33. Functional Requirement 9 – Host Intrusion Detection Service

ID	FUNC-HIDS-9
Type	Non-Functional
Title	Lightweight Operation
Description	The HIDS shall be designed to operate with minimum acceptable overhead in terms of hardware and resource consumption on a given host where it operates.
Priority	Must
Dependency	N/A

Table 34. Functional Requirement 10 – Host Intrusion Detection Service

ID	FUNC-HIDS-10
Type	Non-Functional
Title	Performance
Description	The HIDS shall sustain operations, without any packet drop or performance penalty, up to 1000 pps or up to 1 Mbps communications throughput for soft-real time anomaly detection.
Priority	Must
Dependency	N/A

Table 35. Functional Requirement 11 – Host Intrusion Detection Service

ID	FUNC-HIDS-11
Type	Non-Functional
Title	Detection Time
Description	The HIDS shall offer time to detection of less than 10 ms, or, in other words, at least 100 decision makings per second to address soft-real time anomaly detection. This time includes when behavioural features are given to the HIDS to time decision of anomaly/not anomaly is taken. This time excludes the generation of behavioral statistics from the host environment.
Priority	Must

Dependency	N/A

Table 36. Functional Requirement 12 – Host Intrusion Detection Service

ID	FUNC-HIDS-12
Type	Non-Functional
Title	Open-source Adoption
Description	The HIDS shall adopt off-the-shelf open-source modules for raw access and processing of host logs, such as for example GoAccess (https://goaccess.io), Drain3 (https://github.com/logpai/Drain3), or Graylog Open (https://graylog.org/products/source-available/) to extend the HIDS visibility and extract suitable metrics on top of the log structures to support anomaly detection.
Priority	Must
Dependency	N/A

Table 37. Functional Requirement 13 – Host Intrusion Detection Service

ID	FUNC-HIDS-13
Type	Functional
Title	Log Analysis
Description	The HIDS shall support log analysis of well-known application servers such as Apache and Nginx and in selected deployments such as Kubernetes clusters that represent a wide choice for provisioning of enterprise services and applications.
Priority	Must
Dependency	N/A

Table 38. Functional Requirement 14 – Host Intrusion Detection Service

ID	FUNC-HIDS-14
Type	Functional
Title	Extended correlation of patterns (including logs)
Description	The HIDS should support correlation of host network behavior, HW resource utilization, and log analysis for an extended and comprehensive detection of anomalies and intrusions.
Priority	Must
Dependency	N/A

Table 39. Functional Requirement 15 – Host Intrusion Detection Service

ID	FUNC-HIDS-15
Type	Non-Functional
Title	Windows Support
Description	The HIDS will first provide the core functionality for Windows and enable support in other OSs using cross-platform technologies and programming languages.
Priority	Should
Dependency	N/A

Table 40. Functional Requirement 16 – Host Intrusion Detection Service

ID	FUNC-HIDS-16
Type	Non-Functional
Title	Net info API
Description	The HIDS shall be given access permissions to host network interfaces for the monitoring of network connections and traffic to/from the host environment.
Priority	Must
Dependency	N/A

Table 41. Functional Requirement 17 – Host Intrusion Detection Service

ID	FUNC-HIDS-17
Type	Non-Functional
Title	Resources consumption API
Description	The HIDS shall be given access permissions to host HW resource utilization APIs or through intermediary application APIs.
Priority	Must
Dependency	N/A

Table 42. Functional Requirement 18 – Host Intrusion Detection Service

ID	FUNC-HIDS-18
Type	Functional
Title	Automation - simplicity of use
Description	The HIDS shall offer a high level of automation in terms of configuration and training on legitimate host activities with the minimum possible cybersecurity expertise required.
Priority	Must
Dependency	N/A

Table 43. Functional Requirement 19 – Host Intrusion Detection Service

ID	FUNC-HIDS-19
Type	Functional
Title	Detection Capabilities
Description	The HIDS shall be able to detect attacks from at least three of the following categories: (i) malware/rootkit/ransomware, (ii) botnet attacks, (iii) Malware C&C attacks, (iv) FDI, MitM, Unauthorized access, and (v) DoS/DDoS, TCP SYN, ICMP Ping, DNS Amplification. Note that metrics such as F1 score, accuracy, false positives, false negatives, etc., will be provided later as KPIs.
Priority	Must
Dependency	N/A

