



Artificial Intelligence Threat Reporting and Incident Response System

D4.7 - IRIS-enhanced MeliCERTes platform

Project Title:	Artificial Intelligence Threat Reporting and Incident Response System
Project Acronym:	IRIS
Deliverable Identifier:	4.7
Deliverable Due Date:	31/12/2023
Deliverable Submission Date:	15/01/2024
Deliverable Version:	V1.0
Main author(s) and Organisation:	Dimitrios Skias (INTRA), Sofia Tsekeridou (INTRA)
Work Package:	WP4 Collaborative Secure and Trusted Cyber-Threat Intelligence Sharing
Task:	Task 4.6: IRIS-enhanced MeliCERTes platform for secure and trusted online communication, collaboration and information sharing
Dissemination Level:	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 contains.



Quality Control

	Name	Organisation	Date
Editor	Dimitrios Skias	INTRA	15/1/2024
Peer Review 1	Eleni Darra	CERTH	12/1/2024
Peer Review 2	Mihai Guranda	DNSC	15/1/2024
Submitted by (Project Coordinator)	Gonalo Cadete	INOV	15/1/2024

Contributors

Organisation
NETCOMPANY-INTRASOFT SA (INTRA)

Document History

Version	Date	Modification	Partner
V0.1	15/10/2023	ToC	INTRA
V0.2	23/10/2023	First draft	INTRA
V0.4	3/12/2023	Second draft	INTRA
V0.7	20/12/2023	General updates	INTRA
V0.8	11/01/2024	Review ready version	INTRA
V0.9	15/01/2024	Peer-reviewed version	CERTH, DNSC
V1.0	15/01/2024	Final version	INTRA, INOV

Legal Disclaimer

IRIS is an EU project funded by the Horizon 2020 research and innovation programme under grant agreement No 101021727. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The IRIS Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.



Contents

1 Introduction.....	7
1.1 Deliverable Purpose.....	7
1.2 Relations to other activities	7
1.3 Document Overview	8
2 IRIS-enhanced Melicertes platform (eme) overview	9
2.1 MeliCERTes CSP	9
2.2 EME ecosystem in IRIS architecture	11
2.3 IRIS EME platform's high-level objectives and vision	13
2.4 IRIS EME platform's requirements.....	13
3 IRIS-enhanced MelicERTES platform design	17
3.1 IRIS-EME platform Architecture.....	17
3.1.1 IRIS-EME platform (CI Operator instance)	18
3.1.2 IRIS-EME platform (CERT/CSIRT Operator instance)	18
3.2 IRIS-EME platform components.....	19
3.3 IRIS-EME platform implementation	20
3.4 IRIS-EME platform operation.....	21
3.4.1 Keycloak IMS.....	23
3.4.2 MeliCERTes 2 - Cerebrate	25
3.4.3 INTELMOQ.....	27
3.5 Interfaces and data models	28
3.6 IRIS-EME platform Database Schema.....	30
3.7 IRIS-EME Unified Dashboard – SIEM	31
3.8 Implementation.....	32
3.9 EME-CI UI	32
3.9.1 EME-CI UI Homepage	32
3.9.2 EME-CI UI Policy.....	34
3.9.3 EME-CI UI Scanning.....	34
3.9.4 IRIS-EME CI UI Threats	35
3.10 EME-CERT UI.....	37
3.10.1 EME-CERT UI Homepage	37
3.10.2 IRIS-EME CERT UI Threats	38
3.11 Applications integrated in IRIS-EME UI	39
3.11.1 ATIO - Workflow Manager (OWM) - UI	39
3.11.2 MISP application - UI	40
3.11.3 SiHoneyPot – UI	41
4 IRIS-EME platform deployment and validation	42
4.1 IRIS-EME platform installation.....	42



