Artificial Intelligence Threat Reporting and Incident Response System

D2.2 – User and Technical Requirements Specification

Project Title:	Artificial Intelligence Threat Reporting and Incident Response System
Project Acronym:	IRIS
Deliverable Identifier:	D2.2
Deliverable Due Date:	28/2/2022
Deliverable Submission Date:	28/2/2022
Deliverable Version:	V1.3
Main author(s) and Organisation:	Andrew Roberts (TALTECH)
Work Package:	WP2 – System Co-Design
Task:	Task 2.2 – User and Technical Requirements Specification
Dissemination Level:	PU: Public

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it

Quality Control

	Name	Organisation	Date
Editor	Andrew Roberts	TalTech	28/02/2022
Peer Review 1	Txema Lecea	CISCO	25/02/2022
Peer Review 2	Nikita Akmaikin	FVH	25/02/2022
Submitted by (Project Coordinator)	Nelson Escravana	INOV	28/02/2022
Resubmitted by (Project Coordinator)	Gonçalo Cadete	INOV	30/06/2023

Contributors

Organisation
Gustavo Gonzalez-Granadillo (ATOS)
Rodrigo Rodriguez Diaz (ATOS)
Susana Gonzalez Zarzosa (ATOS)
Sofia Tsekeridou (INTRA)
Roland Kromes (TUD)
João Rodrigues (INOV)
Jose Lecea (CISCO)
Bruno Vidalenc (THALES), Filippo Rebecchi (THALES)
Ryan Heartfield, Nathan Hue (CLS)
Theodora Tsikrika, Stefanos Vrochidis (CERTH)
Marius Preda (DNSC)
Sofia Tsekeridou, Dimitris Skias (INTRA)
René Serral (UPC)
Gonçalo Cadete (INOV)
Sébastien Bardin (CEA)
Vasiliki-Georgia (Giovana) Bilali, Dimitrios Skias (ICCS)
Elisavet Grigoriou (SID)
Eleni Darra (CERTH)

Document History

Version	Date	Modification	Partner
V0.1	30/09/2021	Creation of Initial Document	TALTECH
V0.2	05/10/2021	Updated with Technical Requirement Elicitation Methodology	ATOS
V0.3	10/01/2022	Updated with Partners' feedback for requirements and KPIs	TALTECH
V0.4	20/01/2022	Updated with SOTA	TALTECH
V0.5	01/02/2022	Update with End-User PUC feedback	TALTECH
V0.6	10/02/2022	Updated with CERT feedback	TALTECH
V0.7	18/02/2022	Updated with CERT feedback	TALTECH
V0.8	20/02/2022	Updated with feedback from 1st Draft Review	TALTECH
V1.0	28/02/2022	Final version	TALTECH, INOV
V1.1	22/06/2023	Update with feedback from PO	TALTECH
V1.2	27/06/2023	Update with feedback from CitySCAPE	TALTECH
V1.3	30/06/2023	Update from Review by ATOS	TALTECH, ATOS

Legal Disclaimer

Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

Abbreviation/ Acronym	Meaning
AI	Artificial Intelligence
API	Application Programmable Interface
ATA	Autonomous Threat Analytics
AV	Autonomous Vehicle
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CTI	Collaborative Threat Intelligence
DDoS	Distributed Denial-of-Service
DPA	Data Protection and Accountability
GDPR	EU General Data Protection Regulation
IDS	Intrusion Detection System
IoC	Indicator of Compromise
IoT	Internet of Things
IPS	Intrusion Prevention System
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
MeliCERTes	Cybersecurity platform developed as part of EU Strategy for Cybersecurity
MISP	Malware Information Sharing Platform
ML	Machine Learning
OWM	Orchestration Workflow Manager
PUC	Pilot Use-Case
RSU	Road Sign Unit
STIX	Structured Threat Information Expression
TAO	Advanced Threat Intelligence and Analytics Orchestration
TAXII	Trusted Automated Exchange of Intelligence Information
TTPs	Tactics, Techniques, Procedures
VPN	Virtual Private Network
XSS	Cross Site Scripting

Executive Summary

This document reports on the user and technical requirements that the IRIS platform will have to satisfy. It is linked to task T2.2 and elicits a range of important requirements for the design of the IRIS platform. These include:

- End-User Requirements;
- IRIS Platform Functional and Technical Requirements;
- KPIs;
- State-of-the-Art of key technical integration areas;
- Initial threat portfolio of the three smart city PUCs.

In the End-User requirement elicitation process, it became clear that the primary requirements for the MeliCERTes enhancements developed in the IRIS project, that were common to all participants in the IRIS CERT advisory group, were:

- Modular design;
- Enable extensibility in design of tools;
- Open APIs that allow seamless platform integration.

PUC End-Users expressed the importance for the IRIS platform to be design with the following in mind:

- Facilitate seamless deployment of the IRIS platform in the PUC End-User environment;
- Support existing technical standards (MISP, STIX/TAXII etc.) and processes (RFC formats for incident response reports etc.);
- Usability features to enable technical users to configure and use the IRIS platform.

The process of elicitation End-User requirements also extracted a few important considerations for the design of the IRIS platform. Predominantly, the MeliCERTes ecosystem has been upgraded from version1 to version2. Furthermore, the request to engage with the MeliCERTes development community during the project.

The IRIS Platform Functional and Technical Requirements and associated KPIs are presented in this report. During the requirements elicitation and KPI definition process it became clear that these will need to be updated iteratively during the lifespan of the project as the dependencies and interactions between each of the tools and modules are still being explored. The State-of-the-Art and Initial Threat Portfolio, also, presented information useful for the IRIS platform design.

1 INTRODUCTION

1.1 Project Introduction

As existing and emerging smart cities continue to expand their IoT and AI-enabled platforms, this introduces novel and complex dimensions to the threat intelligence landscape linked with identifying, responding, and sharing data related to attack vectors, based on emerging IoT and AI technologies.

IRIS's vision is to integrate and demonstrate a single platform addressed to CERTs/CSIRTs for assessing, detecting, responding to and sharing information regarding threats & vulnerabilities of IoT and AI-driven ICT systems. To achieve this, IRIS brings together experts in cybersecurity, IoT, AI, automated threat detection, response, and recovery.

IRIS aims to help European CERTs/CSIRTs minimize the impact of cybersecurity and privacy risks as well as threats introduced by cyber-physical vulnerabilities in IoT platforms and adversarial attacks on AI-provisions and their learning/decision-making algorithms.

The IRIS platform will be demonstrated and validated on three highly realistic environments with the engagement of 3 smart cities (in Helsinki, Tallinn, and Barcelona) along with the involvement of national CERTs/CSIRTs, and cybersecurity authorities.

The project duration extends from September 2021 to August 2024.

1.2 Deliverable Purpose

This report is linked to task T2.2 "User and technical requirements specification". This task involved analysing the end-user, technical and business requirements that will drive the design and development of a proof-of-concept IoT and AI threat reporting and incident response system for CERTs/CSIRTs. Furthermore, this deliverable analysed the cybersecurity threats targeting IoT and AI driven ICT infrastructures, systems, and applications and the requirements of each end-user. These include both the functional aspects of the core system and interfaces and the non-functional requirements, covering:

(a) security requirements.

(b) requirements for personal data protection and GDPR compliance, including decisions on what data will be anonymized, what policies will be enforced on them, and how the user will access data necessary for decision making.

All partners of the consortium have coordinated to specify these requirements.

The objectives of this deliverable have been met, it must also be noted that the specification of IRIS requirements and KPIs is an agile process, to be conducted along iterative, incremental, and adaptive cycles, according to software development best practice [29]. The up-to-date artifacts are made available in the official IRIS repository.

1.3 Relation to other Tasks and Deliverables

This task collects the requirements of the different IRIS stakeholders (e.g., CERTs/CSIRTs, cybersecurity professionals, cybersecurity services providers) obtained through standard techniques (e.g., questionnaires). The list of these requirements regarding the IRIS platform functionalities will be used to validate the IRIS platform in work package WP6. Then, KPIs will be devised (based on these requirements) to create a set of measurable goals for the IRIS platform validation.

This task will observe the recommendations of Task 1.5 (Ethical, Legal, Privacy Monitoring and Regulatory Compliance).

This task will also define the technical requirements of the solution provided by the IRIS platform, building upon the user requirements identified through Task 2.1 (Use-Cases and Application Scenarios Definition). Key technological areas will be identified, and their state-of-the-art will be studied to establish their potential for integration at the IRIS platform.

Additionally, an initial threat portfolio will be established to build the basis for the development of the ATA module to be developed within Task 3.2 (Autonomous Threat Analytics). The output of this task will be used in Task 2.5 (Overall System Design and Functional Architecture) to define the IRIS system design and functional architecture.

KPIs will be redefined in the scope of task T7.1 "Pilot plans and methodology" and reported in deliverable D7.1.

1.4 Document Organisation

This document is organized as follows:

Section 2 presents the methodology used in the requirements elicitation process

Section 3 details information of the initial use-case analysis, including an identification of IRIS stakeholders.

Section 4 presents the IRIS End-User requirements.

Section 5 presents the IRIS Platform End-User requirements, grouped into functional and technical requirements.

Section 6 presents the Key Performance Indicators for the IRIS platform architecture.

Section 7 details the state-of-the-art for key technical integration areas; Threat Analytics, Collaborative Threat Intelligence, Threat Intelligence Orchestration, Data Protection Accountability and Auditability, and Cyber Ranges.

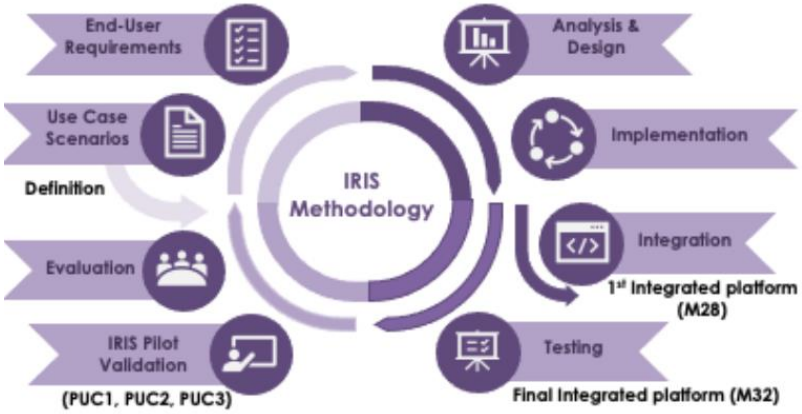
Section 8 provides an initial threat portfolio of each of the IRIS pilot use-cases for consideration of autonomous threat analysis and detection.

Section 9 concludes the document.

2 METHODOLOGY

The IRIS methodology is characterized by the following principles: (i) coverage of both research and innovation activities, based on distinct, yet interrelated activities for specifying and producing the IRIS platform and validating it in the scope of the IRIS pilots; (ii) an **ethics-driven and user-centric approach** based on the identification of ethics and legal foundations to be considered and active engagement of all stakeholders throughout the project's development, deployment and pilot processes ensuring the collaborative nature of the IRIS approach; (iii) an **iterative and phased development approach**, which is reflected in both the system and pilots' development methodology; and (iv) an **agile market-oriented approach** suitable for reaching the target TRL levels, which emphasizes continuous integration of requirements and feedback from stakeholders. Figure 1 depicts the overall IRIS methodology.

Figure 1 – Overall IRIS Methodology



Requirement definition is a fundamental part of the IRIS methodology. Requirements definition determines the building blocks for which the IRIS platform will be built.

2.1 Requirements Definition Methodology

The requirements definition process adopted an iterative methodology. The methodology followed the following phases:

Phase 1: Initial Use Case and Stakeholder analysis

- **Use-case analysis** was conducted, summarizing all the information already available in relation to the specific scenario/use case of each of the IRIS Pilot-Use-Cases (PUC). This analysis started from the revision of

the IRIS platform architecture in the project proposal and takes advantage of the output coming from the use-case and vision analysis in WP2, Task2.1 (delivered M4).

- **Stakeholder Analysis** was conducted to describe the "who" of the project and this "who" is identified by the stakeholders who will be impacted by the system.

Output: The output of this phase is an understanding of the types of stakeholders impacted by IRIS and components of the IRIS platform.

Phase 2: Definition of IRIS Requirements

- **Definition of End-User Requirements**, exploiting the outcomes of the previous step via analysis, the stakeholder target groups for requirements elicitation are selected. Standard investigative methods and techniques are developed and executed to elicit the End-User requirements for the IRIS Platform:

  - ***Surveying***, consists of proposing a set of questions to stakeholders to quantify their opinions, then to analyse data to identify the area of interest of stakeholders.

  - ***Interviews***, consisting of structured interviews with IRIS stake holder control groups.

  - ***Brainstorming***, to understand, from the perspective of the user, how they will interact with the system and what requirements are key for the design of the system.

Output: The output of this activity is IRIS End-User functional and technical requirements.

- **Definition of IRIS Platform Functional and Technical Requirements**

The IRIS platform functional and technical requirements were defined through the following steps:

1. Extraction of functional and technical requirements from analysis of the IRIS platform contained in the proposal and D2.1 – Use-Cases and vision analysis.
2. Tool owners validate extracted requirements and provide additional functional and technical requirements.

3. Revision of technical and functional requirements based on the outcomes of the end-user requirements.
4. Multiple iterative revision of the technical and functional requirements by tool owners to ensure that

Output: The output of this activity is the IRIS platform functional and technical requirements.

Phase 3: Normalization and Prioritization of IRIS Requirements
Requirements have been formatted using the following structure:

- **ID** is a *required* field that uniquely identifies a requirement. It allows establishing links from other related requirements. For visual distinction between requirements of different types, ID is composed of two parts separated by a dash ("-"): the first part represents a string label common to all requirements of a given type (an acronym of the type), while the second part represents a number. Note that numbers are unique within requirements of the same type. *Examples*: FUNC-30, T_PLAT-12.
- **Parent** is an *optional* field. If present, its value is the ID of requirement that is a given requirement's logical parent. This allows us to build hierarchical view of requirements. The parent-child relationship denoted with this field typically links a high-level requirement to a (set of) more detailed requirement(s).
- **Dependency** is an *optional* field. If present, it contains ID of requirement that is logically related to a given requirement but not in a way that fits a traditional parent-child relationship. Note that dependency is recorded only on the dependent requirement, e.g. on the source, and not on the target.

Regarding the type, it's a *required* field that represents the type of requirement. We can differentiate between two basic types of requirements: *functional* and *technical*:

- **Functional** requirements (identified by "FUNC" prefix) concern (core or supporting) functionality of the IRIS platform and its building blocks. They address *what* the platform or its constituents should do.
- **Technical** requirements (identified by "T-" prefix) are related to the technical aspects of the IRIS Platform and its building blocks. For clarity, we broke them down into four subtypes:
    - *Platform* requirements (identified by "T-PLAT" prefix) are associated with the design and implementation aspects covering *how* the platform or its building blocks should work to cover the envisioned functionality. Typically, platform requirements outline how building blocks are connected.

- *Security* requirements (identified by "T-SECU" prefix) deal with security aspects of the platform, for instance the implementation of security mechanisms supporting confidentiality, integrity, and availability.
- *Usability* requirements (identified by "T-USAB" prefix) are related to the practicality of developed software, ease of use, user-friendliness, responsiveness, and user experience in general.
- *Performance* requirements (identified by "T-PERF" prefix) give constraints on latencies, availability and resource usage or handling.

Priority is a *required* field that indicates how important it is to satisfy a given requirement in the IRIS solution relative to the given time frame. In our case the time frame spans the duration of the project. 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 successful realization of IRIS 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 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

Phase 4: IRIS Platform Validation Key Performance Indicators (KPIs)

Tool owners defined KPIs based on the understanding of the IRIS platform and End-Users expectations detailed in the requirements definition phase. The KPIs represent an initial contribution and will be updated throughout the project, including in activities such as Task 2.5 (Overall System Design and Functional Architecture), and Task 7.2 (Pilot plans and methodology).

Phase 5: Research to inform the development of IRIS Modules

- **State-of-the-Art Analysis**

State-of-the-Art analysis has been conducted on key technical integration areas which were identified in the initial use-case analysis. The State-of-the-Art provides the research foundations that will assist with the design and

development of the enhancements for the MeliCERTes ecosystem delivered in the IRIS project.

- **Initial Threat Portfolio for Autonomous Analytics and Detection**

An initial threat portfolio was developed for each of the PUC Smart Cities; Barcelona, Tallinn, and Helsinki. The initial threat portfolio details cyber threat scenarios identified by the PUC owners as being relevant for the design of the ATA module.

2.2 Traceability

The deliverable D2.6 – IRIS Reference Architecture and Platform Design, will provide a table which reflects how the IRIS architecture and platform design have mapped to the End-User and Platform requirements. From this, it will be possible to assess the traceability of the requirements to the design of the architecture and IRIS platform. This will confirm which functional and platform requirements have been included in the IRIS platform. Furthermore, the WP3 and WP4 will produce deliverables which demonstrate the development of the prototype modules covering the functional requirements identified. WP5 will provide detailed information about the Virtual Cyber Range and training environments. Practical demonstration, that the system operates according to the requirements, will be evaluated in WP7 – Pilot Use Cases and reported in the corresponding deliverable D7.5 (IRIS pilot evaluation report).

3 INITIAL USE-CASE ANALYSIS

3.1 Use-Case and IRIS Platform Analysis

To extrapolate requirements of the IRIS Platform it is important to deconstruct the constituent components which make up the IRIS Platform. This is due wide array of tools being developed in the IRIS project and the considerable complexity of integrating these tools in a common platform. The IRIS framework, displayed in Figure 1, provides a good option for segmenting functional and technical requirements. Requirements will be grouped based on the modules:

- Automated Threat Analytics and Detection
- Collaborative Threat Intelligence and Orchestration
- Data Protection, Accountability and Auditing
- Hands-on, Collaborative and Immersive Cybersecurity Training

Figure 2. The IRIS Concept and its technological innovations

3.2 IRIS Stakeholder Identification

IRIS End-Users were identified based on analysis of the proposal and IRIS D2.1. The proposal specifically highlights partners that fulfill the role of End-Users in the IRIS project. Furthermore, the predominance of CERTs/CSIRTs as End-Users is also highlighted in both the proposal and D2.1. Therefore, those that are impacted as End-Users of the IRIS project consist of:

- PUC End-Users
- CERTs/CSIRTs
- Cybersecurity providers

4 IRIS END-USER REQUIREMENTS

The End-User requirements section describes the following:

- Functional aspects of the core system and interfaces.
- Non-functional requirements: a) security requirements, b) privacy requirements (GDPR compliance, anonymisation of data, policy enforcement, user access policy)

The End-User Stakeholders were grouped into two control groups and differing methods of requirement elicitation were applied.

4.1 IRIS End-User Requirements

To illicit feedback from end-users to build requirements for the IRIS platform, 2 stakeholder control groups were created.

Group 1 stakeholders consisted of End-Users of the IRIS platform as identified in the IRIS grant agreement (depicted in Table 1).

Group 1 – End Users	
Organisation	**Role**
DNSC	**End-User**
UPC	**End-User, PUC 1**
IMI-BCN	**End-User, PUC 1**
CISCO	**End User, PUC1 Infrastructure Provider**
TalTech	**End-User, PUC 2**
Forum Virium Helsinki	**End-User PUC 3**

Table 1 IRIS End-User Stakeholder Group 1

The complete feedback from the IRIS Stakeholder Group 1 can be found using this link: https://partners.inov.pt/iris-h2020/index.php/f/10921 and in Appendix A.

Group 2 stakeholders consisted of EU CERTs/CSIRTs. Two structured interviews were held with the IRIS CERT Advisory Group on the 2nd of February 2022 and the 11th of February. The CERTs participated were asked to provide their opinions on each of the modules of the IRIS platform and their requirements. The complete feedback from the IRIS Stakeholder Group 1 can be found using this link: https://partners.inov.pt/iris-h2020/index.php/f/10921 and in Appendix B.

4.1.1 End-User Functional Requirements

ID	FUNC-End_User-01	Priority	SHOULD
Name	*IRIS Platform Availability*		
Description	The IRIS Platform should be available 24/7.		
Rationale	End-Users have indicated the importance of the IRIS Platform and tools having the capability to support 24/7 monitoring of AI and IoT Systems.		
Traceability	Assessed by End-Users during the PUCs (WP7).		

ID	FUNC-End_User-02	Priority	SHOULD
Name	*IRIS Platform Architecture*		
Description	The IRIS platform should be constructed of a modular design, allowing tools integrated within MeliCERTes platform to be also used as a stand-alone.		
Rationale	The CERT stakeholder group indicated that this was one of the most important design considerations. Modularity will allow CERTs to choose which tools in the MeliCERTes ecosystem they use. Tools developed for the MeliCERTes ecosystem should be interoperable with other tools and enable extensibility.		
Traceability	End-Users will assess the functionality of tools both as stand-alone and as integrated with MeliCERTes (WP7).		

ID	FUNC-End_User-03	Priority	MUST
Name	*IRIS User Access*		
Description	The IRIS platform will enable access to multiple simultaneous users.		
Rationale	This is important for End-Users as multiple CERT operators will access the platform simultaneously. Also, PUC End-Users expect the platform to be able to be accessed by multiple simultaneous users.		
Traceability	End-Users will assess this functionality in WP7 PUCs.		