6.1.4 AI-driven Analytics

Table 44. Functional Requirement 1 – AI-driven Analytics

ID	FUNC-AI-1
Type	Functional
Title	Data Preprocessing
Description	The module should preprocess the data in Data Analytics database to prepare it for analysis by AI algorithms.
Priority	Should
Dependency	FUNC-DA-4

Table 45. Functional Requirement 2 – AI-driven Analytics

ID	FUNC-AI-2
Type	Functional
Title	Smart Correlation
Description	The module must perform intelligent correlation of data sent to the Data Analytics database identifying relationships and dependencies between security events.
Priority	Must
Dependency	N/A

Table 46. Non-Functional Requirement 1 – AI-driven Analytics

ID	NFUNC-AI-1
Type	Non- Functional
Title	Performance

Description	The module should have minimal impact on performance and latency, ensuring efficient and timely correlation of events.
Priority	Should
Dependency	N/A

Table 47. Non-Functional Requirement 2 – AI-driven Analytics

ID	**NFUNC-AI-2**
Type	Non- Functional
Title	Interpretability
Description	The module should provide interpretable results and insights to enable security analysts to understand and validate the findings.
Priority	Should
Dependency	N/A

6.2 Threat Intelligence Sharing and Collaboration

6.2.1 Threat Intelligence Collection and Storing

Table 48. Functional Requirement 1 – Threat Intelligence Collection and Storing

ID	**FUNC-TICS-1**
Type	Functional
Title	Ingestion support for 3rd party threat intelligence feeds
Description	The component shall support ingestion of 3rd party threat intelligence feeds such as OSINT leveraging standard, widely accepted formats and protocols such as TAXII/STIX, HTTP(S)/CSV with the capability to create custom parsers for ingested data.
Priority	Must
Dependency	N/A

Table 49. Functional Requirement 2 – Threat Intelligence Collection and Storing

ID	**FUNC-TICS-2**
Type	Functional
Title	Add/Remove/Edit events
Description	The events within the component need to support the capability to add/remove/edit individual fields to entries to accommodate the threat intelligence generation process and its evolving landscape.
Priority	Must
Dependency	N/A

Table 50. Functional Requirement 3 – Threat Intelligence Collection and Storing

ID	FUNC-TICS-3
Type	Functional
Title	Threat Intelligence ingestion from the Detection and Response hub
Description	The component shall provide the means to ingest threat intelligence from the Detection and Response hub such as indicators of compromise for investigated alerts or incidents.
Priority	Must
Dependency	N/A

Table 51. Functional Requirement 4 – Threat Intelligence Collection and Storing

ID	FUNC-TICS-4
Type	Functional
Title	Dataset
Description	The dataset shall accommodate all pertinent information necessary for most indicators of compromise which need to be stored.
Priority	Must
Dependency	N/A

Table 52. Functional Requirement 5 – Threat Intelligence Collection and Storing

ID	FUNC-TICS-5
Type	Functional
Title	Threat Intelligence sources
Description	The component shall support ingestion of 10 or more different CTI tools and methods collecting technical, tactical, operational, and strategic intelligence sources.
Priority	Must
Dependency	N/A

6.2.2 Threat Intelligence Sharing

Table 53. Functional Requirement 1 – Threat Intelligence Sharing

ID	FUNC-TIS-1
Type	Functional
Title	Field Encryption
Description	The Threat Intelligence Sharing component must encrypt field values which would otherwise discourage threat intelligence sharing.
Priority	Must

Dependency	N/A

Table 54. Functional Requirement 2 – Threat Intelligence Sharing

ID	**FUNC-TIS-2**
Type	Functional
Title	Field Anonymization
Description	The Threat Intelligence Sharing component must anonymize field values which would otherwise discourage threat intelligence sharing.
Priority	Must
Dependency	N/A

Table 55. Functional Requirement 3 – Threat Intelligence Sharing

ID	**FUNC-TIS-3**
Type	Functional
Title	Anonymous reporting
Description	The Threat Intelligence Sharing component should be able to hide/mask the sender of the IoC to enable anonymous sharing.
Priority	Optional
Dependency	N/A

Table 56. Functional Requirement 4 – Threat Intelligence Sharing

ID	**FUNC-TIS-4**
Type	Functional
Title	Threat Intelligence Sharing - NTA
Description	The component will be able to store IoCs which may be used to create rules within NTA.
Priority	Should
Dependency	N/A