4.2 IRIS-EME platform deployments.....	43
4.3 Testing	44
4.4 Future plans	44
5 Conclusions.....	45
6 References.....	46

List of Figures

Figure 1: IRIS High-Level Architecture (Tool View).....	11
Figure 2: IRIS platform's functional requirements relevant to EME.....	15
Figure 3: IRIS platform's non-functional requirements relevant to EME.....	16
Figure 4: IRIS EME high-level communication.....	17
Figure 5: IRIS-EME CI operator's instance architecture.....	18
Figure 6: IRIS-EME CERT/CSIRT instance architecture	19
Figure 7: IRIS-EME platform Keycloak IMS.....	24
Figure 8: IRIS-EME Keycloak operation via ATIO	24
Figure 9: IRIS-EME Keycloak login page	25
Figure 10: IRIS-EME platform's Cerebrate view of individual registered users	26
Figure 11: IRIS-EME platform's Cerebrate view of individual registered organisations.....	26
Figure 12: IRIS-EME platform's Cerebrate view of available Sharing Groups.....	27
Figure 13: IRIS-EME platform's Cerebrate view of the Broods that allow for data synchronisation among instances of Cerebrate.....	27
Figure 14: IRIS-EME platform's REST API	29
Figure 15: IRIS-EME platform's Database Schema	30
Figure 16: IRIS EME-CI Homepage.....	32
Figure 17: IRIS-EME CI Policy view	34
Figure 18: IRIS-EME CI policy explanation	34
Figure 19: IRIS-EME CI UI Threat view	35
Figure 20: IRIS-EME CI UI Threats view (approved).....	36
Figure 21: IRIS-EME CERT UI Homepage (upper part)	37
Figure 22: IRIS-EME CERT UI Homepage (bottom part)	38
Figure 23: IRIS-EME CERT UI Threats view	39
Figure 24: ATIO Orchestrator Workflow Manager (OWM) listing organisations workflows.....	40
Figure 25: IRIS-EME MISP instance login page	41
Figure 26: Integrated into HELM charts components of IRIS-EME platform (so far)	42
Figure 27: Installation process for the IRIS-EME platform deployment.....	43
Figure 28: CERT-1 deployment.....	43
Figure 29: CI-1 deployment.....	43
Figure 30: CI-2 deployment.....	43



List of Abbreviations and Acronyms

Abbreviation/ Acronym	Meaning
AI	Artificial Intelligence
API	Application Programming Interface
ATA	Automated Threat Analytics
ATIO	Advanced Threat Intelligence Orchestrator
CERTs	Computer emergency response teams
CACAO	Collaborative Automated Course of Action Operations
CSIRTs	Computer security incident response teams
CSP	Cyber Security Platform
CTI	Collaborative Threat Intelligence
DB	Database
DPA	Data Protection and Accountability
EME	Enhanced MeliCERTes Ecosystem
HP	Hyperledger Fabric
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IoT	Internet of Things
JSON	JavaScript Object Notation
MISP	Malware Information Sharing Platform
OAuth AAA	Open Authentication Authentication, Authorisation and Accounting
STIX	Structured Threat Information eXpression
VDM	Vulnerability Discovery Manager
UI	User Interface
WP	Work Package
OWM	Orchestrator Workflow Manager



Executive Summary

Deliverable D4.7 “IRIS-enhanced MeliCERTes platform”, the outcome of task T4.6 of the IRIS workplan, presents the IRIS enhanced MeliCERTes platform (IRIS EME) in terms of its concept and objectives, architectural design, implemented functionalities along with development details, functional and non-functional requirements alignment status and operational workflows for its main target stakeholders: CI Operators and CERTs/CSIRTs.

The present report serves as a demonstrator of the IRIS EME platform providing advanced dashboard, extended knowledge base, diverse communities of users, and customized views and access to shared incidents, CTI and other information.



1 INTRODUCTION

IRIS contributes towards a European strategic autonomy in IoT and AI cybersecurity. It considers the complete range of cybersecurity and privacy risks associated with IoT and AI-enabled ICT systems and their associated technical and human factors threat intelligence challenges. IRIS addresses the confidentiality, integrity and availability of the data collected, analysed, shared and generated during IoT and AI operations in an ICT system operating within a smart city context within diverse application domains (public safety, transport, energy). It also assesses the reputability of the data collection process and the data processed in relation to its impact on an ICT system's performance and behaviour to achieve and maintain cyber resilience. In addition, it equips CERTs/CSIRTs with a state-of-the-art incident information sharing and response toolkit to mitigate large-scale cybersecurity incidents.