ID	FUNC-End_User-04	Priority	MUST
Name	*ATA – Cyber Threat Detection and Analysis – Attack Types*		
Description	The IRIS platform detection and analysis will extend to the following cyber-attacks: ○ Attacks on availability of AI and IoT systems (DDoS Attacks etc.) ○ Attacks on integrity of AI and IoT Systems (AI and ML Evasion, data manipulation etc.) ○ Attacks on confidentiality of AI and IoT Systems (Data interception)		
Rationale	This is an essential requirement of the IRIS project description of action and an expectation of the PUC End-Users. Furthermore, the CERTS/CSIRTS expressed the need for detection of different types of attacks.		
Traceability	This will be assessed in PUCs (WP7) and an evaluation provided in D7.5 – IRIS Pilot Evaluation Report.		

ID	FUNC-End_User-05	Priority	SHOULD
Name	*ATA – Expected Response Time*		
Description	The IRIS platform should provide threat analysis within a range of 5 minutes to 1 hour after an incident alert.		
Rationale	This range was provided by the End-User stakeholder groups as appropriate to enable efficient Cyber Incident Response.		
Traceability	This will be assessed by End-Users during the PUCs (WP7).		

ID	FUNC-End_User-06	Priority	SHOULD
Name	*IRIS Platform – Reporting*		
Description	The IRIS Platform should be capable of reporting results in an automated format as well as allowing the End-User to customize the format of reports.		
Rationale	This is a requirement of both End-User stakeholder groups as well as the requirement of the IRIS project description of action.		
Traceability	This will be assessed by End-Users during the PUCs (WP7).		

ID	FUNC-End_User-07	Priority	COULD
Name	*ATA – Intrusion Detection Features*		
Description	IRIS Platform intrusion detection could include the following capability: ○ Agentless setup (as an option) ○ Support heterogeneity of devices type and communication protocols ○ Support Resource limitations of IoT devices such as CPU, memory, and energy ○ ML-based detection: Feature extraction and datasets		
Rationale	Requested by PUC End-Users for the deployment of IRIS as part of the PUC.		
Traceability	These features are part of the ATA Threat Detection Components (Task 3.2). The performance of the listed capability will be followed in D3.2 and later in D7.5 with the evaluation.		

ID	FUNC-End_User-08	Priority	SHOULD
Name	*IRIS Platform – Self-Recovery Time*		
Description	IRIS platform should provide timely automated response and recovery results within a range of near real-time (minimal delay in terms of seconds) to a few minutes.		
Rationale	Requirement defined by both stakeholder groups. Response time is not defined in the IRIS description of action and both stakeholder groups had differing opinions.		
Traceability	This will be assessed in PUCs (WP7) and the evaluation provided in D7.5– IRIS Pilot Evaluation Report.		

ID	FUNC-End_User-09	Priority	MUST
Name	*Intelligence Orchestration*		
Description	The user of the intelligence orchestrator module will have the capability to intervene manually to the system and change the proposed response.		

Rationale	This functional requirement is described in the description of action. Both stakeholder groups expressed the importance of the "human-in-the-loop" to provide a final decision before response configurations recommended by automated response are applied. This was deemed particularly important in order to secure their trust in the system, as the ones being the sole responsible for taking the final decisions on which response actions will be applied from the ones that the system will recommend, especially when critical assets or sub-nets of the critical infrastructure are affected, since this entails legal responsibilities for the affected stakeholders. A Decision Support System supports rather than automatically makes decisions, especially when these concern critical decisions relating to accountability and impact.
Traceability	This requirement will be tracked in D4.4 – IRIS Advanced Threat Intelligence Orchestrator and D7.5 – IRIS Pilot Evaluation Report.

ID	**FUNC-End_User-10**	**Priority**	**MUST**
Name	*Standardised Ontologies/Taxonomies*		
Description	The IRIS Platform will contain a standardized taxonomy/ontology which is mapped to widely used, existing ENISA and/or NIST taxonomies/ontologies (STIX 2.1, MISP Standards etc.).		
Rationale	This functional requirement is described in the description of action. Both stakeholder groups expressed the importance of this requirement.		
Traceability	. The details of the standardized ontologies/taxonomies finally supported by IRIS Platform will be reported in D4.1 Dynamic Repositories of Threats and Vulnerabilities.		

ID	**FUNC-End_User-11**	**Priority**	**SHOULD**
Name	*Enhanced MeliCERTes Ecosystem*		
Description	The IRIS platform will enhance the existing MeliCERTes ecosystem for CTI, threat sharing and monitoring of services. These extensions should provide open APIs that are shared with CERTs/CSIRTs and third parties.		
Rationale	CERTs want the ability to seamlessly integrate different tools in the		

	MeliCERTes ecosystem.
Traceability	This requirement will be evaluated in the PUCs (WP7) where it can be verified the availability of the open APIs offered by the extensions.

ID	**FUNC-End_User-12**	**Priority**	**MUST**
Name	*Data Protection and Auditability*		
Description	The IRIS platform will be GDPR compliant and use existing privacy enhancing features of the MeliCERTes ecosystem such as the trust circles feature.		
Rationale	This functional requirement is described in the IRIS project description of action and is considered essential by the End-User stakeholders. Also, CERTs have expressed the importance of GDPR in their work, as well as existing functionality to protect privacy.		
Traceability	This requirement will be traced throughout the iterative phases of this project. Including in D2.6, to ensure that the system is designed to adhere to GDPR, based on the outputs of D2.3, where ethics and data protection requirements will be analysed.		

ID	**FUNC-End_User-13**	**Priority**	**MUST**
Name	*CTI – Information Classification*		
Description	IRIS platform should provide real-time communication and collaborative information sharing, that will enable the ability to classify information using methods such as the traffic light protocol (TLP).		
Rationale	CERTs indicated the sharing of threat information in the CTI modules as the most important capability in the MeliCERTes platform and required TLP to classify CTI data.		
Traceability	This functionality will be assessed in Task 4.2 where the classification information methodology will also be reported and further during the PUCs (WP7).		

ID	**FUNC- End_User-14**	**Priority**	**SHOULD**
Name	*Cyber Range Training Scenarios*		
Description	Cyber range training scenarios should be realistic and include red and blue teaming type simulations.		
Rationale	CERTs requested that the cyber range simulations should consider inclusion of red teaming scenarios.		

Traceability	Training scenarios will be defined in WP5, specifically deliverables D5.1 and D5.2. The functionality of the VCR will be evaluated during the PUCs (WP7) and the results, reported on, in the numerous WP7 deliverables.

ID	**FUNC- End_User-15**	**Priority**	**COULD**
Name	*Cyber Range Training Audience*		
Description	The cyber range scenarios could enable diverse training types such as: collaborative exercises and individual, role-based training.		
Rationale	CERTs expressed an interest in the cyber range training being able to service multiple CERT operator roles.		
Traceability	Training scenarios will be defined in WP5, specifically deliverables D5.1 and D5.2. The functionality of the VCR will be evaluated during the PUCs (WP7) and the results, reported on, in the numerous WP7 deliverables.		

4.1.2 End-User Non-Functional Requirements

ID	T-PLAT-END_USER-01	Priority	MUST
Name	*IRIS Platform - Deployment*		
Description	IRIS components will be able to be accessed locally, and in an off-premises/hosted/cloud environment.		
Rationale	This is a requirement of the PUC End-Users as part of their considerations for the deployment of IRIS within the PUC. This is also a requirement of CERT stakeholder group.		
Traceability	This requirement will be tracked in the D2.6 – IRIS Platform and Reference Architecture, D6.4 – Integrated IRIS Platform and D7.5 – Pilot Evaluation.		

ID	T-PLAT-END_USER-02	Priority	SHOULD
Name	*Storage Requirements*		
Description	The IRIS Platform should be able to store, at-least, up to 1TB per month.		
Rationale	Storage requirement was extrapolated from the PUC End-User survey responses. As the project progresses and the understanding of data flows in the PUC deployment architectures increases, storage requirements may change.		
Traceability	This requirement will be reported on in D7.5 – Evaluation Report.		

ID	T-PLAT-END_USER-03	Priority	SHOULD
Name	*Data Input Format*		
Description	Input data that the IRIS Platform should support include: ○ PCAP files ○ Physical interfaces (eth1..) ○ Log files (.csv, log ingestion) ○ Streaming flows (Kafka, MQTT, Redis ingestion)		
Rationale	This requirement was extrapolated from the PUC End-User survey responses. As the project progresses and the understanding of the PUC deployment architectures increases, this requirement may		

	change.
Traceability	The input data that IRIS platform can support will be progressively evaluated throughout the development of the tools and pilot implementation, including D6.1 (APIs for integration with smart city's IoT and AI-enabled infrastructures) and D7.5 (Pilot Evaluation Report). Associated work packages include WP3 and WP5 (inputs for Virtual Cyber Range)

ID	**T-PLAT-END_USER-04**	**Priority**	**SHOULD**
Name	*Data Output Format*		
Description	Data formats supported by the IRIS Platform should include Syslog, XML and JSON.		
Rationale	This requirement was extrapolated from the PUC End-User survey responses and the CERT group interviews. As the project progresses and the understanding of the PUC deployment architectures increases, this requirement may change (data formats may be added to).		
Traceability	This requirement will be tracked in the D2.6 – IRIS Platform and Reference Architecture, D6.4 – Integrated IRIS Platform and D7.5 – Pilot Evaluation. WP3 and WP4 will also report on the design of the individual IRIS components.		

ID	**T-PLAT-END_USER-05**	**Priority**	**SHOULD**
Name	*Incident Reporting Format*		
Description	IRIS platform should support the following formats for detected events: ○ Standard Syslog ○ Standard/CEF ○ RFC3164 ○ RFC3164/CEF		
Rationale	This requirement was extrapolated from the PUC End-User survey		

	responses and the CERT group interviews. As the project progresses and the understanding of the PUC deployment architectures increases, this requirement may change (incident reporting formats may be added to or reduced).
Traceability	This requirement will be tracked in the D2.6 requirements and D6.1 (APIs for integration with the smart city's IoT and AI-enabled infrastructures)). WP3 and WP4 deliverables will also detail the design of individual IRIS components. The requirement will be further evaluated during the pilot deployment and the cybersecurity incident response scenarios, also including in the cyber range.

ID	**T-PLAT-END_USER-06**	**Priority**	**SHOULD**
Name	*CTI Format*		
Description	IRIS should be able to support formats used by End-Users for threat information sharing include: JSON, STIX/TAXII, txt and PDF (Reports), Syslog, CSV		
Rationale	This requirement was extrapolated from the PUC End-User survey responses and the CERT group interviews. As the project progresses and the understanding of the PUC deployment architectures increases, this requirement may change (CTI data format may be added to or reduced).		
Traceability	The formats supported will be reported/tracked in WP3 and WP4, design of individual IRIS components. The performance will be evaluated in D7.5 pilot evaluation.		

ID	**T-SECU-END_USER-07**	**Priority**	**SHOULD**
Name	*User Authentication*		
Description	Access to the IRIS platform should be available via either multi-factor authentication and/or token-based authentication.		
Rationale	This requirement was extrapolated from the PUC End-User survey responses and the CERT group interviews. It is classified as "should" as it is not listed as an essential requirement in the IRIS project description of action.		

Traceability	WP3 and WP4 deliverables will detail the design of individual IRIS components. WP6 will detail the integration of the IRIS environment to the pilot infrastructure. User authentication will also be evaluated during system integration testing and pilot evaluation.

ID	**T-PLAT-END_USER-08**	**Priority**	**SHOULD**
Name	*IRIS Platform – Monitoring Capability*		
Description	The IRIS Platform should be able to monitor common IoT and ML/AI APIs and protocols. Some of these include, but are not limited to: o Serial Ports o TCP/IP o REST APIs o JSON APIs o Ethernet o Data Factory Resources o DNS o HTTP/HTTPs o Proprietary protocols (IEC104 etc.) o IoT protocols: MQTT, CoAP, ZigBee, 6LowPAN etc.		
Rationale	This requirement was extrapolated from the PUC End-User survey responses and the CERT group interviews. As the project progresses and the understanding of the PUC deployment architectures increases, this requirement may change (list of protocols may be added to or reduced).		
Traceability	WP3 and WP4 deliverables will detail the design of individual IRIS components. WP6 will detail the integration of the IRIS environment to the pilot infrastructure. WP5 deliverables will also detail what protocols will be monitored in the VCR. D7.5 will provide the pilot evaluation report.		

ID	T-PLAT-END_USER-09	Priority	SHOULD
Name	*IRIS Platform User Interface*		
Description	IRIS platform should be able to be accessed via web interface and through mobile device friendly user interface.		
Rationale	This requirement was extrapolated from the PUC End-User survey responses and the CERT group interviews. It is classified as "should" as it is not listed as an essential requirement in the IRIS project description of action.		
Traceability	D6.4 Integrated IRIS Platform will detail the IRIS Platform User Interface and D7.5 will provide the evaluation results.		

5 IRIS PLATFORM REQUIREMENTS

5.1 Functional Requirements

This section lists the functional requirements of the IRIS platform as elicited from the IRIS platform tool owners.

5.1.1 Automated Threat Analytics Module (ATA)

5.1.1.1 IoT and AI-provision Risk & Vulnerability Assessment

ID	FUNC -ATA-01	Priority	SHOULD
Name	*Risk & Vulnerability Assessment - Zero-days vulnerabilities*		
Description	Capability to map abnormal behaviours detected in the target system with attack patterns that can be associated to the presence of zero-days vulnerabilities.		
Rationale	Rule-based systems are difficult to get complete enough, as the space of possible adversarial behaviours is too large. Hence the idea to leverage abnormal behaviour detection, able to first learn what normal behaviour is, and then to detect significant deviations as proxies for likely evidence of attacks.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked through D3.2 IRIS AI Threat Analytics and Detection Engine, D4.1 Dynamic repositories of threats and vulnerabilities and D4.2 Report on Dynamic Knowledge Repositories of Threats for IoT and AI driven ICT systems. It will be further evaluated in the PUCs(WP7) and reported on in D7.5 Evaluation Report.		

ID	FUNC-ATA-02	Priority	SHOULD
Name	*Risk & Vulnerability Assessment – Risk Analysis*		
Description	Capability to perform a thorough risk analysis that comprises the identification of several security factors, such as root causes, impact, damage, and remediation.		
Rationale	Risk and vulnerability assessment requires risk analysis which rely on the analysis of root causes, impact, damage and remediation.		
Parent	No parent		
Dependency	No dependencies		

Traceability	This requirement will be tracked through D3.1 IRIS Risk and Vulnerability Assessment Module, D3.2 IRIS AI Threat Analytics and Detection Engine, D4.1 Dynamic repositories of threats and vulnerabilities and D4.2 Report on Dynamic Knowledge Repositories of Threats for IoT and AI driven ICT systems. It will be further evaluated in the PUCs(WP7) and reported on in D7.5 Evaluation Report.

ID	**FUNC-ATA-03**	**Priority**	**SHOULD**
Name	*Risk & Vulnerability Assessment - Identification Approaches*		
Description	Capability to be able to explore combinations of possibly expensive formal approaches (e.g., symbolic execution) and lightweight practical techniques (e.g., fuzzing), guided by static analysis, applied to the IoT firmware.		
Rationale	Program analysis techniques are important as they allow to discover unknown vulnerabilities. Yet, no technique taken in isolation is perfect, hence the need for combinations in order to find good trade-offs between scalability and precision.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked through D3.2 IRIS AI Threat Analytics and Detection Engine, It will be further evaluated in the PUCs(WP7) and reported on in D7.5 Evaluation Report.		

ID	**FUNC-ATA-04**	**Priority**	**MUST**
Name	*Risk & Vulnerability Assessment - Threat Intelligence Integration*		
Description	Capability to be able to use intelligence sharing functionalities, for the knowledge base enrichment.		
Rationale	Essential for threat intelligence integration		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked through D3.2 IRIS AI Threat Analytics and Detection Engine, D4.1 Dynamic repositories of threats and vulnerabilities and D4.2 Report on Dynamic Knowledge Repositories of Threats for IoT and AI driven ICT systems. It will be further evaluated in the PUCs (WP7) and reported on in D7.5 Evaluation Report.		

ID	FUNC-ATA-05	Priority	SHOULD
Name	*Risk & Vulnerability Assessment – APIs*		
Description	Provide an API to request the scan of devices and retrieve the results and statistics of previous scan activities.		
Rationale	Vulnerability Assessment feature		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked through D4.3 APIs for Advanced Threat Intelligence Orchestration and in the PUCs (WP7) and D7.5 Evaluation Report.		

ID	FUNC-ATA-06	Priority	MUST
Name	*Risk & Vulnerability Assessment - ML Techniques*		
Description	Capability to use machine learning techniques for the detection of unknown vulnerability patterns		
Rationale	Advanced techniques for vulnerability assessment.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked through D3.1 IRIS Risk and Vulnerability Assessment Module, D3.2 IRIS AI Threat Analytics and Detection Engine, D3.3 IRIS Risk-Based Self Response and Self-Recovery Module and D4.4 IRIS Advanced Threat Intelligence Orchestrator. It will be further evaluated in the PUCs(WP7) and reported on in D7.5 Evaluation Report.		

ID	FUNC-ATA-07	Priority	MUST
Name	*Risk & Vulnerability Assessment – Scans programmability*		
Description	Capability to be able to perform vulnerability analysis either automatically (based on a previous scheduled scan or the request of another IRIS component), or manually, as required by the end-user.		
Rationale	Vulnerability analysis		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked through D3.1 IRIS Risk and Vulnerability Assessment Module. It will be further evaluated in the PUCs (WP7) and reported on in D7.5 Evaluation Report.		

ID	FUNC-ATA-08	Priority	SHOULD
Name	*Risk & Vulnerability Assessment – Level of scan*		
Description	Capability to select the level of scan to be performed.		
Rationale	Vulnerability Assessment feature		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked through D3.1 IRIS Risk and Vulnerability Assessment Module. It will be further evaluated in the PUCs (WP7) and reported on in D7.5 Evaluation Report.		

5.1.1.2 Autonomous AI threat analytics and detection engine

ID	FUNC-ATA-09	Priority	MUST
Name	*Threat Analytics – Monitoring*		
Description	Collection and monitoring of the unique characteristics of IoT and AI-provision, such as the data they consume and generate, as well as their responses to different technical workflows and interactions between them.		
Rationale	Threat Analytics feature		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D6.1 APIs and Data models for integration of PUC infrastructure with IRIS platform. The evaluation of this functionality will be evaluated in the pilots which focus on IoT and AI technologies and subsequently reported on in D7.5.		

ID	FUNC-ATA-10	Priority	SHOULD
Name	*Threat Analytics – CERT/CSIRT Functionality*		
Description	Provide CERTs/CSIRTs with a plug-and play threat detection interface for integrating heuristic patterns and models to IoT and AI infrastructures.		
Rationale	Threat Analytics feature		
Parent	No parent		
Dependency	No dependencies		
Traceability	The prototype component of the Threat and Analytics Engine will be detailed in D3.2. The functionality of the tool will be evaluated during		

	WP7 pilots and reported on in the associated WP7 deliverables. DNSC and CERT advisory group will provide feedback as to the functionality of the IRIS platform for CERT/CSIRT collaboration.

ID	FUNC-ATA-11	Priority	MUST
Name	Threat Analytics – Telemetry		
Description	Provide continual threat telemetry for vulnerability assessment, response and self-recovery and threat intelligence publication.		
Rationale	Threat Analytics feature		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in WP3 and WP4 which focus on the individual IRIS components. D3.4 Digital Twin HoneyPot Deception Module will play a crucial role in generation of threat telemetry. The functionality for continual threat telemetry will be evaluated during WP7 pilots and reported on in the associated WP7 deliverables.		

5.1.1.3 Risk-based response and self-recovery

ID	FUNC-ATA-12	Priority	MUST
Name	*Risk-based response functionality*		
Description	Provide novel risk-based response mechanisms which intelligently assess threat analytics inputs from multiple sources.		
Rationale	This requirement is needed as it is central to responding to threats targeting AI and IoT infrastructures.		
Parent	No parent		
Dependency	FUNC-ATA-01, FUNC-ATA-02, FUNC-ATA-03, FUNC-ATA-05, FUNC-ATA-06, FUNC-ATA-08, FUNC-ATA-13		
Traceability	This requirement will be tracked in WP3 and WP4. Specifically D3.3 IRIS Risk-Based Response and Self-Recovery Module. D7.5 will report on the results of the risk-based response functionality during the PUCs.		

ID	FUNC-ATA-13	Priority	SHOULD
Name	*Risk-based response - Application of game theoretic response strategies*		
Description	Capability to apply game-theoretic strategies for finding optimal response solutions based on the impact of the different threats (i.e.,		

	indicators of compromise) and the system(s) affected, including the corresponding remediation actions that can be taken.
Rationale	This requirement is needed as it is central to finding optimal response solutions to threats targeting AI and IoT infrastructures.
Parent	FUNC-ATA-13
Dependency	FUNC-ATA-12
Traceability	This requirement will be tracked in WP3 and WP4. Specifically, D3.3 IRIS Risk-Based Response and Self-Recovery Module. D7.5 will report on the results of the risk-based response functionality during the PUCs.

ID	**FUNC-ATA-14**	**Priority**	**SHOULD**
Name	*Risk-based response - Standardized actions*		
Description	Capability to enable the extraction a standardized set of actions that will represent the optimal response and self-recovery strategy.		
Rationale	This requirement is needed as it is central to responding to threats targeting AI and IoT infrastructures using standardized response and self-recovery actions.		
Parent	FUNC-ATA-13		
Dependency	FUNC-CTI-01, FUNC-CTI-02		
Traceability	This requirement will be tracked in WP3 and WP4. Specifically, D3.3 IRIS Risk-Based Response and Self-Recovery Module. D7.5 will report on the results of the risk-based response functionality during the PUCs.		