Table 57. Functional Requirement 5 – Threat Intelligence Sharing

ID	**FUNC-TIS-5**
Type	Functional
Title	Threat Intelligence Sharing - HIDS
Description	The component shall provide threat intelligence to the Host Intrusion Detection Service (HIDS) component in HIDS-supported formats.
Priority	Should
Dependency	N/A

Table 58. Functional Requirement 6 – Threat Intelligence Sharing

ID	FUNC-TIS-6
Type	Functional
Title	Threat Intelligence Sharing – Course of Actions
Description	The Threat Intelligence Sharing component must support the exchange of information regarding the Course of Actions in a standardized way (such as MISP and STIX formats). This facilitates the ingestion or consumption of information by other security controls for detection or blocking purposes.
Priority	Must
Dependency	N/A

Table 59. Functional Requirement 7 – Threat Intelligence Sharing

ID	FUNC-TIS-7
Type	Functional
Title	Playbook sharing
Description	The Threat Intelligence Sharing component should integrate extensions to enable playbook sharing and management via MISP & STIX 2.1.
Priority	Should
Dependency	N/A

Table 60. Functional Requirement 8 – Threat Intelligence Sharing

ID	FUNC-TIS-8
Type	Functional
Title	Manual export format
Description	Threat intelligence shall be exported in industry-standard, widely supported formats such as STIX, JSON, MISP, CSV.
Priority	Must
Dependency	N/A

Table 61. Functional Requirement 9 – Threat Intelligence Sharing

ID	FUNC-TIS-9
Type	Functional
Title	Information synchronization
Description	The component shall support synchronization of threat intelligence between different instances.
Priority	Must
Dependency	N/A

Table 62. Functional Requirement 10 – Threat Intelligence Sharing

ID	FUNC-TIS-10
Type	Functional
Title	Generate reports
Description	The component shall support the generation of reports in formats such as PDF, based on a predefined dashboard.
Priority	Should
Dependency	N/A

6.2.3 Threat Intelligence Enrichment and Contextualization

Table 63. Functional Requirement 1 – Threat Intelligence Enrichment and Contextualization

ID	FUNC-TIEC-1
Type	Functional
Title	Dashboards and visualizations
Description	The component shall provide visualizations such as graphs by pivoting on the data stored. The visualizations need to pivot based on fields such as threat actor, IP, malware, domain name and to showcase relationships between them.
Priority	Must
Dependency	N/A

Table 64. Functional Requirement 2 – Threat Intelligence Enrichment and Contextualization

ID	FUNC-TIEC-2
Type	Functional
Title	Assets information retrieval
Description	The component shall be able to retrieve asset information to contextualize & consider relevance of CTI.
Priority	Must
Dependency	N/A

Table 65. Functional Requirement 3 – Threat Intelligence Enrichment and Contextualization

ID	FUNC-TIEC-3
Type	Functional
Title	AI-Driven Enrichment

Description	The component should leverage AI/ML algorithms to perform enrichment.
Priority	Could
Dependency	N/A

Table 66. Functional Requirement 4 – Threat Intelligence Enrichment and Contextualization

ID	FUNC-TIEC-4
Type	Functional
Title	Relevance Scoring
Description	The component should be able to score the relevance of the shared objects according to a given asset type and software/hardware components.
Priority	Should
Dependency	N/A

Table 67. Functional Requirement 5 – Threat Intelligence Enrichment and Contextualization

ID	FUNC-TIEC-5
Type	Functional
Title	Confidence Level
Description	The component shall support a mechanism stating the confidence level of stored indicators.
Priority	Must
Dependency	N/A

Table 68. Functional Requirement 6 – Threat Intelligence Enrichment and Contextualization

ID	FUNC-TIEC-6
Type	Functional
Title	MITRE support
Description	The component shall accommodate a method that supports MITRE ATT&CK TTPs.
Priority	Must
Dependency	N/A

6.2.4 Sighting Support

Table 69. Functional Requirement 1 – Sightings Support

ID	FUNC-SS-1
Type	Functional
Title	Threat Intelligence sightings
Description	When an indicator is seen within the organization on which the Detection and Response Hub – Data Analytics supports, the threat intelligence component shall increase the sightings level and/or confidence level.
Priority	Must
Dependency	N/A

Table 70. Functional Requirement 2 – Sightings Support

ID	FUNC-SS-2
Type	Functional
Title	Threat Intelligence sightings
Description	When an indicator is propagated from an instance of the threat intelligence platform, the sightings and/or confidence level shall be increased.
Priority	Should
Dependency	N/A