To combat emerging IoT and AI attack vectors, there is an urgent demand for threat detection and intelligence frameworks and toolkits that are "collaborative-first". Specifically, information sharing is privacy-oriented and is designed to support European CERT and CSIRT networks with tools for autonomous collaborative threat intelligence (detecting, sharing, advancing timely awareness, collaborating, responding, and recovering) via AI-enabled human-in-the-loop companions, and to crucially support continuous federated pan-European and human-centric training community platforms.

Several ongoing research and development activities report the need of the society to efficiently handle threat intelligence, security information, and incident sharing for the effective prevention, management and response of cyber-attacks against services or critical infrastructures. There is increased ongoing effort, coordinated by ENISA, to establish a de facto platform for security information sharing, secure online communication and collaboration among all relevant stakeholders offering services or owners of CIs (Operators of Essential Services) and CERTs/CSIRTs in a distributed architecture (i.e., different instances running at the infrastructure of different authorities).

1.1 Deliverable Purpose

This deliverable presents the IRIS-Enhanced MeliCERTes Ecosystem, its vision and concept, and describes in detail the respective implemented IRIS-Enhanced MeliCERTes platform (EME). It shades light on the architectural design of the platform, on the objectives and requirements that were set and addressed, on the functionalities that the system delivers and on the implementation details of the platform.

1.2 Relations to other activities

This document is the main deliverable of T4.6. It aims to demonstrate the design and implementation details of the EME platform. It is closely related to Deliverables D2.2 and D2.6 that describe the user and technical requirements and the IRIS platform and reference architecture respectively.



In addition, since the IRIS-EME ecosystem closely interacts and integrates, both at backend but also at UI level, all the technical developments conducted in the framework of WP4, this deliverable is closely linked to all the WP4 associated deliverables. Moreover, this report is associated with D6.3 that describes the integrated IRIS platform (1st release) since the backend integration tests of the IRIS-EME platform and the respective results have been described there. Lastly, it is associated with WP7 deliverables that concern the IRIS pilot use cases, providing inputs for the implementation of the latter.

1.3 Document Overview

Section 1 provides the introduction of the present Deliverable.

Section 2 presents in brief the IRIS-Enhanced MeliCERTes platform's concept, including the IRIS-EME ecosystem placement within the IRIS defined architecture, the IRIS-EME high level objectives/vision and the platform's requirements.

Section 3 contains the IRIS-Enhanced MeliCERTes detailed design, internal platform architecture, constituent components description, as well as it details the IRIS-EME implementation approach and its operational workflows.

Section 4 outlines the functional and operational details of the unified IRIS-EME dashboard, that unites at UI the information (and individual UIs) of the other IRIS components of WP4.

Section 5 presents the IRIS-EME platform deployment and validation information.

Finally, Conclusions provide a summary of the work that has been presented in the deliverable and mention the future steps that concern the IRIS-EME platform updates and use within the remaining project activities.



2 IRIS-ENHANCED MELICERTES PLATFORM (EME)

OVERVIEW

The IRIS project envisions a single secure platform addressed to CERTs/CSIRTs as well as OESs (Operators of Essential Services) for assessing, detecting, responding to and sharing information among each other, regarding threats & vulnerabilities of IoT and AI-driven ICT systems. The IRIS-Enhanced MeliCERTes platform, thus, constitutes a distributed ecosystem hereinafter mentioned as IRIS Enhanced MeliCERTes Ecosystem (EME), which aims to help European CERTs/CSIRTs to collaborate effectively among themselves as well as with CI Operators, in order to minimise the impact of cybersecurity and privacy risks as well as the threats introduced by cyber-physical vulnerabilities in IoT platforms and adversarial attacks on AI provisions and their learning/decision-making algorithms.