ID	**FUNC-ATA-15**	**Priority**	**SHOULD**
Name	*Risk-based response - Decision making*		
Description	Capability to guarantee that risk-based decision making will be supervised with policies defined by CERT/CSIRT operators.		
Rationale	This requirement is needed as it is central to providing IRIS's human-in-the-loop for response functionality.		
Parent	FUNC-ATA-14		
Dependency	FUNC-End_User-12		
Traceability	This requirement will be tracked in WP3 and WP4. Specifically, D3.3 IRIS Risk-Based Response and Self-Recovery Module. D5.3 will detail IRIS Lab Pods for CERTS/CSIRTS. D7.5 will report on the results of the risk-based response functionality during the PUCs. DNSC and CERT advisory group will provide feedback as to the functionality of the IRIS platform for CERT/CSIRT collaboration.		

ID	FUNC-ATA-16	Priority	SHOULD
Name	*Risk-based response - Trigger/Threshold conditions*		
Description	Capability to guarantee that policies will establish the trigger/threshold conditions for self-recovery based on the optimal impact resolution reported.		
Rationale	This requirement is needed as it is central to providing IRIS's human-in-the-loop for response functionality.		
Parent	FUNC-ATA-14		
Dependency	FUNC-End_User-12		
Traceability	This requirement will be tracked in WP3 and WP4. Specifically, D3.3 IRIS Risk-Based Response and Self-Recovery Module. D7.5 will report on the results of the risk-based response functionality during the PUCs.		

ID	FUNC-ATA-17	Priority	SHOULD
Name	*Risk-based response - VCR testing functionality*		
Description	Capability to test and evaluate automated risk-based response input and output inside the IRIS Virtual Cyber Range (VCR) module as a Lab Pod.		
Rationale	This requirement is needed as it is central to testing and evaluating the risk-based response functionality of the IRIS platform during the IRIS pilot use cases.		
Parent	FUNC-ATA-14		
Dependency	FUNC-VCR-01, FUNC-VCR-02, FUNC-CTI-01, FUNC-CTI-02		
Traceability	This requirement will be tracked in D5.3 IRIS Lab Pods for CERTS/CSIRTS. D7.5 will also provide results from the PUCs.		

5.1.1.4 Digital Twin Honeypot Telemetry and Analytics Modules

ID	FUNC-ATA-18	Priority	SHOULD
Name	*Support customized analytics – Create Dashboards or reports on Demand*		
Description	Capability to build customized analytics to enable the expansion of security features using self-service analytics.		

Rationale	Log analysis is used in analytics to look for security issues while protecting user privacy. To help improve detection efficiency, self-learning AI algorithms should be developed.
Parent	Artificial intelligence algorithms
Dependency	No dependency with other component
Traceability	This requirement will be tracked in D3.4 IRIS Digital Twin HoneyPot Deception Models and D3.2 AI Threat Analytics and Detection Engine. D7.5 will report the results of the PUCs.

ID	**FUNC-ATA-19**	**Priority**	**SHOULD**
Name	*Automated Threat detection*		
Description	Incorporate parser development to centralize and normalize data, which saves time and effort, is a feature of automated threat detection. The aim is to deceive possible attackers from detecting the real device. Unauthorized attempts to enter the environment will be detected automatically by DT Honeypot.		
Rationale	Prevent security incidents and/or harm from occurring by accurately identifying and responding to possible IRIS system risks.		
Parent	Automated Threat Analytics Module		
Dependency	No Dependency		
Traceability	This requirement will be tracked in D3.4 IRIS Digital Twin HoneyPot Deception Models and D3.2 AI Threat Analytics and Detection Engine. D7.5 will report the results of the PUCs.		

ID	**FUNC-ATA-20**	**Priority**	**MUST**
Name	*Service Analysis*		
Description	Smart Service analysis to be based on Digital twin data		
Rationale	The DT data is analysed and visualized using ML models, which offer insights and suggestions and assist decision-making.		
Parent	Machine Learning models		
Dependency	Automated Threat Analytics module		
Traceability	This requirement will be tracked in D3.4 IRIS Digital Twin HoneyPot Deception Models and D3.2 AI Threat Analytics and Detection		

	Engine. D7.5 will report the results of the PUCs.

ID	FUNC-ATA-21	Priority	SHOULD
Name	*List with countermeasure exploits and usage patterns*		
Description	Capability to support automated threat intelligence orchestration for implementing proactive defence measures against threats.		
Rationale	ATA will utilize the DT Knowledge base which includes this list.		
Parent	Artificial intelligence algorithms		
Dependency	No dependency with other component		
Traceability	This requirement will be tracked in the WP3 and WP4 deliverables. D7.5 will report the results of the PUCs.		

ID	FUNC-ATA-22	Priority	SHOULD
Name	*Incident response*		
Description	Observable analysers and operation automation responders to be included in the DT honeypot. Published MISP threat incidents will be disseminated in this manner.		
Rationale	It is necessary to prevent such events from occurring if a threat is traced and identified. If the system becomes contaminated, it will be isolated to prevent further spread. Honeypots, for example, are a type of deception technology that improves the efficiency and effectiveness of incident response. Detection criteria and the range of imitation in response must be tailored to the attack scenario.		
Parent	No parent		
Dependency	MISP threat sharing platform		
Traceability	This requirement will be tracked in D3.4 IRIS Digital Twin HoneyPot Deception Models and D3.2 AI Threat Analytics and Detection Engine. D7.5 will report the results of the PUCs.		

ID	FUNC-ATA-23	Priority	SHOULD
Name	*Mitigation actions*		
Description	Capability to scale operations and adapt to threats against IoT and AI-driven systems		
Rationale	For specific Use case scenarios, software-based and tailored		

	mitigation measures will be used.
Parent	Automated Threat Analytics module
Dependency	Automated Threat Analytics module
Traceability	The ability of the ATA module to support IoT and AI systems will be evaluated in the PUCs(WP7).

ID	**FUNC-ATA-24**	**Priority**	**COULD**
Name	*Automated Incident sharing*		
Description	Capability for Digital Twin Honeypot to be able to share incidents with MISP.		
Rationale	Allows the DT to have varying levels of security depending on the sensitivity of the data it carries. Cyber-physical systems are vulnerable to security risks and privacy breaches caused by communication technologies and protocols, so the suitable strategy must be implemented to increase cybersecurity. MISP's threat sharing platform will be used as free and open-source software to facilitate information sharing, including cyber security indications – this will be accessed through the enhanced MeliCERTes ecosystem.		
Parent	No parent.		
Dependency	Enhanced MeliCERTes Ecosystem - MISP threat sharing platform		
Traceability	This requirement will be tracked in D3.4 IRIS Digital Twin HoneyPot Deception Models and D3.2 AI Threat Analytics and Detection Engine. D7.5 will report the results of the PUCs.		

5.1.2 Cyber Threat Intelligence Module

5.1.2.1 Dynamic Repositories of Threats and Vulnerabilities

ID	FUNC-CTI-01	Priority	MUST
Name	*Intelligence Storage*		
Description	Capability to receive and store structured intelligence from threats identified by the ATA module.		
Rationale	For storage of structured intelligence		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in WP3 and WP4 and specifically, D3.2 AI Threat Analytics and Detection Engine. D7.5 will report the results of the PUCs.		

ID	FUNC-CTI-02	Priority	MUST
Name	*Information Analysis*		
Description	Capability to allow the resulting information to be subsequently verified and updated by domain experts through the MISP platform.		
Rationale	Enabling threat information enrichment by experts		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in WP3 and WP4 which are the prototypes of the IRIS components. D5.3 will provide Lab PODS for CERTS/CSIRTS in which threat information analysis will be a part of. D7.5 will report the results of the PUCs.		

5.1.2.2 CERTs/CSIRTs collaborative threat intelligence sharing

ID	FUNC-CTI-03	Priority	MUST
Name	*Intelligence correlation of internal and external sources*		
Description	Capability to correlate the intelligence collected locally and through external feeds		
Rationale	The threat intelligence sharing component must be able to utilize and correlate in the most efficient way the information from CERT/CSIRTs (Enhanced MeliCERTes Ecosystem) and T3.2 in order to enhance the information from ATA.		

Parent	No parent
Dependency	No dependencies
Traceability	This capability will be mapped in D2.6 to some of the IRIS components developed in WP4. The details of the implementation will be reported in D4.2. This capability will be practically evaluated during the WP7 Pilot Use-Cases in conjunction with CERT/CSIRTs.

ID	**FUNC-CTI-04**	**Priority**	**MUST**
Name	*Dynamic generation of taxonomies and ontologies*		
Description	Capability to leverage the dynamically generated taxonomies and ontologies.		
Rationale	The threat intelligence sharing component must be able to dynamically generate taxonomies and ontologies and expand them based on existing data from CERT/CSIRTs (Enhanced MeliCERTes Ecosystem) and T3.2, targeting on IoT and AI-based systems in order to enhance the information from ATA.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be mapped in D2.6 to some of the IRIS components developed in WP4. The details of the implementation will be reported in D4.2. This capability will be practically evaluated during WP7 Pilot Use Cases.		

ID	**FUNC-CTI-05**	**Priority**	**MUST**
Name	*Automatic correlation of new data*		
Description	Capability to automatically correlate new data added to the platform with existing intelligence based on different attributes (such as Indication of Compromise - IoC).		
Rationale	Correlation mechanisms will be used in order to enrich/correlate existing data with newly acquired data.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be mapped in D2.6 to some of the IRIS components developed in WP4. The details of the implementation will be reported in D4.2. This capability will be practically evaluated during WP7 Pilot Use Cases.		

5.1.2.3 Advanced threat intelligence and Analytics Orchestration (TAO)

ID	FUNC-CTI-06	Priority	MUST
Name	*Orchestrator intelligent workflow*		
Description	Capability to track system for the automated or semi-automated processes.		
Rationale	The OWM (Orchestration Workflow Manager) will offer a workflow design functionality, orchestration process monitoring and Threat Sharing and Response tasks management by a tracking system for the automated or semi-automated processes.		
Parent	No parent		
Dependency	Cerebrate[1] of Enhanced MeliCERTes Ecosystem		
Traceability	This requirement will be tracked in WP4, specifically, D4.4 IRIS Advanced Threat Intelligence Orchestrator. This capability will be practically evaluated during WP7 Pilot Use Cases.		

ID	FUNC-CTI-07	Priority	MUST
Name	*Incorporation of data from external and internal sources for extracting predictive measures.*		
Description	Capability to receive information (coming from the CTI module and the enhanced MeliCERTes ecosystem) in order to extract recommended response measures given the functionality can be provided by a subcomponent of the system.		
Rationale	The Threat Sharing and Response manager must be able to intervene and provide information about the recommended response measures.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in WP3 and WP4. This capability will be practically evaluated during WP7 Pilot Use Cases.		

[1] https://cerebrate-project.org/

5.1.2.4 Enhanced MeliCERTes Ecosystem (EME)

ID	FUNC-EME-01	Priority	MUST
Name	*Cyber Threat Intelligence presentation/visualization – Unified Dashboard*		
Description	Capability to present through GUI/unified Dashboard, the collected cyber threat intelligence related information to the participating entities (e.g. organizations and CERTs/CSIRTs)		
Rationale	Essential component to the EME enhancements.		
Parent	FUNC-CTI-05, FUNC-CTI-07		
Dependency	T_PLAT-CTI-09		
Traceability	This requirement will be tracked in D4.7 IRIS-Enhanced MeliCERTes Platform. This capability will be practically evaluated during the WP7 Pilot Use-Cases in conjunction with CERT/CSIRTs.		

ID	FUNC-EME-02	Priority	MUST
Name	*Threat Intelligence Companion integration*		
Description	Capability to provide/receive input about the recommended response measures.		
Rationale	Part of the information sharing package for exchanging threat information.		
Parent	FUNC-CTI-10		
Dependency	FUNC-EME-03		
Traceability	This requirement will be tracked in WP3 and WP4 and, specifically, D4.7 IRIS-Enhanced MeliCERTes Platform. This capability will be practically evaluated during the WP7 Pilot Use-Cases in conjunction with CERT/CSIRTs.		

ID	FUNC-EME-03	Priority	MUST
Name	*Risk-based optimisation/ranking module integration*		
Description	Capability to receive a risk-based optimisation/ranking information that will support CSIRTs/CERTs on decision making		
Rationale	Part of the information sharing package for exchanging threat information.		
Parent	FUNC-CTI-10		
Dependency	FUNC-EME-02		
Traceability	This requirement will be tracked in WP3 and WP4 and, specifically,		

	D4.7 IRIS-Enhanced MeliCERTes Platform. This capability will be practically evaluated during the WP7 Pilot Use-Cases in conjunction with CERT/CSIRTs.

ID	FUNC-EME-04	Priority	SHOULD
Name	Pan-European cybersecurity knowledge base		
Description	Capability to store and augment the cybersecurity knowledge base of AI targeted attacks, incidents, countermeasures etc. at a Pan-European level.		
Rationale	Improve community knowledge base.		
Parent	No parent		
Dependency	No dependency		
Traceability	This requirement will be tracked in WP3 and WP4 and, specifically, D4.7 IRIS-Enhanced MeliCERTes Platform. This capability will be practically evaluated during the WP7 Pilot Use-Cases in conjunction with CERT/CSIRTs..		

ID	FUNC-EME-05	Priority	MUST
Name	*Secure communication and collaboration*		
Description	Capability to securely communicate and collaborate online with a more extended pool of stakeholders/operators.		
Rationale	MeliCERTes platform will guarantee that there will be secure communication and collaboration. DLT will also support information immutability, traceability and accountability.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in WP3 and WP4 and, specifically, D4.7 IRIS-Enhanced MeliCERTes Platform. This capability will be practically evaluated during the WP7 Pilot Use-Cases in conjunction with CERT/CSIRTs.		

ID	FUNC-EME-06	Priority	MUST
Name	*Enhanced MeliCERTes architecture distribution*		
Description	Requires being distributed, with different customized instances deployed at each stakeholders' premises.		
Rationale	The architecture of the enhanced MeliCERTes ecosystem must be able to be distributed.		

Parent	No parent
Dependency	No dependencies
Traceability	This requirement will be tracked in WP3 and WP4 and, specifically, D4.7 IRIS-Enhanced MeliCERTes Platform. This capability will be practically evaluated during the WP7 Pilot Use-Cases in conjunction with CERT/CSIRTs.

5.1.3 Data Protection and Accountability (DPA) Module

ID	FUNC-DPA-01	Priority	MUST
Name	*General - accountability, auditability and traceability*		
Description	Capability to guarantee accountability, auditability and traceability of the activities performed in the IRIS system.		
Rationale	Guarantee overall integrity and correctness of the operations of IRIS system.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 and D4.6. The performance of the DLT component will be evaluated in the PUCs and detailed in D7.5.		

ID	FUNC-DPA-02	Priority	MUST
Name	*General - Immutable event log*		
Description	Capability for the DLT to serve as an immutable event log for the collaborative threat intelligence network.		
Rationale	Guarantee auditability of actions		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 and D4.6. The performance of the DLT component will be evaluated in the PUCs and detailed in D7.5.		

ID	FUNC-DPA-03	Priority	MUST
Name	*General - Private Networks*		
Description	Capability for the DLT architecture to enable a collaborative threat intelligence community to maintain its own permissioned ledger within an authenticated private network.		
Rationale	Guarantee management autonomy of the DLT within each threat intelligence community and efficiency of DLT		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 and D4.6. The performance of the DLT component will be evaluated in the PUCs and detailed in D7.5.		

ID	FUNC-DPA-04	Priority	MUST
Name	*General - Multi-layer security*		
Description	Multi-layer security to be employed to guarantee DLT security.		
Rationale	Guarantee security of the DLT system		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 and D4.6. The performance of the DLT component will be evaluated in the PUCs and detailed in D7.5.		

ID	FUNC-DPA-05	Priority	MUST
Name	*Off-chain data*		
Description	Capability for data about interactions of IRIS modules to be stored on off-chain databases, using Cloud-based storage system. The ledger should only store data pointers which securely link to the cloud storage system.		
Rationale	Guarantee IRIS systems interactions data privacy		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 and D4.6. The performance of the DLT component will be evaluated in the PUCs and detailed in D7.5.		

ID	FUNC-DPA-06	Priority	MUST
Name	*Stored data protection*		
Description	Capability for the DLT to leverage data protection functions/encryption systems to protect stored data.		
Rationale	Guarantee protection of stored data		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 and D4.6. The performance of the DLT component will be evaluated in the PUCs and detailed in D7.5.		

ID	FUNC-DPA-07	Priority	MUST
Name	*Consensus mechanism*		
Description	Block data validation process to be followed via an appropriate consensus mechanism prior to data storage in the ledger,.		
Rationale	Guarantee correctness of data stored		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 and D4.6. The performance of the DLT component will be evaluated in the PUCs and detailed in D7.5.		

ID	FUNC-DPA-08	Priority	MUST
Name	*Interaction - Ledger Query API*		
Description	API for allowing querying the ledger to be implemented. Holders of the appropriate keys will be able to access to the data.		
Rationale	Allow ledger querying		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 and D4.6. The performance of the DLT component will be evaluated in the PUCs and detailed in D7.5.		

ID	FUNC-DPA-09	Priority	MUST
Name	*Interaction - Stakeholder interaction smart contract*		
Description	Smart contract, enabling stakeholders' interaction with the ledger to be implemented. This smart contract will enable stakeholders' authentication and will capture their behaviour and operations. This smart contract will also ensure event log and attestation history to be traceable, immutable and end-to-end transparent to authenticated partners.		
Rationale	Allow secure stakeholder's interaction with DLT		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 and D4.6. The performance of the DLT component will be evaluated in the PUCs and detailed in D7.5.		

ID	FUNC-DPA-10	Priority	MUST
Name	*Interaction - API for IRIS modules*		
Description	API for proper interaction with other IRIS modules to be in place. This API will identify data read's and write activities.		
Rationale	Allow data collection from IRIS modules		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 and D4.6 and D6.1 APIs and Data Models for smart city infrastructure integration with IRIS components. The performance of the DLT component will be evaluated in the PUCs and detailed in D7.5.		

ID	FUNC-DPA-11	Priority	MUST
Name	*Private Network - membership authentication*		
Description	Appropriate membership authentication mechanism to be in place.		
Rationale	Guarantee appropriate authentication to the DLT		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 and D4.6. The performance of the DLT component will be evaluated in the PUCs and detailed in D7.5.		

ID	FUNC-DPA-12	Priority	MUST
Name	*Private Network - external partners access*		
Description	Capability to dynamically extend access to the permissioned ledger to external partners.		
Rationale	Guarantee appropriate authentication to the DLT		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 and D4.6. The performance of the DLT component will be evaluated in the PUCs and detailed in D7.5.		

5.1.4 Virtual Cyber Range (VCR)

5.1.4.1 Human-Centric Collaborative Online IoT & AI training and cybersecurity exercises

ID	FUNC-VCR-01	Priority	MUST
Name	*Training Knowledge Transfer and CERT/CSIRT Requirements*		
Description	Capability to use a cyber range to transfer to the trainees not only knowledge, but also the abilities and attitudes that meet the needs of CERTs/CSIRTs.		
Rationale	Part of the requirements of the VCR.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked within WP5, which has multiple deliverables related to training scenarios. These include D5.1, 5.2, 5.3 and 5.4. The pilot deployment evaluation will be detailed in D7.5.		

5.1.4.2 IRIS lab pods for CERTs/CSIRTs

ID	FUNC-VCR-02	Priority	MUST
Name	*MeliCERTes for IRIS lab pods*		
Description	Capability to guaranteeing that virtual IRIS enhanced-MeliCERTes nodes include fully functional ATA, CTI and DPA modules.		
Rationale	Part of the requirements of the IRIS lab pods for VCR.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in WP5, specifically D5.4 IRIS Cyber Range. D6.3 and D6.4 will detail the integration of the IRIS Platform. D7.5 will provide the evaluation of the PUCs.		

ID	FUNC-VCR-03	Priority	MUST
Name	*Capability*		
Description	Capability for the VCR to be employed for testing, validation, and training purposes.		
Rationale	Part of the requirements for VCR.		
Parent	No parent		
Dependency	No dependencies		

Traceability	This requirement will be tracked in WP5, specifically D5.1 IRIS Cybersecurity Exercises and Training Lab. D6.3 and D6.4 will detail the integration of the IRIS Platform. D7.5 will provide the evaluation of the PUCs.

5.1.4.3 IRIS Cyber Range Environment Platform and Dashboard

ID	FUNC-VCR-04	Priority	MUST
Name	*Modelling and emulating real-world scenarios*		
Description	Capability of the VCR to model and emulate real-world scenarios enabling collaborative CERTs/CSIRTs training		
Rationale	Part of the requirements for VCR.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in WP5, specifically D5.1 IRIS Cybersecurity Exercises and Training Lab. D6.3 and D6.4 will detail the integration of the IRIS Platform. D7.5 will provide the evaluation of the PUCs.		

ID	FUNC-VCR-05	Priority	MUST
Name	*Sandbox*		
Description	Capability to operate as a sandbox to train and test new response methodologies in a safe environment		
Rationale	Part of the requirements for VCR.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in WP5, specifically D5.1 IRIS Cybersecurity Exercises and Training Lab. D6.3 and D6.4 will detail the integration of the IRIS Platform. D7.5 will provide the evaluation of the PUCs.		

ID	FUNC-VCR-06	Priority	MUST
Name	*Virtualization Technologies and Software Components*		
Description	Capability to leverage established virtualization technologies and softwarised components		

Rationale	Part of the requirements for VCR.
Parent	No parent
Dependency	No dependencies
Traceability	This requirement will be tracked in WP5, specifically D5.2 IRIS Scenario and Asset Catalogue and D5.4 IRIS Cyber Range. D6.3 and D6.4 will detail the integration of the IRIS Platform. D7.5 will provide the evaluation of the PUCs.

ID	***FUNC-VCR-07***	**Priority**	**MUST**
Name	*Cyber Range Virtual Assets*		
Description	Capability to provide an easy-to-use catalogue of assets for setting up training scenarios (via drag & drop or via description models), including all the ATA, CPI, and DPA pods developed in IRIS		
Rationale	Part of the requirements of the IRIS lab pods for VCR.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in WP5, specifically D5.2 IRIS Scenario and Asset Catalogue and D5.4 IRIS Cyber Range. D6.3 and D6.4 will detail the integration of the IRIS Platform. D7.5 will provide the evaluation of the PUCs.		

ID	**FUNC-VCR-08**	**Priority**	**MUST**
Name	*Virtualized SIEM*		
Description	Capability to host the virtualized SIEM in the cyber range platform for the real-time monitoring and notification of security events of the emulated system		
Rationale	The cyber range platform will host the virtualized SIEM (Security Information and Event Management) component, grouping security information and event management functionalities for the real-time monitoring and notification of security events of the emulated system.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in WP5, specifically D5.2 IRIS Scenario and Asset Catalogue and D5.4 IRIS Cyber Range. D6.3 and D6.4 will detail the integration of the IRIS Platform. D7.5 will provide the evaluation of the PUCs.		

ID	FUNC-VCR-09	Priority	MUST
Name	*Situational Awareness*		
Description	Capability to provide a user interface with features of situational awareness to the trainees.		
Rationale	Part of the requirements for VCR.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in WP5, specifically D5.2 IRIS Scenario and Asset Catalogue and D5.4 IRIS Cyber Range. D6.3 and D6.4 will detail the integration of the IRIS Platform. D7.5 will provide the evaluation of the PUCs.		

5.2 Technical Requirements

5.2.1 Automated Threat Analytics

5.2.1.1 IoT and AI-provision Risk & Vulnerability Assessment

ID	T_PLAT-ATA-01	Priority	MUST
Name	*Risk & Vulnerability Assessment – Standards*		
Description	Capability to provide sharing mechanisms with external entities using standard well-known standards and formats (e.g., JSON, STIX).		
Rationale	Part of the requirements of the ATA module design.		
Parent	FUNC_EME-04, T-PLAT-END_USER-06		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D3.2 IRIS AI Threat Analytics and Detection Engine. WP6 will track the integration and testing of IRIS Components. D7.5 will provide the evaluation of the ATA platform in the pilot deployments.		

ID	T-PLAT-ATA-02	Priority	MUST
Name	*Risk & Vulnerability Assessment – Management*		
Description	Capability to integrate with the Autonomous AI threat analytics and detection engine for an appropriate risk and vulnerability management.		
Rationale	Part of the requirements of the ATA module design.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D3.2 IRIS AI Threat Analytics and Detection Engine. WP6 will track the integration and testing of IRIS Components. D7.5 will provide the evaluation of the ATA platform in the pilot deployments.		

ID	T-USAB-ATA-03	Priority	SHOULD
Name	*Risk & Vulnerability Assessment – GUI*		
Description	Capability to provide a web-based user interface where the user can see the status of the scans and the corresponding reports.		
Rationale	Part of the requirements of the ATA module design.		
Parent	No parent		
Dependency	No dependencies		

Traceability	The detailed design on the prototype provided in WP3 and reported in D3.2. The practical evaluation will be performed in WP7 Pilot Use Cases.

ID	**T-SECU-ATA-04**	**Priority**	**SHOULD**
Name	*Risk & Vulnerability Assessment – SSO integration*		
Description	Capability to offer integration with SSO mechanisms.		
Rationale	Part of the requirements of the ATA module design.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D3.2 IRIS AI Threat Analytics and Detection Engine. WP6 will track the integration and testing of IRIS Components. D7.5 will provide the evaluation of the ATA platform in the pilot deployments.		

ID	**T-SECU-ATA-05**	**Priority**	**SHOULD**
Name	*Risk & Vulnerability Assessment – Secure APIs*		
Description	Capability to offer secure APIs by including authentication and authorization mechanisms on them		
Rationale	Part of the requirements of the ATA module design.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D3.2 IRIS AI Threat Analytics and Detection Engine. WP6 will track the integration and testing of IRIS Components. D6.1 will detail the APIs and Data models for the integration of the pilot infrastructure with the IRIS platform. D7.5 will provide the evaluation of the ATA platform in the pilot deployments.		

5.2.1.2 Autonomous AI threat analytics and detection engine

ID	T_PLAT-ATA-06	Priority	MUST
Name	*Threat Analytics – ML Classifiers*		
Description	Capability to develop "sentinel" machine learning anomaly classifiers for IoT, and AI threat-intelligence enriched knowledge-framework to monitor attack patterns against IoT infrastructure and AI-provisioned systems.		
Rationale	Part of the requirements of the ATA module design.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and reported in D3.2. The practical evaluation will be performed in WP7 Pilot Use Cases.		

ID	T_PLAT-ATA-07	Priority	MUST
Name	*Detection Engine – Integrate IoCs*		
Description	Capability to develop a detection engine to dynamically integrate indicators of compromise related to IoT and AI threats, derived from threat intelligence reporting and process orchestration, with support for dynamic and incremental improvements to detect existing and novel attacks.		
Rationale	Part of the requirements of the ATA module design.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and reported in D3.2. The practical evaluation will be performed in WP7 Pilot Use Cases.		

5.2.2 Risk Based Response and Self-Recovery

ID	T_PLAT-ATA-08	Priority	MUST
Name	*Detection Telemetry Ingest – ATA threat event parsers*		
Description	Capability to ingest detection telemetry via remote network/API service sent to the response module from the "Autonomous AI threat analytics and detection engine" in JSON format. Ingested telemetry is required to be parsed and processed the response module to generate the necessary data points for the "risk-based" response AI process.		
Rationale	This requirement is needed as it is central for the response module to generate the necessary data points for the "risk-based" response AI process.		
Parent	No Parent		
Dependency	No Dependency		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and reported in D3.2. The practical evaluation will be performed in WP7 Pilot Use Cases.		

ID	T_PLAT-ATA-09	Priority	SHOULD
Name	*Response Recommendation – Response Strategy Objects*		
Description	Provide a "response strategy" JSON object which contains a series of recommended response steps in JSON format. The response strategy is required to be sent to the CTI module to forward threat response actions to target users/systems.		
Rationale	This requirement is needed as it is central to developing IRIS's "risk-based" response strategy.		
Parent	T_PLAT-ATA-06		
Dependency	T_PLAT-ATA-11		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and reported in D3.2. The practical evaluation will be performed in WP7 Pilot Use Cases.		

5.2.3 Digital Twin Honeypot Telemetry and Analytics Modules

ID	T_PLAT-ATA-10	Priority	MUST
Name	*Data collection Interfaces*		
Description	Capability for the DT Honeypot to be able to infer data acquired during the run time to incorporate them into the Digital Twin knowledge base.		
Rationale	An interface will be used to collect raw data from the Honeypot.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and D3.2 and D3.4. The practical evaluation will be performed in WP7 Pilot Use Cases.		

ID	T_PLAT-ATA-011	Priority	MUST
Name	*Vulnerability identification*		
Description	Capability for exposing functional and internal systems components to facilitate the discovery of new attack vectors.		
Rationale	As the first line of protection, the use of digital twins, honeypots, and machine learning algorithms has the potential to reduce system vulnerabilities while also speeding up the time it takes to notice a system vulnerability.		
Parent	Artificial Intelligence algorithms		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and D3.2 and D3.4. The practical evaluation will be performed in WP7 Pilot Use Cases.		

ID	T_PLAT-ATA-012	Priority	MUST
Name	*User interface to present attack telemetry*		
Description	Capability for a real attack to be represented in attack telemetry. DT Honeypot will provide an attack telemetry channel to the ATA and CTI modules so that new IoT and AI technologies can be tested in the field. Honeypot's capacity to turn raw data into threat intelligence is what makes it unique.		
Rationale	Data from the DT will be used to demonstrate IRIS's ability to deliver threat analytics for advanced IoT and AI attacks, as well as to simplify the collection of ML attack telemetry.		
Parent	No parent		

Dependency	No dependencies
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and D3.2 and D3.4. The practical evaluation will be performed in WP7 Pilot Use Cases.

ID	**T_PLAT-ATA-13**	**Priority**	**MUST**
Name	*Honeypot Availability*		
Description	Required the Honeypot to be available to get attacked, exploited and probed.		
Rationale	Provide a virtualized honeypot out there that can attract and collect data from attackers. The DT will be fed with the data that has been acquired. Depending on the application, log files or network traffic logs may be used to collect the data.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and D3.2 and D3.4. The practical evaluation will be performed in WP7 Pilot Use Cases.		

5.2.4 Cyber Threat Intelligence (CTI) Module

5.2.4.1 Dynamic Repositories of Threats and Vulnerabilities

ID	T_PLAT-CTI-01	Priority	MUST
Name	*Machine learning and other methods*		
Description	Capability to use rule-based and machine learning-based methods for dynamic generation of taxonomies and ontologies.		
Rationale	Rule based techniques can be used to identify keywords/key phrases in order to map the collected information to taxonomies and ontologies. Machine learning techniques can be used to (semi-) automatically map the collected information to taxonomies and ontologies.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and WP4. The practical evaluation will be performed in WP7 Pilot Use Cases.		

ID	T_USAB-CTI-02	Priority	MUST
Name	*Dynamic taxonomies and ontologies*		
Description	Capability to use techniques for generating dynamic taxonomies and ontologies in a semi-automatic way.		
Rationale	The automation in processing of the generated threat information is crucial. Dynamic update of the generated taxonomies and ontologies.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.1 and D4.2 which focus on the Dynamic knowledge repositories for threats and vulnerabilities. WP3 and WP4 will detail how the IRIS components interact/use the taxonomies. D7.5 will report on the performance of the IRIS components in the PUCs.		

5.2.4.2 CERTs/CSIRTs collaborative threat intelligence sharing

ID	T_PLAT-CTI-03	Priority	MUST
Name	*Threat intelligence sharing component*		
Description	Provide connectivity among the orchestrator, the ATA and DPA modules of the platform, the collection of information from external repositories, and their sharing configurations.		
Rationale	Guarantee that it will connect with orchestrator, ATA and DPA modules allowing for swift threat identification, precision response and collaboration among intelligence sharing tools and technologies.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and WP4. The practical evaluation will be performed in WP7 Pilot Use Cases.		

ID	T_PLAT-CTI-04	Priority	MUST
Name	*Threat intelligence sharing collection capabilities*		
Description	Capability to automatically collect the threat intelligence extracted from the ATA module.		
Rationale	ATA is the main module that will identify IoT and Al threats. Automatic collection is mandatory due to the vast amount of information data.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and WP4. The practical evaluation will be performed in WP7 Pilot Use Cases.		

ID	T_SECU-CTI-05	Priority	MUST
Name	*DPA and blockchain technologies*		
Description	Capability to automatically update when new data entries interact with the DPA to efficiently and securely store the collected information in the cloud using DPA's blockchain-based storage mechanisms.		
Rationale	All the information inside the IRIS platform must be under the DPA protection/enhanced capabilities.		
Parent	No parent		
Dependency	No dependencies		

Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and WP4. The practical evaluation will be performed in WP7 Pilot Use Cases.

ID	**T_USAB-CTI-06**	**Priority**	**MUST**
Name	*CTI user friendliness*		
Description	Provide a GUI that will support the presentation and editing of the collected data and the configuration of the underlying gathering, correlation, and sharing procedures.		
Rationale	The Accessibility capabilities are important of the overall user experience.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and WP4. The practical evaluation will be performed in WP7 Pilot Use Cases.		

ID	**T_SECU-CTI-07**	**Priority**	**MUST**
Name	*Filtering and anonymization techniques*		
Description	Capability to support advanced filtering and anonymization techniques.		
Rationale	The filtering and anonymization technique will help organization protect of the accidentally sharing of classified or sensitive information.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and WP4. The practical evaluation will be performed in WP7 Pilot Use Cases.		

5.2.4.3 Advanced threat intelligence and Analytics Orchestration (TAO)

ID	T_PLAT-CTI-08	Priority	MUST
Name	*Integration of interfaces*		
Description	Requires being able to provide integration through interfaces.		
Rationale	A set of APIs will be developed, in order Advanced Threat Intelligence and Analytics Orchestrator exchanging data among tools.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and WP4. The practical evaluation will be performed in WP7 Pilot Use Cases.		

ID	T_PLAT-CTI-09	Priority	MUST
Name	*Creation of dynamic workflows*		
Description	Provide a design of automatic/semi-automatic execution capabilities (through Orchestration Workflow Manager (OWM))		
Rationale	A workflow is provided (a visual depiction) enabling users execute or modify it as they preferred.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and WP4. The practical evaluation will be performed in WP7 Pilot Use Cases.		

ID	T_PLAT-CTI-10	Priority	SHOULD
Name	*Usage of playbooks/runbooks*		
Description	Process and manage the creation of workflows based on playbooks/runbooks		
Rationale	Includes important information for the execution of a workflow, such as background information and procedures to successfully execute security-related tasks, or address incidents (runbooks), similar workflows, operating procedures, and cultural values required to approach and complete tasks in a consistent way (playbooks).		
Parent	No parent		
Dependency	No dependencies		

Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and WP4. The practical evaluation will be performed in WP7 Pilot Use Cases.

ID	**T_PLAT-CTI-11**	**Priority**	**MUST**
Name	*Command execution requests*		
Description	Capability for command execution requests to be defined based on existing solutions and the OpenAPI specification.		
Rationale	Leverage on SoTA and existing solutions with the intention to enhance the range of IRIS capabilities.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and WP4. The practical evaluation will be performed in WP7 Pilot Use Cases.		

ID	**T_PLAT-CTI-12**	**Priority**	**MUST**
Name	*Adheres SOAR capabilities*		
Description	The development of Threat Intelligent Orchestrator to be designed based on security, orchestration, automation, recovery capabilities.		
Rationale	Based on SoTA, many commercial tools and services related to TAO capabilities are designed following SOAR capabilities, facilitating the processes.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D2.6. and detailed design on the prototype provided in WP3 and WP4. The practical evaluation will be performed in WP7 Pilot Use Cases.		

5.2.4.4 Enhanced MeliCERTes Ecosystem

ID	T_PLAT-EME-01	Priority	MUST
Name	*Sharing capabilities of MeliCERTes*		
Description	Capability for more secure and efficient security information representation in standardized formats and sharing capitalizing and extending existing ontologies, such as STIX 2.1.		
Rationale	The sharing of the threat information is crucial. STIX 2.1 or STIX 2.2 are popular sharing methods		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.7 IRIS Enhanced MeliCERTes platform. The practical evaluation will be performed in WP7 Pilot Use Cases.		

ID	T_USAB-EME-02	Priority	MUST
Name	*MeliCERTes dashboard*		
Description	Provide customized views of its dashboard and security incident reporting capabilities, access control and access rights to shared data in accordance to the type of user/operator and the type of service /infrastructure they provide.		
Rationale	Customised MeliCERTes dashboard based on stakeholders needs.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.7 IRIS Enhanced MeliCERTes platform. The practical evaluation will be performed in WP7 Pilot Use Cases.		

ID	T-SECU-EME-03	Priority	MUST
Name	Access control and Access rights capabilities		
Description	Provide access control and access rights to shared data in accordance to the type of User/Operator and the type of Service/Infrastructure they provide.		
Rationale	Access Control rights are important for security of the system.		
Parent	FUNC-EME-07		

Dependency	FUNC-EME-01
Traceability	This requirement will be tracked in D4.7 IRIS Enhanced MeliCERTes platform. The practical evaluation will be performed in WP7 Pilot Use Cases.

5.2.5 Data Protection and Accountability (DPA) Module

5.2.5.1 Advanced real-time data protection and recovery

ID	T_SECU-DPA-01	Priority	MUST
Name	*Data Encryption/Decryption tool*		
Description	Requires being able to investigate the usage of encryption schemes such as self-encryption (SE) to provide end-to-end encryption to the privacy toolkit.		
Rationale	Provides the data encryption and decryption		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 IRIS Secure Crypto Functions for Data Management and D4.6 IRIS DLT-based control services for accountability, traceability, and auditing. The evaluation will be detailed in D7.5 IRIS Pilot Evaluation Report.		

ID	T_SECU-DPA-02	Priority	MUST
Name	*Digital Signature for authentication*		
Description	Requires being able to use a lightweight cryptographic digital signature (DS).		
Rationale	Provides the data authentication		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 IRIS Secure Crypto Functions for Data Management and D4.6 IRIS DLT-based control services for accountability, traceability and auditing. The evaluation will be detailed in D7.5 IRIS Pilot Evaluation Report.		

ID	T_SECU-DPA-03	Priority	MUST
Name	*Anonymous encryption*		
Description	Requires being able to use anonymous encryption and signature schemes to “hide” the identities either in a group of users or in encryption/decryption and signature keys.		
Rationale	Capability for the data signature and encryption with hidden IDs.		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 IRIS Secure Crypto Functions for Data Management and D4.6 IRIS DLT-based control services for		

	accountability, traceability and auditing. The evaluation will be detailed in D7.5 IRIS Pilot Evaluation Report.

ID	T_SECU-DPA-04	Priority	MUST
Name	*Data Recovery Tool*		
Description	Capability to support data recovery, by using a secret sharing (SS) scheme.		
Rationale	Ensures data recovery		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 IRIS Secure Crypto Functions for Data Management and D4.6 IRIS DLT-based control services for accountability, traceability and auditing. The evaluation will be detailed in D7.5 IRIS Pilot Evaluation Report.		

5.2.5.2 DLT-based accountability, auditing and traceability

ID	T_PLAT-DPA-05	Priority	MUST
Name	*Offline Data Storage with DLT*		
Description	Capability to combine a cloud-based storage system with a DLT.		
Rationale	DLT controlled cloud-based storage		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 IRIS Secure Crypto Functions for Data Management and D4.6 IRIS DLT-based control services for accountability, traceability and auditing. The evaluation will be detailed in D7.5 IRIS Pilot Evaluation Report.		

ID	T-PLAT-DPA-06	Priority	MUST
Name	*Off-chain data*		
Description	Capability for the event logs for the collaborative threat intelligence network interactions to be stored on off-chain databases, using Cloud-based storage system. The ledger should only store data pointers which securely link to the cloud storage system.		
Rationale	Guarantee IRIS systems interactions data privacy		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 IRIS Secure Crypto Functions		

	for Data Management and D4.6 IRIS DLT-based control services for accountability, traceability and auditing. The evaluation will be detailed in D7.5 IRIS Pilot Evaluation Report.

ID	T-PLAT-DPA-07	Priority	MUST
Name	*Consensus mechanism*		
Description	Prior to data storage in the ledger, a block data validation process will be followed via an appropriate consensus mechanism.		
Rationale	Guarantee correctness of data stored		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 IRIS Secure Crypto Functions for Data Management and D4.6 IRIS DLT-based control services for accountability, traceability and auditing. The evaluation will be detailed in D7.5 IRIS Pilot Evaluation Report.		

ID	T-PLAT-DPA-08	Priority	MUST
Name	*Interaction - Ledger Query API*		
Description	Provide API for allowing querying the ledger to be implemented. Holders of the appropriate keys will be able to access to the data.		
Rationale	Allow ledger querying		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 IRIS Secure Crypto Functions for Data Management and D4.6 IRIS DLT-based control services for accountability, traceability and auditing. Also, D6.1 APIs and Data Models for the integration of Smart City's infrastructure with the IRIS platform. The evaluation will be detailed in D7.5 IRIS Pilot Evaluation Report.		

ID	T-PLAT-DPA-09	Priority	MUST
Name	*Interaction - Stakeholder interaction smart contract*		
Description	Provide a smart contract, enabling stakeholders' interaction with the ledger, will be implemented. This smart contract will enable stakeholder's authentication and will capture their behaviour and operations. This smart contract will also ensure event log and attestation history to be traceable, immutable, and end-to-end transparent to authenticated partners.		

Rationale	Allow secure stakeholder's interaction with DLT
Parent	No parent
Dependency	No dependencies
Traceability	This requirement will be tracked in D4.5 IRIS Secure Crypto Functions for Data Management and D4.6 IRIS DLT-based control services for accountability, traceability and auditing. The evaluation will be detailed in D7.5 IRIS Pilot Evaluation Report.

ID	**T-PLAT-DPA-10**	**Priority**	**MUST**
Name	*Interaction - API for IRIS modules*		
Description	Provide an API for proper interaction with other IRIS modules that will be in place. This API will identify data read's and write activities.		
Rationale	Allow data collection from IRIS modules		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 IRIS Secure Crypto Functions for Data Management and D4.6 IRIS DLT-based control services for accountability, traceability and auditing. Also, D6.1 APIs and Data Models for the integration of Smart City's infrastructure with the IRIS platform. The evaluation will be detailed in D7.5 IRIS Pilot Evaluation Report.		