In a nutshell, the main objective that the EME aims to address is to develop a collaborative threat intelligence and information sharing toolkit that allows ICT stakeholders and European CERTs/CSIRTs to create and seamlessly share context-rich information about cyber threats which are targeting IoT and AI-driven ICT systems, as well as, relevant incidents and recommended response actions.

2.1 MeliCERTes CSP

The core IT platform upon which the IRIS-Enhanced MeliCERTes platform has been developed has been the open source MeliCERTes CSP, 2nd version¹.

The Cyber Security Platform MeliCERTes is part of the European Strategy for Cyber Security. MeliCERTes is a network for establishing confidence and trust among the national Computer Security Incident Response Teams (CSIRTs) of the Member States and for promoting a swift and effective operational cooperation. Member States CSIRTs participate on an equal footing in the MeliCERTes Core Service Platform (CSP) within verified Trust Circles for sharing and collaborating on cyber security incidents.

The MeliCERTes primary purpose has been to facilitate cross-border co-operation encompassing data exchange among two or more computer security incident response teams (CSIRTs) based on the concept of trust circles. MeliCERTes uses open-source tools developed and maintained by the CSIRT teams. This allows the collaboration between the CSIRT teams, including incident management, threat intelligence, secure communications, and artefact analysis.

¹ [Open platform and tools to facilitate the collaboration among Computer Security Incident Response Teams — ENISA \(europa.eu\)](#)



The core component of MeliCERTes 2 is Cerebrate². Cerebrate is an open-source platform meant to act as a central tool for MeliCERTes 2 and provide a central interface to manage different tools and different settings for them, thus offering tight integration with various open-source security tools. Cerebrate provides a way to build an open source security ecosystem of tools in pursuit of enabling organisations' autonomy and independence. Cerebrate also integrates a versatile directory solution to manage constituents, members and partners in information sharing communities such as ISACs, CSIRT networks or any closed or public sharing groups.

MeliCERTes CSP (both MeliCERTes 1 and MeliCERTes 2) have now concluded their activities, having released the MeliCERTes platform as open source software, accessible at: [MeliCERTes Project - knowledge base | docs](#).

Within IRIS, the Enhanced MeliCERTes Ecosystem will form the basis of developments and will be extended to facilitate Collaborative Cyber-Threat Intelligence Sharing, among CI Operators (e.g., smart city infrastructure operators, IoT infrastructure operators, etc.) and CERTs/CSIRTs with focus on AI and IoT relevant threats and attacks on such infrastructures. The Enhanced MeliCERTes ecosystem (EME) incorporates the majority of the technical developments that concern CTI and incident information sharing and acts as a distributed CTI and incidents information sharing and collaboration interface towards the envisaged users of the IRIS platform. EME is developed as a distributed and customized solution and provides more secure and trusted online communication, collaboration and information sharing among CI operators and CERTs/CSIRTs with a unified customizable dashboard.

IRIS extends the capabilities of the open source MeliCERTes platform and enhances the existing MeliCERTes ecosystem used today by CSIRT/CERT teams by:

- Extending its use to another major user type, that of OESs/CI Operators, providing the respective role and rights management functions for the diverse types of users and roles and their access, according to the need to know principle, to the managed and shared cybersecurity information.
- Integrating (through the IRIS Orchestrator) with the IRIS Automated Threat Detection Tools deployed on the respective critical/smart city infrastructure, and aggregating/visualizing relevant information on critical infrastructure assets, potential automatically detected threats, attacks and incidents, that are immediately communicated/shared in real-time to the respective stakeholders with need to know rights to ensure timely situational awareness, information sharing and trigger response actions.
- Providing advanced cybersecurity incident reporting and management (SIEM) capabilities
- Offering advanced and more extended information visualisations and customizable UIs/frontend with respect to both access and visualization of information as well as dashboard service provisioning, depending on the accessing user role,