ID	**T-SECU-DPA-11**	**Priority**	**MUST**
Name	*Permission ledger access to external partners*		
Description	Capability to dynamically extend permissioned ledger access to external partners on-demand.		
Rationale	Part of the requirements of the DPA		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 IRIS Secure Crypto Functions for Data Management and D4.6 IRIS DLT-based control services for accountability, traceability and auditing. The evaluation will be detailed in D7.5 IRIS Pilot Evaluation Report.		

ID	**T-SECU-DPA-12**	**Priority**	**MUST**
Name	*Stored data protection*		
Description	The DLT will leverage data protection functions/encryption systems to		

	protect stored data.
Rationale	Guarantee protection of stored data
Parent	No Parent
Dependency	No Dependency
Traceability	This requirement will be tracked in D4.5 IRIS Secure Crypto Functions for Data Management and D4.6 IRIS DLT-based control services for accountability, traceability, and auditing. The evaluation will be detailed in D7.5 IRIS Pilot Evaluation Report.

ID	**T-SECU-DPA-13**	**Priority**	**MUST**
Name	*Private Network - membership authentication*		
Description	Appropriate membership authentication mechanism will be in place.		
Rationale	Guarantee appropriate authentication to the DLT		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 IRIS Secure Crypto Functions for Data Management and D4.6 IRIS DLT-based control services for accountability, traceability, and auditing. The evaluation will be detailed in D7.5 IRIS Pilot Evaluation Report.		

ID	**T-SECU-DPA-14**	**Priority**	**MUST**
Name	*Private Network - external partners access*		
Description	Capability to enable dynamically extending access to the permissioned ledger to external partners.		
Rationale	Guarantee appropriate authentication to the DLT		
Parent	No parent		
Dependency	No dependencies		
Traceability	This requirement will be tracked in D4.5 IRIS Secure Crypto Functions for Data Management and D4.6 IRIS DLT-based control services for accountability, traceability, and auditing. The evaluation will be detailed in D7.5 IRIS Pilot Evaluation Report.		

5.2.6 Virtual Cyber Range (VCR)

5.2.6.1 IRIS lab pods for CERTs/CSIRTs

ID	T_PLAT-VCR-01	Priority	SHOULD
Name	*Information Models*		
Description	Capability to leverage standardized YAML-based information models.		
Rationale	YAML-Based information models		
Parent	No parent		
Dependency	No dependencies		
Traceability	The deployment of the VCR will be tracked in D5.4 IRIS Cyber Range Platform. Results of the VCR will be reported in D7.5.		

ID	T_PLAT-VCR-02	Priority	SHOULD
Name	*Interfaces*		
Description	Capability to make extensive use of RESTful interfaces to simplify their runtime orchestration and will align with cloud-native principles.		
Rationale	RESTFul interfaces to simplify runtime orchestration.		
Parent	No parent		
Dependency	No dependencies		
Traceability	The deployment of the VCR will be tracked in D5.4 IRIS Cyber Range Platform. Results of the VCR will be reported in D7.5.		

5.2.6.2 IRIS Cyber Range Environment Platform and Dashboard

ID	T_PLAT-VCR-03	Priority	MUST
Name	*Access Requirements*		
Description	Capability to support multiple users working either independently over the same replicated infrastructure (or on different infrastructures) or cooperating as a team on a single target.		
Rationale	Enable multiple users in VCR.		
Parent	No parent		
Dependency	No dependencies		
Traceability	Scenarios for multiple users will be defined in D5.1. The deployment of the VCR will be tracked in D5.4 IRIS Cyber Range Platform. Results of the VCR will be reported in D7.5.		

ID	T_PLAT-VCR-04	Priority	MUST
Name	*Virtualization*		
Description	Capability to use security asset and IRIS component in a virtualized way (in VM or container)		
Rationale	Part of the requirements for virtualization of assets and SIEM.		
Parent	FUNC-VCR-07, FUNC-VCR-08		
Dependency	No dependencies		
Traceability	IRIS Scenario and Asset Catalogue will be defined in D5.2. The deployment of the VCR will be tracked in D5.4 IRIS Cyber Range Platform. Results of the VCR will be reported in D7.5.		

6 KEY PERFORMANCE INDICATORS FOR IRIS PLATFORM VALIDATION

In this chapter the KPIs for each of the IRIS modules have been defined.

6.1 Automated Threat Analytics and Detection

ID	ATA _KPI_01
Name	Threat Detection – Actions
KPI Description	The Threat detection module will be able to detect at least 3 types of cyber-attacks, example: Rogue IoT Devices and Sensors, DoS, ML-Evasion,
Linked Requirements	FUNC-ATA-01, FUNC-ATA-06, T-PLAT-ATA-O1
Assessment	Action: Demonstrate on PoC the ability to block attacks. Output Report: Report of IRIS Platform validation in WP7 (M28-36).

ID	ATA _KPI_02
Name	Risk-based response – Response Action Updates
KPI Description	For each new detected attack risk-based response will provide the capability to dynamically update/select response actions, based on changes in attack type severity, impact, victim system type.
Linked Requirements	T_PLAT-ATA-07,
Assessment	Action: Dynamic response action selection based on different detected attacks, exhibited in the pilot demonstrations. Output Report: Output Report: Report of IRIS Platform validation in WP7 (M28-36).

6.2 Collaborative Threat Intelligence and Orchestration

ID	CTI_KPI_01
Name	Incident Recovery Time
KPI Description	The CTI module will enhance incident recovery and will demonstrate a 20% reduction of average recovery time for incidents that involve IoT or AI.
Linked	

Requirements	
Assessment	Action: Recovery time for incidents that involve the IoT and AI systems in the PUCs will be assessed during the PUC demonstration. Output Report: Output Report: Report of IRIS Platform validation in WP7 (M28-36).

ID	**CTI_KPI_02**
Name	Efficiency and flexibility
KPI Description	Above 60% acceptance of IRIS's resource-efficiency and flexibility in IoT & AI security analytics and threat intelligence reported by CERTs/CSIRTs through questionnaires.
Linked Requirements	FUNC-CTI-12
Assessment	Action: Recovery time for incidents that involve the IoT and AI systems in the PUCs will be assessed during the PUC demonstration. Output Report: Output Report: Report of IRIS Platform validation in WP7 (M28-36).

ID	**CTI_KPI_03**
Name	Time to execute workflow
KPI Description	The orchestration workflow will show enhanced capability by enabling more timely propagation of threat indicators than manual workflows (with the same number of steps).
Linked Requirements	FUNC-CTI-09
Assessment	Action: Assessment of the performance of the orchestration workflow manager will be conducted in the PUC demonstrations. Indicators for assessing performance will be developed in Task 7.1. Timeframes for propagation of indicators of compromise will be compared between manual and orchestration workflows. Output Report: Output Report: Report of IRIS Platform validation in WP7 (M28-36).

6.3 Data Protection, Accountability and Auditing

ID	DPA – KPI-01
Name	API performance MS6
KPI Description	For all DLT APIs, DLT APIs performance (latency and throughput) is fully achieved (more than 85%) by month 34 (MS6).
Linked Requirements	FUNC-DPA-01, FUNC-DPA-10
Assessment	Output Report: Initially detailed in D4.6[[M26] and D4.7[M28] detailing the IRIS-DLT based components and the IRIS-enhanced MeliCERTes platform. Final results will be included in report of IRIS Platform validation in WP7 (M28-36).

6.4 Hands-on, Collaborative and Immersive Cybersecurity Training

ID	VCR – KPI_01
Name	Virtual Cyber Range scenario capability
KPI Description	The Virtual Cyber Range will be able to replicate to over 90% a predefined scenario of at least 4 steps.
Linked Requirements	T_PLAT-VCR-01 FUNC-VCR-05 FUNC-VCR-06 FUNC-VCR-07 FUNC-VCR-09 FUNC-VCR-10
Assessment	Output: D5.2 and D5.3 IRIS lab pods or CERTs/CSIRTs, report on how each of the different IRIS components have been replicated in the VCR.

7 STATE-OF-THE-ART KEY TECHNICAL INTEGRATION AREAS

This chapter presents a state-of-the-art for key technical of the IRIS Platform architecture. These key technical areas have been identified as:

1. Threat Analytics
2. Collaborative Threat Intelligence
3. Threat Intelligence Orchestration
4. Data Protection Accountability and Auditing
5. Cyber Ranges

The aim of the state-of-the-art is to provide guidance to the IRIS system co-design process of task 2.5.

7.1 Threat Analytics

Detecting attacks against IoT and AI-provisions introduces a unique challenge for traditional proactive threat detection systems, such as network or host-based intrusion detection systems. Attacks against IoT systems often take advantage of a lack of inherent security in their data generation and consumption and the inherent embedded and static nature of their operation, whereas for AI provisions attacks are subtly interweaved in input data that is designed to disrupt or confuse their decision making
process.

Detection of adversarial threats against machine learning systems has become a crucial security capability as the proliferation of AI-provisions in smart transport systems, predictive maintenance, economic and environmental monitoring increases the potential for these systems to be compromised. Existing development for defence against adversarial AI focuses heavily on protecting the training phase of AI to provide detection measures that improve the resilience of the AI platform against adversarial samples that would poison or evade its model-based logic and affect its performance. Recent advancements have explored hybrid adversarial detection mechanism for training and inference, whereby similarity-based detection of benign and malicious apps is employed at inference time to update training samples for improving the detection robustness of the ML classifier, once it is retrained. This is a promising concept but does not address the challenge of identifying real-time malformed or spoofed content that systematically confuses or poisons the decision-making processes of an AI system, outside of its training process. There is a gap in detection capabilities that address real-time training and inference (e.g., online AI), where the process of analysis and filtering of malicious data points needs to be continuous. While various methods for AI threat detection have

been devised, none of these systems formulate detected threats into structured threat intelligence. This prevents the timely sharing of threat analytics with security teams monitoring similar systems.

To address this challenge, IRIS will extend the capabilities of traditional intrusion detection systems to monitor the unique characteristics of IoT and AI-provision, such as the data they consume and generate, as well as their responses to different technical workflows and interactions between them. IRIS will develop "sentinel" machine learning anomaly classifiers for IoT, and AI that will monitor for abnormal deviations in behavioural data telemetry and decision response. The autonomous threat analytics engine will employ a threat-intelligence enriched knowledge-framework to monitor attack patterns against IoT infrastructure and AI-provisioned systems.

The automated threat analytics and detection engine of IRIS will apply data-driven and intelligent AI monitoring techniques holistically to continuously assess the normal behaviour of devices, systems, and their data footprint. IRIS will develop retrofittable "sentinel" machine learning models to passively assess IoT and AI-systems' data, bidirectional control system commands, and device actuation/response events. Its AI-driven detection and analytic modules will embed detection with specific AI training processes, statistical and probabilistic correlations between source system data and AI-decision output to derive anomalies related to data payload that may poison or evade the AI model logic. The detection classifiers will continuously evaluate behavioural data profiles of system telemetry and establish temporal patterns in different data telemetry "signatures". These capabilities will be combined to develop collaborative-threat analytic models of IoT and AI processes and infrastructure, and independent IoT and AI systems for establishing the source, type, and target of attacks (e.g., IoT device à AI model poisoning à AI Control System Process). To facilitate efficient propagation and ingestion of threat detection analytics, the detection engine will include extensible APIs that support the translation of detection parameters into structured IoC and schema derived from the CTI open taxonomy for IoT and AI repositories. It will ensure detections can be shared in an actionable format, amongst CSIRTs/CERTs with consistent data standards for incident response. The advancement of the state-of-the-art addresses a gap between detection of threats and systematic, automated orchestration of their indicators, with a toolkit that allows CSIRTs/CERTs to define the programmability of the detection analytics workflow. The detection engine API will provide simple interfaces for updating IoT & AI threat detection engine models and heuristics with IoCs and detection parameters received from external threat intelligence sources in the IRIS-enhanced MeliCERTes ecosystem.

7.2 Collaborative Threat Intelligence

7.2.7 Cyber Threat Intelligence Landscape

In today's connected world, attackers can harm and attack different devices and organisations by using a plenary of tools. The cyber-attacks generated by the attackers inflict harm to individuals and organisations and put their normal daily operations at risk. To defend against these attacks, the latter use different defence methods such as Intrusion Detection Systems (IDS) that are constantly looking for artefacts that can reveal an attacker's actions. For example, an IDS system can observe an IP that seems to cause abnormal behaviour to an organisations system. These artefacts, generally known as Indicator of Compromise (IoC), offer basic information about an attack, which is insufficient to observe the rapidly changing landscape of cyber-attacks. As a response, Tactics, Techniques and Procedures (TTPs) can describe in a more general way the actions of the attackers and are considered a powerful way to defend against them [1][2].

Cyber Threat Intelligence (CTI) generated from IoC and TTPs offer the organisation the opportunity to mitigate the damages caused by attackers. However, CTI appears in formats that do not directly provide defence advantages, and more steps are needed to gain all its benefits [1][2]. As stated by Dalziel et al., CTI must be refined, analysed, and processed to be relevant, actionable, and valuable [3].

7.2.8 Cyber Threat Intelligence Lifecycle

CTI life cycle consists of different distinct steps. First, the relevant sources of information must be identified. These sources are generally composed of threat information captured by security and monitoring tools. Threat information can be collected from sources in an organisation's internal and external environment [4]. Internal sources can be considered information generated by security tools like intrusion prevention systems (IPS), firewalls, host security systems (anti-virus), and others. Computer forensic analysis identifying IoC on operation systems can also offer valuable internal data sources.

On the other hand, external sources are not located in an organisation's operational environment. They can be categorised as public and private, given the degree of accessibility. Unindexed is one more external source category and includes sites accessible only from the deep or the dark web (e.g., chatrooms, forums, marketplaces) [4].

7.2.9 Collection of Internal Sources

Internal sources entail events in an organisation's internal network and hosts. These sources can indicate threats that have passed the security perimeter, infected a system, or tried to enter a restricted system. In general, different internal sources can be identified, such as system logs and events, network events, network utilization and traffic profiles, boundary security devices, anti-virus systems, human and forensic [5].

Internal information can be combined from different logs files such as system and database logs and can even help identify unknown vulnerabilities (zero-days). Event information such as accessed file paths and executed commands is not the only valuable log data information. Sometimes logs entail information that highlights the execution artefacts of events, such as IDs of associated users and the associated context information generated. The time constant is quite beneficial also because a variety of processes are timed or periodically recurring. Other information includes the source of the log event, log sensor data such as ID, location, or manufacturer, and system data [5][6]. Also, the various internal data can reveal the behaviour of attackers or groups of individuals behind an attack. High-level information generated from them, such as TTPs, can make it more difficult for them to change their behaviour and avoid detection. One more benefit of internal information is that it can detect the time interval of attacks (i.e. threats that have already violated a system or are constantly running). The identification of the time-interval is quite beneficial and crucial as it can determine the degree of damage that can provoke to an organisation [5][6].

Honeypots can be utilized in the collection procedure of internal data. Honeypots can be considered simulation environments that can detect the tools and methods that an attacker uses without suffering from the damage commonly caused to a system due to a malicious attack. A honeypot can be defined as an intentionally vulnerable computer system that creates a virtual trap to lure attackers. The term “honeypot” was coined by Spitzner [7], who defined honeypot as a “security resource whose value lies in being probed, attacked, or compromised”. Honeypots are very efficient in terms of the defence procedure of an organisation, such as prevention, detection, and reaction. They can be considered valuable tools in today’s rapidly changing cyber-crime environment [8]. Honeypots can be categorised based on the intended use and the interaction level between an attacker and a system [7][9]. They can be used either for research or production objectives. Low and high interaction honeypots can describe an organisation's damage tolerance level. More specifically, honeypots can access a small number of services or allow more interactions.

CTI from internal log data is highly valuable; however, different problems hide their applicability some challenges. For example, automated log parsing is not a straightforward procedure as log data may appear in human-readable syntax [1]. In contrast to the external sources, the documentation procedure of the collected information can also be considered a challenge. The specific characteristic of an organisation and the different challenges on the collection process harden the whole procedure [10].

7.2.10 Collection of External Sources

Site scraper, web crawlers or API calls to the data source can collect information from external sources [11] [12]. In today’s connected world, valuable information can be

identified not only from the typical internet environment that we usually operate (i.e., surface web) but also from the fraction of the internet that is now directly visible such as the deep and dark web. In this situation, web crawlers can be valuable and provide several advantages. In its basic operation, a crawler visits a URL address and downloads a webpage. Subsequently, it extracts the addresses found in the URL, compares them with a list of visited URLs and adds the non-visited ones to its frontier list. This procedure is repeated for all the domain ranges or sub-domain until fully crawled [11]. Various features such as crawling application, the hardware, and the ability to scale/expand the existing infrastructure can assist in the categorization of crawlers [13][14]. More specifically, three categories are centralised, hybrid: parallel/distributed, and Peer-to-peer.

7.2.11 Cyber Threat Extraction

The next step of the CTI life cycle is intelligence extraction from data collected through external or internal sources. For this step, rule-based and machine learning-based analysis techniques can be used. Information that is collected from internal sources follows a structured format. In general, defence methods such as security monitoring systems can identify IoC and extract knowledge for the attackers by leverage [1] [15]. Furthermore, machine learning techniques such as pattern identification and analysis and anomaly detection can extract valuable CTI from the collected data [1]. On the other hand, data collected from external sources follow a semi-structured or unstructured format. In this case, regular expressions and heuristic approaches can be used.

7.2.12 Cyber Threat Intelligence Correlation

After identifying sources, gathering information, and extracting CTI from internal and external sources, one more critical step is the enrichment of the data using correlation techniques. For that, rule-based correlations are used. Correlation can extract not feasible relationships between different attacks or attacks executed by one person. The TTPs that are generated can assist in a more advanced identification of the action of an attacker.

7.2.13 Cyber Threat Intelligence Sharing

The last part of the CTI cycle is the sharing of information. This procedure is critical as it enables different interested parties (CERTs, CIRTs etc.) to be timely informed about the cyberattack landscape. Various tools or platforms exist that facilitate the sharing of CTI information, such as OpenCTI2, MISP3 and GOSINT4. Among them, the MISP platform

[2] https://www.opencti.io/en/
[3] https://www.misp-project.org/

has gained popularity from cybersecurity professionals. MISP can also be used to store the data. This is useful as it can depict semantic information of various data generated over time. Information visualizations and keyword-based searches capabilities are also essential characteristics of the MISP platform.

7.2.14 Malware Information Sharing Platform (MISP)

Several threat intelligence platforms have been proposed for the collection and sharing of information. Several of them support the collaboration among organisations and CERTs/CSIRTs. MISP[5] is an open-source threat information platform, for collecting, storing, distributing and sharing cyber security indicators and threats about cyber security incidents analysis and malware analysis. In this manner, various communities are able to share all kind of cyber-threats, indicators of compromise. The goal of MISP is to facilitate the sharing of structured information, within the security community.

MISP supports the insertion, gathering, and sharing of threat intelligence information, either manually through a GUI or automatically through its API, PyMISP. It allows the collaboration among the MISP community to efficiently defend against cyber threats. The users are able to determine the granularity of the information they want to distribute in MISP, for instance with respect to the organization level, the community-level, or within their sharing groups. Information that is shared/ distributed through MISP is called an *event*. An event is composed of a list of attributes, including destination IP addresses and file hashes. An attribute is identified with the tuple (category, type, value).

MISP is envisaged to assist the development of IRIS's Collaborative Threat Intelligence sharing and orchestration platform. In addition, it is a significant actor of the envisioned IRIS Enhanced MeliCERTes platform that will be developed within IRIS.

7.2.15 MeliCERTes Core Service Platform

MISP is used in MeliCERTes. MeliCERTes CSP (https://github.com/melicertes/csp), co-developed by INTRA (in the context of the SMART 2015/1089 tender call and awarded project [EC19]) to provide such capabilities in a distributed architecture (i.e., different instances running at the infrastructure of different authorities) – the target users have been CERT/CSIRT authorities. MeliCERTes CSP is a modular platform that interlaces various services that not only offers a complete security incident management solution but also allows CSIRTs to share information and collaborate with each other within verified Trust Circles. A follow up project has been funded to be extended and adopted by the relevant authorities – MeliCERTes 2. In the context of IRIS project, MeliCERTes 2

[4] http://gosint.readthedocs.io/en/latest/
[5] https://www.mispproject. org/

technical activities will be investigated in order to form a strong base for the implementation of the IRIS enhanced ecosystem.

7.2.16 OpenCTI

OpenCTI[6] is an open source cyber threat intelligence platform, following a community-centred approach. OpenCTI objectives include, CTI storage, organization, visualization and sharing. Through observables (e.g TTPs) and indicators of compromise OpenCTI aims to create a comprehensive tool providing both non-technical and technical information, linking each piece of information to its primary source (e.g. MISP event. Furthermore, OpenCTI provides:

Knowledge management database: which incorporates an enforced schema especially tailored for cyber threat intelligence and cyber operations. In addition, it provides multiple tools and viewing capabilities, analysts are able to explore the whole dataset by pivoting on the platform between entities and relations.

Data Visualization: OpenCTI allows analysts to easily visualize any entity and its relationships. Multiple views are available as well as an analytics system based on dynamic widgets. However, currently Cyber Threat investigation capabilities are considered limited but will be improved in the future.

7.2.17 Anomali Threat Platform

Anomali Threat Platform[7], is the commercial counterpart of OpenCTI and offers an integrated suite that is designed to help organizations identify cybersecurity threats, investigate adversaries and respond efficiently and effectively. Anomali, utilized STIX[8], an OASIS standard for representing the cyber threat related information and equips security teams with threat intelligence from premium feeds such as OSINT, STIX/TAXII and ISACs. Within Anomali suite, threats and events receive a severity level score as well as a confidence score. Analysts can delve into each event for more information, such as whether an active threat is underway, what type of threat it is and the like. The solution shows all ingested data and matches it to each indicator of compromise. Anomali platform offers enterprises a single, centralized environment for the collection, management, integration and analysis of all cyber threat intelligence which might be considered a limitation int the context of the IRIS project.

[6] https://www.opencti.io/en/
[7] https://www.anomali.com/
[8] https://oasis-open.github.io/cti-documentation/stix/intro.html

7.2.18 Additional CTI Platforms:

The **GOSINT framework**[9]**:** The GOSINT framework is a project used for collecting, processing, and exporting high quality indicators of compromise (IOCs). GOSINT allows a security analyst to collect and standardize structured and unstructured threat intelligence.

Palo Alto Networks' MineMeld[10] supports the aggregation, correlation, and deduplication of threat intelligence extracted from the feeds of CERTs and ISACs, the enforcement of new prevention controls (i.e. IP blacklists), the evaluation of the feeds' value to an organisation, the extraction and sharing of indications from syslog messages.

EclecticIQ platform[11]**:** consolidates, normalises, and de-duplicates threat intelligence from open-source communities and commercial intelligence suppliers. To organise and enrich the collected threat intelligence, taxonomies are often employed.

7.2.19 Open CTI ontologies and Taxonomies

Within IRIS, Threat Analytics and detection engine aims to facilitate efficient propagation and ingestion of threat detection analytics, thus the detection engine will include extensible APIs that support the translation of detection parameters into structured IoC and schema derived from the CTI open taxonomy for IoT and AI repositories.

In addition, IRIS envisages a dynamic knowledge repository on evolving threats that specifically target IoT and AI-enabled ICT systems. The aim of this repository will be to both facilitate the detection of these threats and support the relevant communication procedures.

NISTIR Taxonomy

To facilitate the enrichment of the knowledge base, the repository will be based on existing taxonomies and ontologies related to threats targeting IoT and AI-based systems, such as those already defined by the U.S National Institute of Standards and Technology - NIST (Draft NISTIR 8269).

NISTIR 8269, provides a taxonomy and terminology of Adversarial Machine Learning with the goal of securing applications of Artificial Intelligence (AI), especially against adversarial manipulations of Machine Learning (ML), by developing a taxonomy and terminology of Adversarial Machine Learning (AML). The taxonomy is arranged in a conceptual hierarchy that includes key types of attacks, defenses, and consequences. The terminology, arranged in an alphabetical glossary, defines key terms associated with the

[9] https://github.com/ciscocsirt/GOSINT
[10] https://github.com/PaloAltoNetworks/minemeld
[11] https://www.eclecticiq.com/platform

security of ML components of an AI system. This taxonomy is very relevant and aligned with the cybersecurity related activities that IRIS aims to tackle and ultimately address.

STIX Ontology

In IRIS, the abovementioned CTI threat analysis and sharing techniques will be driven by secure and efficient security information representation in standardized formats capitalizing and extending existing ontologies, such as **STIX 2.1**[12]

STIX: Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI). STIX enables organizations to share CTI with one another in a consistent and machine-readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively. STIX is especially designed to promote collaborative threat analysis and automated detection, sharing and response.

STIX is a connected graph of nodes and edges. STIX Domain Objects and STIX Cyber-observable Objects define the graph nodes and STIX relationships (including both external STIX Relationship Objects and embedded relationships) define the edges. This graph-based language conforms to common analysis approaches and allows for flexible, modular, structured, and consistent representations of CTI.

STIX is a schema that defines a taxonomy of cyber threat intelligence that is represented by STIX core and Meta objects. Indicatively these objects include among others CTI information that are related to the vulnerability, threat, asset, countermeasure and mitigation actions etc.

Although STIX 2.1 is transport-agnostic, i.e., the structures and serializations do not rely on any specific transport mechanism, a companion CTI specification, TAXII[13] is designed specifically to transport STIX Objects over HTTPS.

Finally, the adoption of standardised data models, like the one defined in STIX, and standardised interfaces, like TAXII or RESTful APIs that will be exposed by the IRIS developed components can assure wider adoption of the IRIS and accelerate its integration with already existing systems.

[12] https://oasis-open.github.io/cti-documentation/stix/intro.html
[13] https://oasis-open.github.io/cti-documentation/taxii/intro.html

7.3 Threat Intelligence Orchestration

Threat Intelligence Orchestrator can be provided as a drastic solution in a cyber-threat challenging world since it not only manages cyber-threat information and processes in IoT and AI-enabled infrastructures, but it also secures smart ecosystems by facilitating threat and vulnerability management, security incident response, and security operations automation. This technical solution adheres to security, orchestration, automation, response (SOAR) capabilities. SOAR capabilities can be benefit by relying on SIEM system's information and leverage on it, by automation and orchestration.

7.3.1 SOAR Definition

As it is referred by Gartner Glossary[14] "SOAR refers to technologies that enable organizations to collect inputs monitored by the security operations team. For example, alerts from the SIEM system and other security technologies — where incident analysis and triage can be performed by leveraging a combination of human and machine power — help define, prioritize and drive standardized incident response activities. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format".

7.3.2 SOAR Commercial and Open-Source Solutions

There are many already existed market-oriented and open-source solutions. Gartner's 2020 SOAR market guide[15] entails a list of representative vendors and their products, including the following: Anomali ThreatStream, Cyware Virtual Cyber Fusion Center, D3 Security D3 SOAR, DFLabs IncMan SOAR, EclecticIQ Platform, FireEye Helix, Fortinet FortiSOAR, Honeycomb SOCAutomation, IBM Security Resilient, LogicHub SOAR+, Micro Focus ArcSight SOAR, Palo Alto Networks Cortex XSOAR, Rapid7 InsightConnect, ServiceNow Security Operations, Siemplify SOAR Platform, Splunk Phantom, Swimlane SOAR, ThreatConnect SOAR Platform, ThreatQuotient ThreatQ, Tines. The open source community is also providing solutions for the Security Orchestration domain. The more interesting and mature is the Shuffle Open-Source platform supports thousands of premade integrations using open frameworks like OpenAPI to ease migration.

Some of the common characteristics of SOAR enabled tools including, workflow automation, incident response playbooks, open plugin framework, case management visual environment, intuitive user interface etc. Furthermore, the benefits arise are prioritizing security operations activities, formalizing triage and incident response, immediate incident detection and automating response, collaboration interface,

[14] https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar
[15] https://www.splunk.com/en_us/form/gartner-soar-market-guide-2020.html

simplified management and streamlining operations, scalability of the system etc. As a result, of the above, security operations teams can be benefit and

- automate iterative response processes,
- time savings for higher priority sorting tasks, and
- a standardized, easy-to-follow response.

The IRIS project will investigate some of the referred tools in D4.3 in order to learn from their innovative assets and capabilities.

7.4 Data Protection, Accountability and Auditing

In this task of the IRIS project, data protection is provided by the combination of self-encryption, secure data sharing schemes, and distributed ledger technology.

7.4.1 Self-Encryption

David Irvine from MadeSafe group [16] published the first data self-encryption scheme [17], which is based on a convergent encryption technique. The main aim of the self-encryption scheme is to encrypt data without user intervention or password. An open-source implementation of self-encryption programmed in Rust is available on GitHub and can be reused freely [18]. The self-encryption contains three main steps (see Figure 2).

The first step is the data chunk creation, in which the initial data (plaintext) is divided into identical data chunks.

The second step contains three main phases. The first phase is computing the hash values for each of the chunks. The cryptographic hash value of a chunk is the unique representation or the so-called digital fingerprint [19] [20] of the chunk. In practice, the hash value is at least 256 bits long; for example, SHA [21], Keccak [22], or Blake2 [23] cryptographic hash function families can be applied in order to calculate the corresponding hash values. The AES-128 block cipher [24] is used to encrypt all data chunks, which requires a secret key (Key) of 16 bytes and an initialization vector (IV) of 16 bytes.

The second phase of the second step is the generation of the secret keys and the initialization vectors for chunks' encryption. The hash values computed in the previous phase are used to create the initialization vectors and keys. For encrypting chunk (C_n), the previous chunk's (C_{n-1}) hash is required for the AES block cipher function. The first 16 bytes of the previous chunk's (C_{n-1}) hash value serves as the key and its last 16 bytes as the initialization vector for the AES block cipher. Obfuscation values (X_n) must also be computed for all chunks at this same phase. The obfuscation value corresponding to chunk (C_n) is determined by concatenating the hash of the current chunk (C_n) and the hash of the first of the two previous chunks (C_{n-2}).

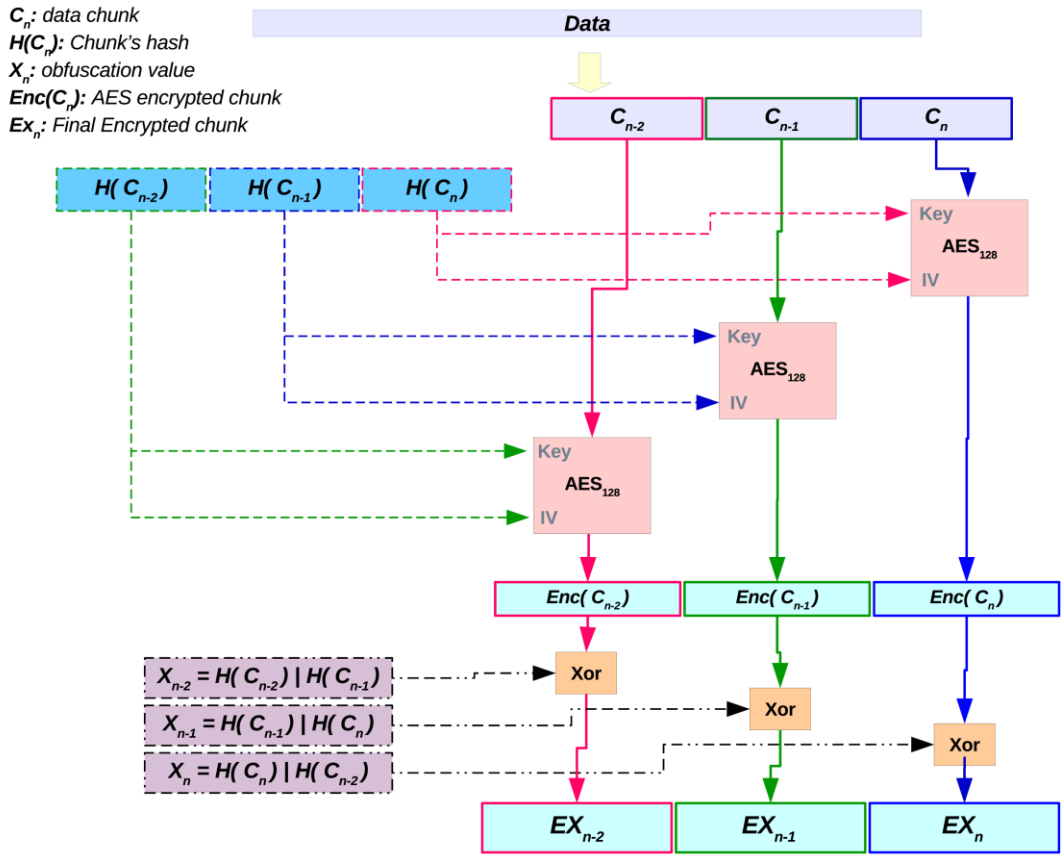


Figure 3. Diagram of self-encryption's principle

The third phase of the second step is the AES encryption of the chunks using the corresponding keys and initialization vectors.

After obtaining the encrypted chunks, obfuscation is applied to each of the AES encrypted chunks (e.g., $Enc(C_n)$). In this last step of the self-encryption, the encrypted chunks are Xor-ed with the obfuscation values computed in the previous step in order to obtain the final encrypted chunks (e.g., EX_n). It must be noted that one obfuscation value (e.g., X_n) is 64 bytes long, contrarily to the size of one AES encrypted chunk, which can be higher than 64 bytes. If the AES encrypted chunk's size exceeds 64 bytes, the obfuscation value is rotationally padded by itself until it achieves the same length as the AES encoded chunk's size.

$H(C_1)$	**$H(EX_1)$**
...	**...**
$H(C_n)$	**$H(EX_n)$**

Table 2. Data Map

The last stage of the self-encryption is the data map creation, which can be represented as a table (see Table 2). The left column of the table contains the hashes of the data chunks, which are required in order to be able to determine the keys and initialization vectors (IV). The data chunks' hashes can be considered the secret keys for the self-encrypted data, which means that these values should not be publicly shared. The right column of the table contains the hashes of the final encrypted chunks. The final encrypted data chunks' hash values can be considered the pointer to the final encrypted data chunks allowing their storage in different locations. Storing data chunks in different locations makes it harder to retrieve the totality of the chunks.

The main advantage of self-encryption is that all final encrypted data chunks and the totality of the keys (hashes of the data chunks, left column) are required to retrieve the initial data. If one of the final encrypted chunks could not be adequately decrypted or one of the keys misses, the concatenation of the decrypted chunks would not return the initial data (plaintext)

7.4.2 Secure Data Sharing

In practice, secure data sharing is used when multiple participants aim to securely share a secret (e.g., a secret key to decrypt a message). In most cases, the secret sharing (k, n) is applied, in which n is the number of participants and k is the threshold which is the minimum number of participants' keys required in order to retrieve the secret.

In particular, the Shamir's Secret Sharing Scheme [25] can be applied in order to share a secret (S_k). In this scheme, a $k-1$ degree polynomial $q(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}$ is used to share the secret, which is equal to the coefficient $a_0 = q(0) = S_k$ of the polynomial. The other coefficients $a1 \dots a_{k-1}$ of the polynomial are generated randomly.

In the scheme, n keys are calculated by the polynomial $(D_1 = q(1), D_2 = q(2), \dots, D_n = q(n))$, which are distributed among the n participants. The secret can be retrieved when at least k participants provide their keys.

An open-source Golang implementation is available on GitHub [26].

7.4.3 Distributed Ledger Technology

The Distributed Ledger Technology (DLT), considered at the time most fitted for the project, is the Hyperledger Fabric [27] private blockchain, which provides the data immutability, transparency, and traceability of all of the blockchain's events.

Hyperledger Fabric blockchain provides a permissioned architecture in which only the known and identified members can participate. Thanks to the so-called Certificate Authorities, the members' identities can also be securely provided. This blockchain is also known as an enterprise blockchain that provides a secure environment to a complete ecosystem in which the operations or business logic of the given use case can be automatized and done thanks to a common agreement. The operations in question can be executed in a secure environment using so-called chain codes or smart contracts.

Smart contracts are digital codes or programs that can be deployed to the blockchain via transactions and can be executed according to specific events on the blockchain. The interaction with the smart contracts and their deployment can be done by using a common agreement called consensus rule. In the case of Hyperledger Fabric, the Practical Byzantine Fault Tolerance (PBFT) [31] is applied as the default consensus rule; however, thanks to Hyperledger Fabric's modularity, the consensus rule can be replaced by other existing ones.

There are several other private and permissioned DLT that could be used on this project. Among them, we highlight the following ones:

- Quorum [28];
- Hyperledger Sawtooth [29];
- Hyperledger Iroha [30].

The main differences between them, including Hyperledger Fabric, are the consensus mechanisms that can vary among them, as well as some other privacy features. The consensus mechanism depends highly on the number of nodes operating within the network.

7.4.4 Combination of Self-Encryption, Secret Sharing and DLT

It can be noted that the cryptographic schemes and the blockchain technology described previously have several advantages. These schemes and technology could be brought together to achieve more secure data protection and accountability.

The self-encryption performs a data map (see Table 2) that contains the secret keys (data chunks' hashes) and the final encrypted data hashes. It must be noted that the secret keys cannot be shared publicly; therefore, Shamir's Secret Sharing could be applied to all of the keys produced by the self-encryption scheme. By applying the secret sharing, a threshold of participants' keys can be required to be able to retrieve the secret keys which are needed to decrypt the self-encrypted data.

On the one hand, blockchain technology combined with the mentioned cryptographic schemes can provide the traceability of the operations by specific smart contracts and APIs.

On the other hand, the hash values of the final encrypted data chunks provided by the self-encryption can be stored on the blockchain. These hash values are the pointers (references) to the final encrypted data chunks, which can be stored on a Cloud infrastructure or on a distributed file system such as InterPlanetary File System [29]. Thanks to the data immutability provided by the blockchain, these hash values cannot be modified or deleted.

Retrieving the final encoded data chunks from their hash values can also be done automatically using specific smart contracts and APIs.

7.5 Cyber Ranges

Cyber ranges are defined as an interactive and simulated representation of a local network. They provide a safe environment to test and exercise cyber skill for product development and security posture testing.

On a technical point of view a Cyber Range is characterized by:

- A multi-level computer simulation environment.
- Network topologies. The environment makes it possible to reproduce network topologies made up of several thousand, or even tens of thousands of nodes. If based on a traditional virtualization system, the novelty lies in the fact that the administrators can easily create and configure network architectures and host.
- Security technologies as firewalls, IPS / IDS, SIEM etc.
- Network traffic generators to inject legitimate or malicious traffic into the environment to create the noise present in any network.

On the human side, Cyber Range generally revolves around two distinct teams:

- The "red team", made up of professional hackers. These reproduce targeted attacks to challenge the defense according to its room for improvement throughout the training.
- The "blue team", responsible for the defense of networks and information systems, which is therefore made up of trainees participating in the training program.

Cyber range purpose is utilized for 3 main targets: research, training and exercises/ competition in cyber security.

Cyber range can be categorized into 3 types: simulation, emulation and hybrid and they all rely on virtualization. But there is two kinds of virtualization. Conventional virtualization such as containers (docker, lxc) and hypervisor (Vmware, qemu, virtualbox etc) and cloud virtualization such as Openstack, terraform, AWS with both, private and public clouds.

But the different Cyber range differ also by the kind of attack/ scenario and network they can simulate. They all are focus on different area. That why the concept of cyber range collaboration emerges, in order to cover a wide spectrum of situation.

Different equipment manufacturers offer Cyber Ranges or simulation environments dedicated to cybersecurity such as Diateam (France), Thales (France), Cyber Test Systems (France), ,Airbus (France) Cyberbit (Israel), Ixia (United States), Ravello Systems (United States) , Sypris (United States), IBM (United States), CybExer, Raytheon, Fujitsu etc..

Many cyber ranges come from universities and research institute. The most used are listed in [Cyber range and testbed for education, training, and research] and [A review of cyber-ranges and testbeds: Current and future trends].

Finally, there is also cyber range coming from European project as Kypo from Concordia European project [https://www.concordia-h2020.eu/kypo-cyber-range/].

8 THREAT PORTFOLIO FOR AUTONOMOUS THREAT ANALYTICS AND DETECTION

An initial threat portfolio has been established to build the basis for the development of the ATA module which is to be developed within Task 3.2 – Autonomous AI threat analytics and detection. Each of the threat portfolios is specific to the PUC focus of the smart city. This is detailed in the IRIS project as:

- **PUC 1 – Barcelona:** Cyber threats to ***confidentiality*** of Barcelona Smart City IoT and control systems.
- **PUC 2 – Tallinn:** Cyber threats to ***availability*** of Tallinn Smart City Autonomous Vehicle Shuttle transportation and AI enabled infrastructure.
- **PUC 3 – Helsinki:** Cyber threats to ***integrity*** of Helsinki Smart City Energy Grid data.

The cyber threat scenarios within each of the PUC will be used to evaluate the IRIS platform against attacks which encompass the information security triad, CIA (Confidentiality, Integrity and Availability).

8.1 PUC1 Barcelona: Threat Portfolio

The crucial assets involved in PUC1 are as follow:

- **NVIDIA Jetson:** System receiving information from Bosch IP Camera and applying Artificial Intelligence to detect physical situations like presence of cyclists and tram. Communication is done using a Netgear managed Fast Ethernet switch.
- **Bosch IP Camera:** Filming the tram stops for the presence of tram and cyclists and sending the information to the Jetson device for analysis. Communication is done using a Netgear managed Fast Ethernet switch.
- **Odroid:** System sending information and alerts using 802.11p to mobile tags present on Barcelona public bicycles alerting the presence of a tram.
- **Netgear switch:** Provides local connectivity between all the components located in the field and backhaul to send this information to I2CAT and BSC through Ca l´Alier hub where passive attack detection is installed.

Figure 4 displays the PUC 1 – Barcelona Smart City Sensor Architecture.