² <https://doc.cerebrate-project.org/>

- Integrating distributed ledger technology for integrity and accountability of aggregated stored information,
- Providing rich threat intelligence capabilities
- Enabling timely (real-time) CTI and incidents information sharing to all users/roles within an extended Trust Circle, that now includes other types of users (CI Operators, Operators of Essential Services, etc.) further from CERTs/CSIRTs
- allowing the definition and enforcement of information sharing policies among the users/roles of the extended Trust Circle
- allowing the apriori definition and customization of automatic or not response actions to known threats and attacks per type of Critical Infrastructure/Asset.
- offering an online collaboration and communication environment among different types of users or communities (CIRTs/CSIRTs, CI Operators/OESs, ISACs, etc.).
- IRIS aims to address a larger user base approach, involving not only CERTs/CSIRTs, but also stakeholders from the IoT and AI domain, service operators, and critical infrastructure providers. IRIS, by extending the MeliCERTes platform, aims to become a flagship operational security system not only for CERTs/CSIRTs, but also for a broader network of cybersecurity professionals and operators of essential services.

2.2 EME ecosystem in IRIS architecture

The final version of the IRIS architecture is described within D2.6 and is illustrated in the following figure:

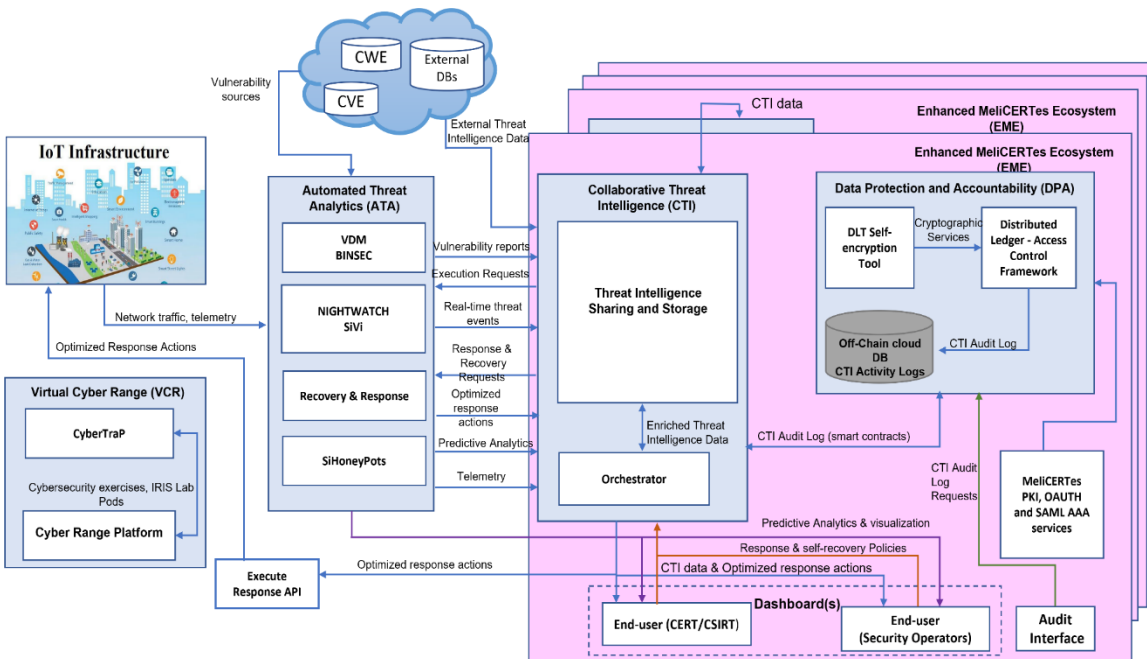


Figure 1: IRIS High-Level Architecture (Tool View)



The IRIS architecture is established in two main pillars namely the Automatic Threat Analytics (ATA) tools that adhere to the AI and IoT related threat detection modules and the IRIS-Enhanced MeliCERTes Ecosystem (EME). More specifically, the EME consists conceptually of the following components:

CTI Sharing and Storage, which enables the collection, storage, correlation and sharing of information about threats, attacks and vulnerabilities from internal and external sources. CTI Sharing and Storage facilitates CTI enrichment based on correlation techniques. The enriched CTI is stored in the CTI Sharing and Storage tool which is based on the MISP platform and corresponds to a platform for storing and disseminating CTI in a secure and efficient manner and in a (semi-) automatic way. CTI Sharing and Storage module is described in D4.1 and D4.2. The sharing procedure enables different interested parties (CERTs, CSIRTs etc.) to be informed in a proper time about the cyberattack landscape. The CTI Sharing and Storage component provides a user-friendly dashboard thus the user can use it to interact with the stored CTI.

DPA, module was designed to support auditing functions for incident responses, ensuring accountability and traceability based on a combination of distributed ledger technologies (DLT), blockchain, self-encryption, and secret key sharing technologies. The DPA enables the traceable, immutable and safe storage of audit data, with access control policies enforced by several blockchain nodes. It leverages the capabilities of the Hyperledger Fabric (HLF) permissioned blockchain to provide an auditing service, as well. DPA is described in detail in D4.6.

ATIO, Advanced Threat Intelligence Orchestrator (ATIO) is a full stack solution, that acts like a middleware system, due to its central location in the architecture, all the data being transferred via it. Therefore, ATIO links ATA, EME (which includes CTI and DPA) and the infrastructure ATIO is described in detail in D4.3 and D4.4. Four backend services and two frontend services compose ATIO. Also, an OPEN-API framework circles it in order to make the component data interoperable.

IRIS-EME platform, of the IRIS-Enhanced MeliCERTes ecosystem (EME) in IRIS is a, timely Incidents and CTI information sharing and reporting, as well as online communication and collaboration platform with an advanced and customizable UI and service provisioning per type of user/role with advanced information visualizations, and backend services for users/roles/rights management, information sharing policies (Trust Circles) management and automatic response actions configuration capabilities. It thus provides a secure and trusted online communication, collaboration and secure information sharing, incidents reporting and management with appropriate response actions among CI operators and CERTs/CSIRTs allowing them to interact with the IRIS platform through a unified customizable dashboard. It further ensures interoperability of information shared among the different EME instances in their distributed setup, but also with other widely used platforms such as MISP.



2.3 IRIS EME platform's high-level objectives and vision

In IRIS, the EME design is driven by a set of key objectives. More specifically the IRIS EME aims to:

- Allow for more secure and efficient security information representation in standardized formats and sharing capitalizing and extending existing ontologies and standards, such as STIX 2.1³ and CACAO playbooks⁴.
- Securely share any type of disclosed information for better preparedness, detection and response capabilities (such as threats, vulnerabilities, incidents, countermeasures, etc.). Thus, promoting wide awareness among the need to know stakeholders within the Trust Circles in a much more timely manner, at the time of occurrence in the case of detected threats and incidents.
- Securely communicate and collaborate online with a more extended pool of stakeholders/operators of essential services or Critical Infrastructures (CI) and with the CERT/CSIRT authorities, capitalizing on the capabilities of the underlying technologies of the proposed enhanced MeliCERTes ecosystem.
- Securely store and augment the cybersecurity knowledge base of AI and IoT systems targeted attacks, incidents, countermeasures, etc. at a European level.
- Provide customized views of its dashboard, 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.
- Offer Authentication and Authorisation (AAA) services such as OATH2, SAML and PKI.
- Follow a distributed architecture approach allowing the enhanced MeliCERTes ecosystem to customized deployments at stakeholders' premises.

2.4 IRIS EME platform's requirements

In this section, the IRIS platform's requirements that need to be addressed by the IRIS EME platform, as presented in D2.6, are shown in a tabular format, alongside presenting their achievement during the implementation of the EME platform prototype, presented in the current Deliverable. These requirements, distinguished in functional and non-functional ones, are either directly or less relevant to the IRIS EME platform. All have been successfully implemented in the released EME platform prototype.