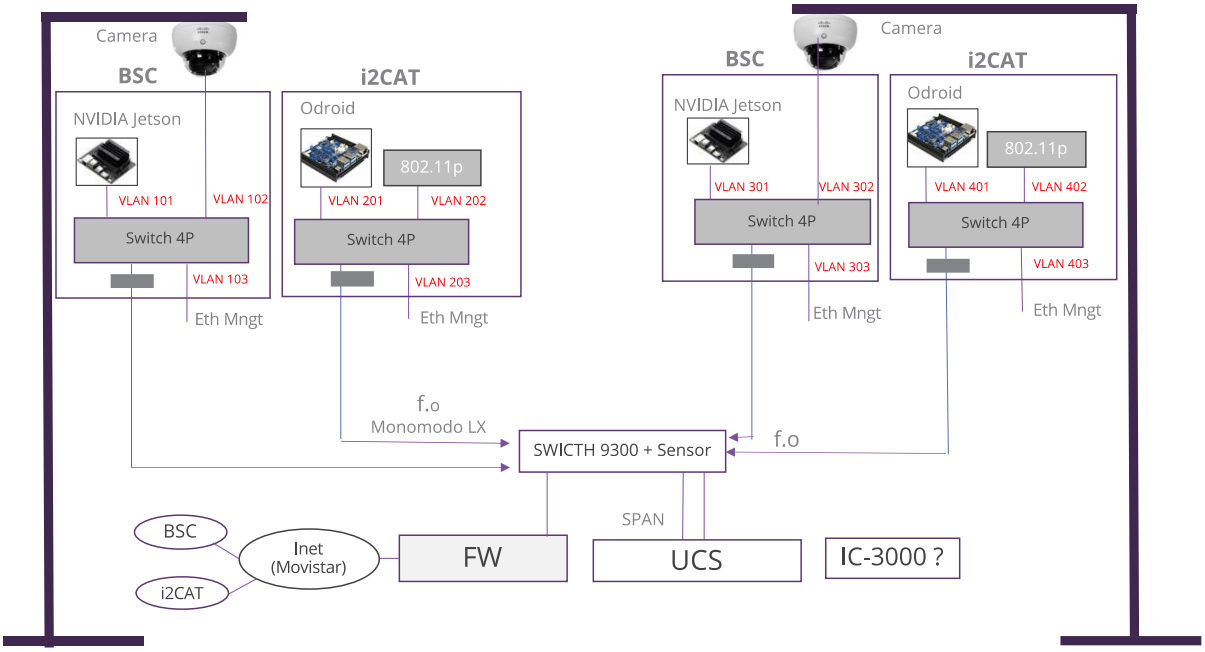


Figure 4. PUC 1-Barcelona Smart City Sensor Architecture

The Initial Threat Portfolio for PUC 1 is as follows:

Threat Scenario 1

Threat Scenario Name	***Pledger Security Notification DDoS and DoS***
Brief Description	The communication link between the Pledger system and the Tram and bicycles are key elements for the security of the pedestrians in Barcelona city. An external attacker motivated to cause any interference on the system to sabotage it, may use a denial-of-service attack to cause the communication link with the Jetson device controlling the presence of a tram, and the remote tags to become unavailable and cause a potential accident and harm pedestrians or cyclists.
Involved Actors	• Teleoperation/Remote Operator • Jetson Management Station • Cyber attacker - external to the system
Involved and affected Asset(s)	• Mobile Network • Teleoperation services • Teleoperation Module • Communication System

Interfaces, Entry and high-level vulnerable points	The attacker performs DoS attack by using open/unfiltered communication ports, lack of network monitoring for non-volumetric DDoS attacks, or any other method that can exploit resource limitation of the Jetson equipment.
Generic Scenario Description	▪ The cyber-attacker launches an attack against network that supports the teleoperation/remote-control station of the Jetson device. ▪ This attack has a low-cost of entry from the attacker and requires relatively low skills (kali linux, Hak5 pineapple, etc.)– thus it has high probability of occurrence. ▪ Implementation of DDoS attack on the network may be instantiated with various techniques and through various network layers - from radio access to TCP/IP – by monitor the network via scanning and reconnaissance and deploying malicious tools on attacker equipment. ▪ The main goal of the attack is the malicious sabotage of the notification system to cause a potential accident and cause harm to Barcelona citizens
Desired Response	The specific type of attacks is proactively taken into account and anticipated through risk analysis and impact assessment. A security support system shall be able to detect anomalous network activity which allow it to automatically activate new firewall rules or other defensive mechanisms to block traffic and monitor malicious behaviour for reporting of adversary tactics, techniques and procedures. Timely incident notification of the security teams, risk management support, and incident reporting and notification of 3rd parties and CERTs are desired.

Threat Scenario 2

Threat Scenario Name	***Pledger Security Notification Active Reconnaissance***

Brief Description	The communication link between the Pledger system and the Tram and bicycles are key elements for the security of pedestrians. An external attacker motivated to cause any interference on the system to sabotage it may use an Active Reconnaissance attack to detect a potential vulnerability or open port and get control of the system. This is not attack by itself, but it could be the precursory step of an attack to detect potential entry vectors on the systems. Early detection of these activities are crucial to protect systems against further attacks
Involved Actors	• Teleoperation/Remote Operator • Jetson Management Station • Cyber attacker - external to the system
Involved and affected Asset(s)	• Mobile Network • Teleoperation services • Teleoperation Module • Communication System
Interfaces, Entry and high-level vulnerable points	The attacker performs Active Reconnaissance attack sending probes to detect open/unfiltered communication ports that can be used to exploit the system.
Generic Scenario Description	▪ The cyber-attacker launches an attack against network that supports the teleoperation/remote-control station of the Jetson or Odroid device. ▪ This attack has a low-cost of entry from the attacker and requires relatively low skills (kali linux, Hak5 pineapple, etc.)– thus it has high probability of occurrence. It can be also an script kiddie just playing around with the different tools but in any case, this symptoms can´t be ignored ▪ Implementation of Reconnaissance attack on the network may be instantiated with various techniques and through various network layers - from radio access to TCP/IP – by monitor the network via scanning and reconnaissance and deploying malicious tools on attacker equipment. ▪ The main goal of the attack is the discovery of entry points to the system to pivot further attacks.

Desired Response	The specific type of attacks is proactively taken into account and anticipated through risk analysis and impact assessment. A security support system shall be able to detect anomalous network activity which allow it to automatically activate new firewall rules or other defensive mechanisms to block traffic and monitor malicious behaviour for reporting of adversary tactics, techniques and procedures. Timely incident notification of the security teams, risk management support, and incident reporting and notification of 3rd parties and CERTs are desired.

Threat Scenario 3

Threat Scenario Name	***Pledger Security Notification Cross Site Scripting***
Brief Description	The communication link between the Pledger system and the Tram and bicycles are key elements for the security of the pedestrians. An external attacker motivated to cause any interference on the system to sabotage it may use a Cross Site Scripting (XSS) attack to bypass the web browser same origin policy and potentially steal user credentials.
Involved Actors	• Teleoperation/Remote Operator • Jetson Management Station • Cyber attacker - external to the system
Involved and affected Asset(s)	• Mobile Network • Teleoperation services • Teleoperation Module • Communication System
Interfaces, Entry and high-level vulnerable points	The attacker performs XSS attack accessing Jetson Management Station Website

Generic Scenario Description	▪ The cyber-attacker launches an attack against network that supports the teleoperation/remote-control station of the Jetson device. ▪ This attack is somewhat sophisticated and requires relatively medium skills (kali linux, Hak5 pineapple, etc.)– thus it has medium probability of occurrence. ▪ Implementation of XSS attack on the network may be instantiated with various techniques and through various network layers - from radio access to TCP/IP – by accessing the web portal and deploying malicious tools on attacker equipment. ▪ The main goal of the attack is the discovery of user credentials and cookies that may put at risk the integrity of the system.
Desired Response	The specific type of attacks is proactively taken into account and anticipated through risk analysis and impact assessment. A security support system shall be able to detect anomalous network activity which allow it to automatically activate new firewall rules or other defensive mechanisms to block traffic and monitor malicious behaviour for reporting of adversary tactics, techniques and procedures. Timely incident notification of the security teams, risk management support, and incident reporting and notification of 3rd parties and CERTs are desired.

Threat Scenario 4

Threat Scenario Name	***Pledger Security Notification Cross Site Request Forgery***
Brief Description	The communication link between the Pledger system and the Tram and bicycles are key elements for the security of the pedestrians. An external attacker motivated to cause any interference on the system to sabotage it, uses a Cross Site Request Forgery on Bosch IP Cameras to trigger actions on the system on behalf of another user. This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera.

Involved Actors	• Teleoperation/Remote Operator • Bosch IP Camera Management Station • Cyber attacker - external to the system
Involved and affected Asset(s)	• Mobile Network • Teleoperation services • Teleoperation Module • Communication System
Interfaces, Entry and high-level vulnerable points	The attacker performs CSRF attack accessing Bosch IP Camera. There is a set of attackers who want to exploit the functionality of surveillance systems specifically. For example, state-actors or thieves performing reconnaissance over a geographic area and criminals planning to blackmail a victim with video footage
Generic Scenario Description	▪ The cyber-attacker launches an attack against network that supports the Bosch IP Camera device. ▪ This attack is somewhat sophisticated and requires relatively medium skills (kali linux, Hak5 pineapple, etc.)– thus it has medium probability of occurrence. ▪ Implementation of CSRT attack on the network may be instantiated with various techniques and through various network layers - from radio access to TCP/IP – by accessing the web portal and deploying malicious tools on attacker equipment. ▪ If Bosch IP Camera is compromised, these systems can provide an attacker with private imagery resulting in a direct explicit violation of privacy. These systems are also lucrative assets to botnet owners since they typically have high bandwidth (for DDoS attacks) and decent compute capabilities (for cryptomining). The features of a surveillance system change the weight of attacker's goals and the defender's priority on the defenses. For example, there is more emphasis on anti-DoS and MitM attacks in surveillance systems than other systems. Overall, the privacy violation of exposed data has much stronger implications than data from other IoTs.
Desired Response	The specific type of attacks is proactively taken into account and anticipated through risk analysis and impact assessment. A security support system shall be able to detect anomalous network activity which allow it to

	automatically activate new firewall rules or other defensive mechanisms to block traffic and monitor malicious behaviour for reporting of adversary tactics, techniques and procedures. Timely incident notification of the security teams, risk management support, and incident reporting and notification of 3rd parties and CERTs are desired.

Threat Scenario 5

Threat Scenario Name	***Bosch IP Camera Man in the Middle Video Injection***
Brief Description	The communication link between the Pledger system and the Tram and bicycles are key elements for the security of the pedestrians. An external attacker motivated to cause any interference on the system to sabotage it, uses Man in the Middle Video Injection on Bosch IP Cameras to manipulate, reroute, or observe network traffic. For example, an agent may perform a man-in-the-middle (MitM) attack in the local network, and then freeze a video image or inject it into a live feed. For the MitM attack, the attacker could reroute traffic through him via ARP poisoning, DHCP/DNS spoofing. For injection, the tool VideoJak may be used to exploit unencrypted video streams using the RTSP or RTP protocols. These protocols are commonly used in video surveillance systems, and may be left unencrypted
Involved Actors	• Teleoperation/Remote Operator • Bosch IP Camera Management Station • Cyber attacker - external to the system
Involved and affected Asset(s)	• Mobile Network • Teleoperation services • Teleoperation Module • Communication System
Interfaces, Entry and high-level vulnerable points	The attacker performs MiTM attack accessing the network used by the Bosch IP Camera. There is a set of attackers who want to exploit the functionality of surveillance systems

	specifically. For example, state-actors or thieves performing MiTM can inject rogue traffic into the network to perform malicious activities without being noticed. In this particular case, this may affect visibility of the operator and an accident can be caused
Generic Scenario Description	▪ The cyber-attacker launches an attack against network that supports the Bosch IP Camera device. ▪ This attack is somewhat sophisticated and requires relatively medium skills (kali linux, Videolak application, Hak5 pineapple, etc.)– thus it has medium probability of occurrence. ▪ Implementation of MiTM attack on the network may be instantiated with various techniques and through various network layers - from radio access to TCP/IP – by accessing the web portal and deploying malicious tools on attacker equipment. ▪ If Bosch IP Camera is compromised, these systems can provide an attacker with private imagery resulting in a direct explicit violation of privacy. Also, an accident can be caused as a consequence of operators being unaware of the real situation on the ground. ▪ The attacker may be able to watch/download live or pre-recorded video footage. Compared to compromising other IoT devices, this results in a significant privacy violation. The attacker could use the content to track people, observe their behaviours, find where valuables are stored, shoulder-surf to steal credentials, determine when to commit a crime, or blackmail an individual. Another concern is that the attacker will alter the contents to plant false evidence such as a prerecorded video loop, or use deep learning to insert an individual performing an activity (a.k.a., a deepfake cover up an on-going crime, or permanently delete footage.
Desired Response	The specific type of attacks is proactively taken into account and anticipated through risk analysis and impact assessment. A security support system shall be able to detect anomalous network activity which allow it to automatically activate new firewall rules or other defensive mechanisms to block traffic and monitor malicious

	behaviour for reporting of adversary tactics, techniques, and procedures. Timely incident notification of the security teams, risk management support, and incident reporting and notification of 3rd parties and CERTs are desired.

8.2 PUC2: Threat Portfolio

The key assets involved in PUC3 are as follows:

- **Autonomous Vehicle Control Platform** is the platform which contains the planning and decision control algorithms for autonomous driving. In Tallinn environment, this platform is based on Autoware.
- **ROS Control Software** is a middleware platform that operates a publishing and subscribing messaging system for autonomous vehicular communications.
- **Autonomous Vehicle Telemetry** is the data generated by the autonomous vehicle and the supporting infrastructure.

The Initial Threat Portfolio for PUC 2 is as follows:

Threat Scenario 1

Threat Scenario Name	***ML Evasion AV Shuttle Autonomous Control***
Brief Description	Training of the ML/AI is of predominant importance for the control algorithm and the autonomous cognition of the autonomous vehicle. If a cyber threat actor was to use a ML evasion attack, which is to maliciously modify the data which the control algorithm is trained on, to produce disruptive behaviour, it would impact the safe navigation of the vehicle in the traffic environment.
Involved Actors	• Cyber attacker with internal access to the system • Remote Control Center Operator • Cybersecurity Administrator • Traffic Management Administrator
Involved and affected Asset(s)	• Autonomous Vehicle Control Platform • ROS Control Software • Autonomous Vehicle Telemetry

Interfaces, Entry and high-level vulnerable points	To initiate this attack the cyber attacker requires access to the ML training data set or ability to upload a malicious data-set to train the ML model.
Generic Scenario Description	▪ Cyber attacker crafts malicious data (example. perturbed image of a Road Sign Unit) ▪ Exploiting access to the ML training dataset, the attacker uploads the malicious data to the training database. ▪ The ML model is trained on the adversarial dataset implanted by the cyber attacker ▪ The AV Shuttle crashes due to the autonomous cognition not recognizing the RSU, due to the adversarial dataset uploaded by the attacker.
Desired Response	The specific type of attacks is proactively taken into account and anticipated through risk analysis and impact assessment. A security support system shall be able to detect anomalous behaviour. Timely incident notification of the security teams, risk management support, and incident reporting and notification of 3rd parties and CERTs are desired.

Threat Scenario 2

Threat Scenario Name	***Message Flooding/DDoS AV Shuttle Communications***
Brief Description	The AV Shuttle autonomous cognition relies on telemetry to ensure correct decision making. Cyber threats which impact the availability of telemetry and communications within the AV shuttle ecosystem can lead to catastrophic consequences for the safe navigation of the AV shuttle.
Involved Actors	• Cyber attacker with internal access to the system • Remote Control Center Operator • Cybersecurity Administrator • Traffic Management Administrator
Involved and affected Asset(s)	• UoP • Autonomous Vehicle Telemetry • Autonomous Vehicle Control Platform • ROS Control Software

	• RSU (V2X)
Interfaces, Entry and high-level vulnerable points	Within the complex architecture of AV and supporting infrastructure there are many gaps regarding authentication of devices and messaging exchange. An attacker with capability to intercept vehicle communications such as V2X (Vehicle to RSU), can learn how to authenticate rogue devices into the AV shuttle ecosystem and send malicious messages.
Generic Scenario Description	▪ A cyber threat actor intercepts communications from the autonomous vehicle and RSUs to the UoP. ▪ The threat actor authenticates a rogue RSU to the AV and UoP. ▪ The threat actor then floods the communication channel, a DDoS, which impacts the availability of AV shuttle messaging to safely navigate. Alternatively ▪ The threat actor creates malicious packets to disrupt the availability of communications between the AV shuttle and RSU. Alternatively ▪ The threat actor creates malicious packets to send erroneous data to the UoP to disrupt the AV shuttle messaging required for safe navigation.
Desired Response	The IRIS platform can detect and alert against cyber threats that impact the availability of the AV shuttle communications. The IRIS platform will provide a notification to the Cybersecurity administrator to take an action which would mitigate against the threat and avoid loss of availability of the AV communications. The Cybersecurity administrator will be able to share CTI with the MeliCERTes community and allow effective cyber incident response with the CERT authorities. The cyber threat should be able to be recorded and replayed in a virtual cyber range environment to allow training of the Cybersecurity administrator.

8.3 PUC3 Helsinki: Threat Portfolio

The key assets involved in PUC3 are as follows:

- **External Router (TOSIBOX LOCK500)** provide remote access for secure connectivity to the smart grid environment.
- **Logic Controller (KNX Wiser)** is used to visualize and control the Home Automation solution in KNX and Modbus networks. The logic controller is also uses as:
    - Gateway to translate and enable communication between different products.
    - As an aggregator to stock, analyze, and send the data.
    - As an event controller that sends email in case of issues
    - Web SCADA visualization for PC and touch devices
    - Cross-Standard gateway between KNX and Modbus RTU/TCP
    - BACnet Server
- **Sensors (Apartment Energy Meters)** provide the telemetry data of the smart grid from the home to sub-system.
- **RTU Network and RTU devices (RTU560 IO, RTU560 CMG)** represent the interface of the physical energy devices (Apartment Energy Meters) and the distributed control system or SCADA system. The RTU network transmits real-time telemetry of the energy sub-system to the master system.
- **Network infrastructure (Switches, Cisco ASA Firewalls)** support the connectivity of the smart grid environment.
- **UoP** is the open API which supports streaming of data (Kafka) to create visual dashboards detailing energy efficiency/usage etc. The UoP has an instance in Helsinki and Tallinn, Estonia.

Figure 5 displays the PUC3 ecosystem and cyber threat scenarios (detailed in D2.1).

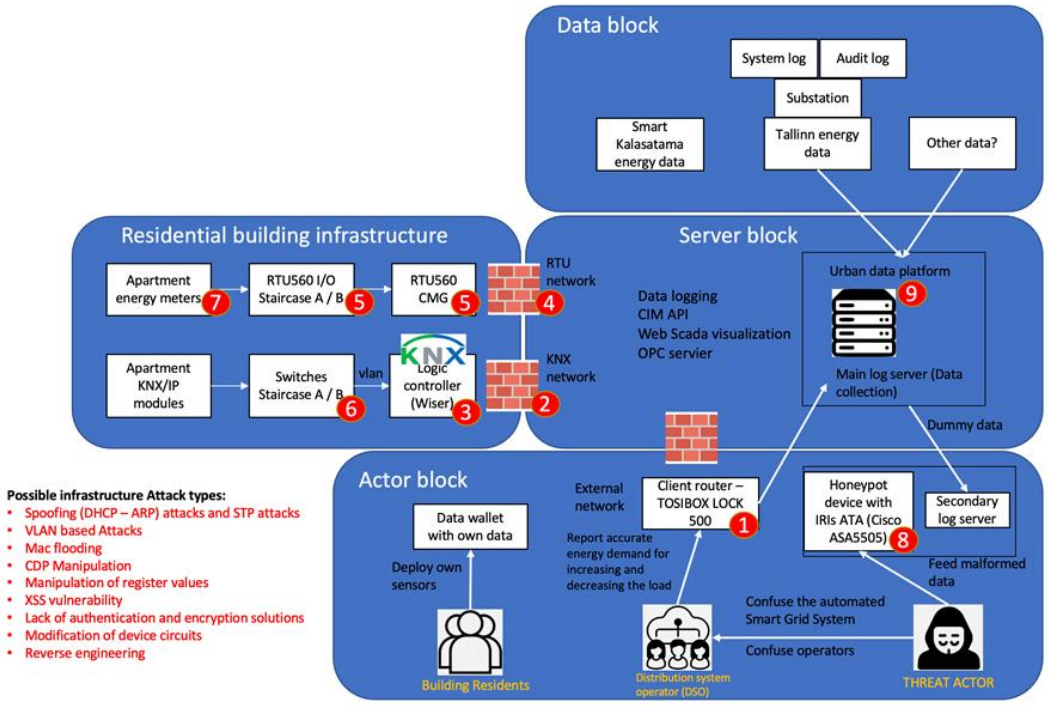


Figure 5. PUC 3 - Helsinki Smart City Sensor Architecture and Cyber Threat Scenarios

The Initial Threat Portfolio for PUC 3 is as follows:

Threat Scenario 1

Threat Scenario Name	***External Router – Unathorised Access***
Brief Description	Remote access and networking device that serves as an endpoint for secure remote connections. Devices connected to the External Router (TOSIBOX LOCK500) are securely accessed over the Internet and most LAN and WAN networks through an encrypted VPN connection.
Involved Actors	• IoT/Smart Grid Operator • Systems Administrator • Cyber attacker - external to the system
Involved and affected Asset(s)	• External Router (TOSIBOX LOCK500)
Interfaces, Entry and high-level vulnerable points	Remote access and networking device that serve as an endpoint for secure remote connections. Any unathorised connections to the external router will allow access to devices on the network and data of the smart grid.
Generic Scenario Description	▪ A cyber attacker compromises the update server of the TOSIBOX. ▪ The cyber attacker develops a firmware update package that includes and exploit enabling remote access to the TOSIBOX ▪ The IoT/Smart Grid operator updates the TOSIBOX firmware with the exploit. ▪ The Cyber Attacker gains access to the TOSIBOX external router.
Desired Response	The specific type of attacks is proactively taken into account and anticipated through risk analysis and impact assessment. A security support system shall be able to detect anomalous network activity and general vulnerabilities/known CVEs. Timely incident notification of the security teams, risk management support, and incident reporting and notification of 3rd parties and CERTs are desired.