³ [Introduction to STIX \(oasis-open.github.io\)](https://oasis-open.github.io)

⁴ [OASIS Collaborative Automated Course of Action Operations \(CACAO\) for Cyber Security TC | OASIS \(oasis-open.org\)](https://oasis-open.org/)



ID	Name/Description	Priority	Achieved
F-DCA-01	The IRIS platform requires being able to support multiple simultaneous users (FUNC-End_User-03) working either independently over the same replicated infrastructure (or on different infrastructures) or cooperating as a team on a single target (T_PLAT-VCR-03)	High	✓
F-DCA-03	Requires being able to provide/receive input about the recommended response measures (FUNC-CTI-10, FUNC-EME-02)	High	✓
F-DCA-04	Being able to receive a risk-based optimisation/ranking information that will support CSIRTs/CERTs on decision making (FUNC-EME-03)	High	✓
F-DFO-01	IRIS Platform requires to contain a standardized taxonomy/ontology mapped to widely used, e.g., STIX 2.1, MISP Standards, etc (FUNC-End_User-10, T_PLAT-CERT-01, FUNC-EME-04, T_PLAT-EME-01)	High	✓
F-DFO-03	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 (FUNC-End_User-06).	Medium	✓
F-DST-01	Requires being able to securely store and enrich the cybersecurity knowledge base of AI targeted vulnerabilities, attacks, incidents, countermeasures, etc. at a European level (FUNC-EME-09, FUNC-ATA-06)	High	✓
F-DST-08	Requires being able to store and augment the cybersecurity knowledge base of AI targeted attacks, incidents, countermeasures etc. at a Pan-European level (FUNC-EME-06)	Medium	✓
F-DSH-01	Collaborative information sharing will enable the ability to classify information such as the traffic light protocol TLP (FUNC-CERT-04)	High	✓
F-DSH-02	Requires being able to use intelligence sharing functionalities, for the knowledge base enrichment (FUNC-ATA-04) which will enhance existing MeliCERTes platform for CTI, threat sharing and monitoring of services (FUNC-CERT-01)	High	✓
F-DSH-04	The IRIS platform should provide real-time communication and collaborative information sharing (FUNC-CERT-06)	Medium	✓
F-DPR-07	Requires being able to detect general vulnerabilities of the target system and attacks which involve common threat actor techniques (FUNC-CERT-02)	High	✓
F-DPR-12	Requires enabling autonomous response by allowing the human-in-the-loop (CERT Response Operator) to make the decision on response actions to detected threats (FUNC-CERT-03)	High	✓



ID	Name/Description	Priority	Achieved
F-DRV-02	Requires being able to present through GUI/unified Dashboard, the collected cyber threat intelligence related information to the participating entities e.g., organizations and CERTs/CSIRTs (FUNC-EME-01)	High	✓

Figure 2: IRIS platform's functional requirements relevant to EME

ID	Name/Description	Priority	Achieved
NF-OPE-01	Requires being able to perform actions either automatically or manually, as needed by the end-user (FUNC-End_User-09, FUNC-ATA-08)	High	✓
NF-OPE-15	IRIS components are required to access locally, and in an off premises / hosted / cloud environment (T-PLAT-End_User-01)	High	✓
NF-OPE-16	Requires being distributed, with different customized instances deployed at each stakeholders' premises (FUNC-EME-10)	High	✓
NF-OPE-17	The IRIS platform should provide threat analysis within a range of 5 minutes to 1 hour after an incident alert (FUNC-End_User-05).	Medium	✓
NF-OPE-18	IRIS platform should provide timely automated response and recovery results within a range of near real-time to a few minutes (FUNC-End_User-08).	Medium	✓
NF-SEC-05	Requires being able to provide access control and access rights to access, use and shared data in accordance with the type of User/Operator and the type of Service/Infrastructure they provide (T_SECU-EME-03, T_USAB-EME-02, Ethics_15)	High	✓
NF-SEC-10	Requires being able to securely communicate and collaborate online with a more extended pool of stakeholders/operators (FUNC-EME-08)	High	✓
NF-USB-04	Requires being able to provide customized views of its dashboard and security incident reporting capabilities (FUNC-EME-07, T_USAB-EME-02)	High	✓
NF-USB-06	The IRIS Platform should be available 24/7 (FUNC-End_User-01)	Medium	✓
NF-MPR-02	Tools developed for the MeliCERTes ecosystem should be interoperable with other tools and enable extensibility (FUNC-CERT-07)	Medium	✓
NF-MPR-03	The tools created for the enhanced MeliCERTes ecosystem should provide open APIs that are shared with CERTs/CSIRTs and third parties (FUNC-CERT-08)	Medium	✓