Threat Scenario 2

Threat Scenario Name	***KNX Controller Vulnerability Exploitation***
Brief Description	KNX is used to visualize and control home and building automation. An attacker can use the lack of security features for authentication and encryption in the home automation network to gain access to the KNX Wiser controller. With access to the KNX controller the attacker can disrupt the residential building infrastructure.
Involved Actors	• IoT/Smart Grid Operator • Systems Administrator • Cyber attacker - external to the system
Involved and affected Asset(s)	• KNX Wiser (Logic Controller) • Residential building infrastructure (KNX Network)
Interfaces, Entry and high-level vulnerable points	The KNX Wiser (Logic Controller) uses a number of different protocols and services to enable functionality such as data visualisation and storage.
Generic Scenario Description	▪ A cyber attacker with access to the LAN, scans the KNX controller for open ports. ▪ From the results of the scan, the cyber attacker finds vulnerabilities systems. ▪ The attacker uses a CVE to exploit access to the KNX Wiser Controller ▪ The cyber attacker disrupts the KNX network through remove/modifying network configurations.
Desired Response	The specific type of attacks is proactively taken into account and anticipated through risk analysis and impact assessment. A security support system shall be able to detect anomalous network activity and general vulnerabilities/known CVEs. Semi-autonomous response should enable a message to be sent to the System Administrator to perform an action to mitigate the risk of the CVE. Timely incident notification of the security teams, risk management support, and incident reporting and

	notification of 3rd parties and CERTs are desired.

Threat Scenario 3

Threat Scenario Name	***Urban Operating/Data Platform – Malformed Data***
Brief Description	The UoP is a software platform used for data collection and analysis and visualisation of smart city (smart grid) data. Integrity of the data is key to ensuring public confidence in smart city IoT systems and for data-driven decision making. A cyber attacker that has the capability to manipulate data in the UoP or being transmitting to the UoP can disrupt the smart grid system.
Involved Actors	• IoT/Smart Grid Operator • Systems Administrator • Cyber attacker - external to the system
Involved and affected Asset(s)	• UoP • Data Block (Smart Kalasadama Energy Data, Tallinn Energy Data, Other Data) • Smart Meter
Interfaces, Entry and high-level vulnerable points	It could be assumed that the attacker has access to the UoP, the internal network, smart meter or is able to read data transmitted to the UoP.
Generic Scenario Description	There could be several different scenarios, these include: ▪ A cyber attacker places a rogue smart meter on the network which transmits erroneous/malicious data to the Smart Kalasadama UoP and to the Tallinn UoP. ▪ A cyber attacker modifies data in either of the Smart Kalasadama UoP or the Tallinn UoP.
Desired Response	The specific type of attacks is proactively taken into account and anticipated through risk analysis and impact assessment. A security support system shall be able to detect anomalous network activity and general vulnerabilities/known CVEs. Semi-autonomous response should enable the rogue transmitting sensor to be blocked. Timely incident notification of the security teams, risk

	management support, and incident reporting and notification of 3rd parties and CERTs are desired.

9 CONCLUSIONS

This deliverable provided the building blocks for the design of the IRIS Platform. This included: End-User requirements, IRIS Platform functional and technical requirements, KPIs for IRIS Platform validation, State-of-the-Art of key technical integration areas and an initial threat portfolio of the PUCs for development of the ATA module.

From the End-User requirements elicitation process, it is clear, that CERTs, which form an essential part of the MeliCERTes ecosystem, would like to see an IRIS Platform designed to ensure: the modular nature of MeliCERTes, extensibility of tools and use, where possible, of open APIs. The PUC End-Users provided detailed requirements for usage of the IRIS Platform.

Functional and technical requirements were provided by the tool developers. Furthermore, KPIs for evaluation of each of the IRIS Platform modules were detailed. Lastly, a state-of-the-art for key integration areas was conducted and an initial threat portfolio for each of the PUCs was provided.

10 REFERENCES

[1] Landauer, M., Skopik, F., Wurzenberger, M., Hotwagner, W., & Rauber, A. (2019, December). A framework for cyber threat intelligence extraction from raw log data. In 2019 IEEE International Conference on Big Data (Big Data) (pp. 3200-3209). IEEE.

[2] Huang, Y. T., Lin, C. Y., Guo, Y. R., Lo, K. C., Sun, Y. S., & Chen, M. C. (2021). Open Source Intelligence for Malicious Behaviour Discovery and Interpretation. IEEE Transactions on Dependable and Secure Computing.

[3] Dalziel, H. (2014). How to define and build an effective cyber threat intelligence capability. Syngress.

[4] Chantzios, T., Koloveas, P., Skiadopoulos, S., Kolokotronis, N., Tryfonopoulos, C., Bilali, V. G., & Kavallieros, D. (2019). The Quest for the Appropriate Cyber-threat Intelligence Sharing Platform. In *DATA* (pp. 369-376).

[5] Ramsdale, A., Shiaeles, S., & Kolokotronis, N. (2020). A comparative analysis of cyber-threat intelligence sources, formats and languages. Electronics, 9(5), 824.

[6] Landauer, M., Skopik, F., Wurzenberger, M., Hotwagner, W., & Rauber, A. (2019, December). A framework for cyber threat intelligence extraction from raw log data. In 2019 IEEE International Conference on Big Data (Big Data) (pp. 3200-3209). IEEE.

[7] L. Spitzner, Honeypots: tracking hackers, Addison-Wesley Reading, 2003.

[8] Zobal, L., Kolář, D., & Fujdiak, R. (2019, October). Current state of honeypots and deception strategies in cybersecurity. In 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT) (pp. 1-9). IEEE.

[9] R. Marty and L. Spitzner, The Value of Honeypots, Part One: Definitions and Values of Honeypots., 2001.

[10] Brown, R., & Lee, R. M. (2019). The evolution of cyber threat intelligence (CTI): 2019 SANS CTI survey. SANS Institute. Available online: https://www. sans. org/white-papers/38790/(accessed on 12 July 2021).

[11] Koloveas, P., Chantzios, T., Alevizopoulou, S., Skiadopoulos, S., & Tryfonopoulos, C. (2021). inTIME: A Machine Learning-Based Framework for Gathering and Leveraging Web Data to Cyber-Threat Intelligence. Electronics, 10(7), 818.

[12] Koloveas, P., Chantzios, T., Tryfonopoulos, C., & Skiadopoulos, S. (2019, July). A crawler architecture for harvesting the clear, social, and dark web for IoT-related cyber-threat intelligence. In 2019 IEEE World Congress on Services (SERVICES) (Vol. 2642, pp. 3-8). IEEE.

[13] Najork, M. (2009). Web Crawler Architecture

[14] Harth, A., Umbrich, J., & Decker, S. (2006, November). Multicrawler: A pipelined architecture for crawling and indexing semantic web data. In International Semantic Web Conference (pp. 258-271). Springer, Berlin, Heidelberg

[15] Ramsdale, A., Shiaeles, S., & Kolokotronis, N. (2020). A comparative analysis of cyber-threat intelligence sources, formats and languages. Electronics, 9(5), 824.

[16] "MadeSafe.net."

[17] D. Irvine, "Self encrypting data," Department of Computer Science, Michigan State University, 72 Templehill, Troon, South Ayrshire, Scotland, UK. KA10 6BE., 2010.Available: https://maidsafe.net/

[18] "Self-Encryption by MaidSafe."

[19] C. Paar and J. Pelzl, *Understanding cryptography: A textbook for students and practitioners*. Springer Science & Business Media, 2009.

[20] B. Preneel, "Cryptographic hash functions," *European Transactions on Telecommunications*, vol. 5, no. 4, pp. 431–448, 1994, doi: https://doi.org/10.1002/ett.4460050406.

[21] T. Hansen and D. E. E. 3rd, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)." RFC 6234; RFC Editor, May 2011. doi: 10.17487/RFC6234.

[22] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, "Keccak sponge function family main document." http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.419.2140&rep=rep1&type=pdf

[23] M.-J. O. Saarinen and J.-P. Aumasson, "The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)." RFC 7693; RFC Editor, Nov. 2015. doi: 10.17487/RFC7693.

[24] D. Joan and V. Rijmen, "AES proposal: Rijndael." 1999.

A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979, doi: 10.1145/359168.359176.

[25] "Shamir's secret sharing scheme in golang."

[26] "Hyperledger fabric."

[27] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, Nov. 2002, doi: 10.1145/571637.571640.

[28] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System." 2014.Available: http://arxiv.org/abs/1407.3561

[29] Software Extension to the PMBOK Guide Fifth Edition, PMI – Project Management Institute, 2013.

ANNEX A – END-USER STAKEHOLDERS CONTROL GROUP 1

From the feedback the following can be inferred about End-User stakeholders use of the IRIS platform:

- The IRIS Platform will be accessed, predominantly, by technical users
- 24/7 availability is required from end-users
- Preference for use of modules will be dictated by the end-user based on their requirements. CERTs are more likely to be interested in collaborative information sharing.
- End-Users expect that the IRIS platform will be able to be configured by both specialists and non-specialists. Therefore, clear instructions and/or user-friendly interfaces are required to cater for non-specialists.
- End-Users expect a modular design, allowing tools integrated within MeliCERTes platform to be also used as a stand-alone.
- The End-Users surveyed favor a hybrid deployment, where some IRIS components are accessed locally, and some are in an off-premise/hosted/cloud environment.
- End-Users want the ability to access the platform via web interface and through mobile-device friendly user interface.
- End-Users expect the IRIS platform to be able to allow over 1000 users to access the platform simultaneously without performance degradation.
- The IRIS Platform needs to be able to store, at-least, up to 1TB per month.
- Access to the platform should be available via either multi-factor authentication and/or token-based authentication.
- AI/IoT technologies suggested for monitoring by End-Users include the following:
    - Serial Ports
    - TCP/IP
    - REST APIs
    - Ethernet
    - Data Factory Resources
    - DNS
    - HTTP/HTTPS
    - Proprietary protocols (IEC104 etc.)
    - IoT protocols: MQTT, CoAP, ZigBee, 6LowPAN etc.
- APIs that IRIS Platform should support include: REST API and JSON API

- Data formats that IRIS Platform should support include: Syslog, XML and JSON.
- Input data that the IRIS Platform should support include:
    - PCAP files
    - Physical interfaces (eth1...)
    - Log files (.csv, log ingestion)
    - Streaming flows (Kafka, MQTT, Redis ingestion)
- End-User preferences for the format that the IRIS platform should provide on detected events:
    - Standard Syslog
    - Standard/CEF
    - RFC3164
    - RFC3164/CEF

Automated Threat Analytics

- End-Users expect the IRIS platform to detect and analyze the following threats:
    - Cyber attacks
    - Cyber-physical attacks
    - Zero-day exploits
    - Network, software and device (IoT) vulnerabilities
- End-Users expect the IRIS platform to detect and analyse:
    - Attacks on availability of AI and IoT systems (DDoS Attacks etc.)
    - Attacks on integrity of AI and IoT Systems (AI and ML Evasion, data manipulation etc.)
    - Attacks on confidentiality of AI and IoT Systems (Data interception)
- End-Users have differing expectations on the length of time for threat analysis to be provided after an incident alert. This ranged from 5 minutes after an incident to 1 hour after an incident.
- Apart from traditional approaches to intrusion detection (signature, anomaly etc.) End-Users noted interest in following IDS features:
    - Agentless setup (as an option)
    - Support heterogeneity of devices type and communication protocols

    - Support resource limitations of IoT devices such as CPU, memory and energy
    - ML-based detection: Feature extraction and datasets
- The IRIS Platform is capable of reporting results in an automated format as well as allowing the End-User to customize the format of reports.

Collaborative Threat Intelligence and Orchestration

- All End-Users rated the most important functionality for the CTI module as: relevant, adequate, accurate, and on-time intelligence about threats
- End-Users expect automated response and recovery results to be provided within a range of near real-time (minimal delay in terms of seconds) and a few minutes.
- End-User also expected that user of the intelligence orchestrator module will have the capability to intervene manually to the system and change the proposed response.
- Strong taxonomy, ontology and validation procedures are important to CERT/CSIRT End-Users. End-Users use customized taxonomies based on the ones recommended by ENISA and NIST. Taxonomies and ontologies are used predominantly in the Incident Response and Incident Handling Process.
- Attributes, End-Users would like to be visualized of the IT/OT system include: Network Traffic, Network status along with risk indicators, IoT device status along with risk indicators, vulnerabilities.
- Main privacy and security concerns of End-Users include:
    - Prototypes/cheap IoT devices (updates non-existent or manual, security model unknown)
    - Demos/pilots which prevent daily application/service/core updates, for example because of version requirements/clashes
    - Protocol security (for example MQQTT or some Docker-based services)
    - Database security (example, some Docket templates have lax/no security and should be checked manually)
    - Improper device authentication
    - Remote access
- End-Users expect solutions to be GDPR compliant
- Formats used by End-Users for threat information sharing include: JSON, STIX/TAXII, txt and PDF (Reports), Syslog, CSV

- The most interesting features for collaborative threat intelligence, nominated by End-Users, include:
    - Trust of the related intelligence
    - Effective intelligence sharing
    - Intelligence consumption
    - Signature-based IDS
    - Behavioural anomaly detection
    - Real-Time alerting
    - Security analytics
    - Impact Assessment

Data Protection & Accountability (DPA)

- The most important privacy consideration for End-Users is that the proposed DPA module incorporate the requirements of GDPR.

Hands-on Collaborative & Immersive Cybersecurity Training

- Each End-User had different expectations as to what the training exercises would be useful for in their organisation. These included:
    - Validating and securing IoT and AI systems
    - Providing best practices according to the state-of-the-art
    - Understanding how to configure, manage and monitor defensive tools to detect and deter cyber threats to IoT and AI systems.
- End-User favored the training to focus on technical staff.

ANNEX B – END-USER STAKEHOLDERS CONTROL GROUP 2

The consolidated commentary from the CERT Advisory Group is provided below:

IRIS Enhanced MeliCERTes Ecosystem

1. ***How do you currently use MeliCERTes platform?***

- National CERTs are active end-users and developers of the MeliCERTes ecosystem. ***MeliCERTes has been upgraded to version 2 by the development***

community only recently and this is used by the CERT/CSIRT network (v1 is deprecated).

- One CERT participating in the interviews is not using MeliCERTes, but, wants to implement it in the future.
- The modular framework of MeliCERTes is important as each CERT utilizes different modules to meet their unique and differing requirements. The ***modularity and extensibility*** of MeliCERTes is an important feature of the design of the platform.
- The enhancements to MeliCERTes, in the IRIS project, *should allow CERTs to* ***use individual modules according to their requirements***.
- Benefits of the MeliCERTes community include: Directory of contacts (ContactDB and Trust Circles), collection of highly used tools, interoperability, and orchestration.
- Key functionality in this user-rich environment is collaboration. MISP, which is part of the MeliCERTes ecosystem, is key for collaborative threat information sharing. There is an inherent requirement for real-time communications. Current activity is focused on integrating MatterMost instant chat within the MeliCERTes ecosystem.

2. ***What CERT Roles use the platform (i.e. Cyber analyst)?***
    - MeliCERTes ecosystem is heavily used within National CERTs. Role types include: Analysts, Operators, Incident Responders, Malware analysts, Forensic Analysts and Sofware Engineers.

3. ***What systems are monitored by MeliCERTes (i.e. All, critical infrastructure)?***
    - Mixed, everything. Each CERT will have a predominant area of focus based on the environment, for example: A stakeholder CERT area of operation is dominated by the financial sector.
    - MeliCERTes is mainly used for CTI, threat sharing and monitoring of services to generate reports. It is also used by the CERT/CSIRT network in exercises for information sharing and CTI.

4. ***Which module(s) do you expect to use the most in your daily activities? (All modules, Automated Threat Analytics, Collaborative Threat Intelligence, Data Protection & Accountability, Cyber Range)?***

- It depends on the requirements of the CERT, the incident response team, and their preferences.
- The predominant factor in the CERTs decision to use a tool is ***usability and interoperability***. If the UI is not user-friendly and not preferred by the incident response team, then it is likely the tool won't be used. If the tool is not interoperable, does not allow the CERT to integrate/collaborate with stakeholders, such as the private sector, it will have limited use.

5. ***One of the aims of the IRIS project is to enhance the capability of the MeliCERTes ecosystem by providing: Threat Analytics Orchestration (TAO), Open Threat Intelligence interface and an intuitive Threat Intelligence Companion. How do you expect to use these capabilities?***
   - We will understand this more as the project evolves and we see more information regarding the modules.
   - Currently, as part of MeliCERTes II ecosystem, the CERTs use cerebrate for orchestration and IntelMQ.
   - An important capability enhancement would be to change the way high-priority notifications are provided from email to more real-time communication. Currently, emails are sent and ignored by local government and private organisations. Better methods for communication are required.
   - It is also essential, and CERTs would be grateful, for the development on the MeliCERTes ecosystem, for tool owners to **share APIs** so they can be used by other CERTs.
   - Toolsets which are created for the MeliCERTes ecosystem should be **interoperable.**
   - Another capability enhancement could be using AI for the automatic generation of incident response reports. This is a use-case where AI could work well.
   - Currently, there is not a shared platform for forensics in the MeliCERTes ecosystem.

Automated Threat Analytics

6. ***What kind of threats/attacks do you expect the IRIS platform to detect and analyse? (Example: Zero-Day exploits, Cyber-Physical Attacks)***
   - General scanning attacks – open ports (RDP/FTP)
   - APTs are difficult to detect, and it is difficult to understand how an automated detection system would work for these types of attacks.
   - CERTs encourage the IRIS project to focus on **common use-cases**, as these are the most typical in the real-world environment. Common use-cases

include **general vulnerabilities** of the target systems, those obvious vulnerabilities which a diverse range of threat actors can exploit.
- Reverse DNS lookup, reconnaissance and scanning tactics are a pain point for CERTs.
- Spoofing attacks are a nuisance. These attacks are characterized as legitimate devices on a network which have been compromised by a threat actor to monitor, intercept and/or perform adversarial behaviour. Such attacks can include botnets. Threat detection and analytics can benefit from ML approaches such as reinforcement learning which can learn from adversarial behaviour and provide early warning of future attacks.

7. ***What is your understanding of autonomous response and self-recovery procedures from a response-time and recovery action perspective? (Example: Attack detected in real-time by ATA and incoming malicious traffic blocked)***
    - There must be caution applied to Autonomous response and recovery systems as they have been abused by attackers.
    - CERTs haven't seen a practical example of where autonomous response and recovery can be applied. Rather autonomous response and recovery are a good candidate for non-operating networks such as honeypots. A suggested use-case could be to apply autonomous response and recovery for a honeypot IoT network that has been targeted by the Mirai botnet.
    - Semi-Autonomous response, human-in-the-loop, is optimal for a production network. Difficulty in autonomous response and recovery is that it can cause more problems and there are difficulties in the communication with third-parties about what changes the autonomous self-recovery has made to the system. This is why it is not acceptable in a critical infrastructure environment.
    - The learning process from threat data analysis should result in improvement in detection and response from the human operator and the ATA system.

Collaborative Threat Intelligence & Data Protection and Accountability

8. ***What are your organisation's technical and managerial requirements regarding CTI exchange?***
    - Traffic light protocol for rating the sensitivity of the information.
    - Circles of trust functionality are important information sharing

9. ***What are your CERTs main privacy and security concerns for CTI Exchange?***
    - Privacy concerns depend on the community
    - GDPR is always important
    - It is difficult to learn and train from the threat data due to GDPR. It is difficult to gain value from data due to requirements for anonymity and data protection.

10. ***Based on the previously mentioned privacy and security concerns, what key functionalities should the CTI module provide to deal with these concerns****?*

    - Integrity of information flow is important
    - Multi Party Computation and Digital Signature solutions are very difficult to implement in a CTI environment.
    - Any capability that adds to integrity and transparency of information is useful.

11. ***Which formats should the CTI module support (e.g., JSON, Stix, etc.) for sharing the threat intelligence information?***
    - There are 100s of different formats for actionable data. Focus on the most common:
        - MISP standard can transform to STIX
        - Yara rules for signatures
        - Intel MQ format

12. ***What cybersecurity-related taxonomies and/or ontologies are you using inside your organization (if any)?***
    - Standard taxonomies (Intel MQ, STIX, MISP)
    - Some CERTs have their own taxonomies, but, are based around MISP
    - There is a range of taxonomies, simplification is desired but a challenge.

13. ***What would be the 3 features most interesting for you in terms of Collaborative Threat Intelligence?***
    - Generally, the most important enhancements to the existing ecosystem are centered on improving the usability and integrity of collaborative information sharing.
    - A mobile interface for CTI exchange would be a great feature.
    - Mapping threats in real-time
    - Gaining a better understanding of response times for actionable CTI

Virtual Cyber Range

14. ***What features are important for you for the Virtual Cyber Range training for the CERTs/CSIRTs? (Example: training for CERT analysts to action detected IoT threats)?***

- Adversarial training is important. Incident responders need to understand the mindset and the tactics of the attackers. Scenarios which allow red teaming are important for blue teams.
- Interoperability. It would be nice to be able to take the cyber range scenario and expand on it and use it on different platforms and in collaborative training environments.
- Translation of honeypot and digital infrastructure to the training environment is useful for more realistic data.

15. What are some of the key threat scenarios, targeting AI and IoT systems, that you would like to see within the VCR training? (Example: 3rd Party Software Library vulnerability)?

- Realistic threat scenarios
- Skill areas such as reverse engineering etc.