ID	Name/Description	Priority	Achieved
NF-MPR-04	The IRIS platform should be constructed of a modular design, allowing tools integrated within MeliCERTes platform to be also used as a stand-alone (FUNC-End_User-02)	Medium	✓
NF-PVC-01	IRIS platform requires being GDPR compliant (FUNC-End_User-11) and use existing privacy enhancing features of the MeliCERTes ecosystem such as the trust circles feature (FUNC-CERT-05)	High	✓

Figure 3: IRIS platform's non-functional requirements relevant to EME

3 IRIS-ENHANCED MELICERTES PLATFORM DESIGN

The IRIS-EME platform design is driven by the IRIS-EME objectives, vision and requirements that were defined by the IRIS platform architecture, as presented in sections 2.3 and 2.4. These present the fundamental basis for proceeding in designing the EME platform internal components and architecture in detail, determining the respective operational workflows for proceeding further to its implementation. This section presents the detailed architecture and design specification of the IRIS EME platform.

3.1 IRIS-EME platform Architecture

The IRIS-Enhanced MeliCERTes platform capitalises for its implementation on and integrates effectively open source software tools (e.g. Keycloak IMS) for user/roles/rights management and the open source MeliCERTes CSP 2 open source software. In addition, it incorporates an advanced custom-made unified dashboard for its diverse target users, a Pan-European IoT and AI cyberthreats knowledge base and additional supporting components (e.g. REST API).

The IRIS-EME platform as it is natively modular, configurable and customizable, offers two distinct modalities. The first one is materialized as the IRIS-EME platform instance within the IRIS EME ecosystem subsystem, that is integrated with the IRIS ATA subsystem instance, all deployed and residing on the Critical Infrastructure side, tailored to be used by CI Operators/OESs. The second one concerns the IRIS-EME platform instance within the IRIS EME ecosystem subsystem, that is tailored for the CERTs/CSIRTs cybersecurity authority operators and is deployed at their premises. IRIS-EME platform distributed deployments lead to multiple points of presence, operating at Pan-European level, following the cloud native, thus guaranteeing high availability, scalability, and reliability. Figure 4, illustrates the high-level interactions that enable the collaboration and sharing of the CTI detected threats and incidents via the IRIS platform.

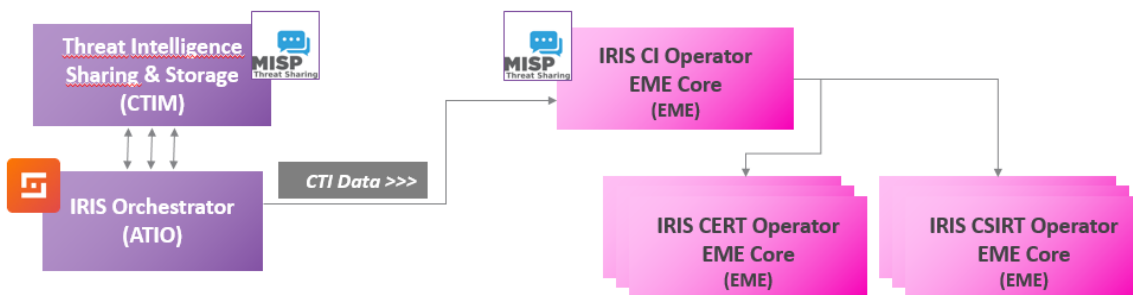


Figure 4: IRIS EME high-level communication

3.1.1 IRIS-EME platform (CI Operator instance)

The IRIS-EME platform instance for the CI operator interconnects directly and remotely with the rest of the IRIS-EME ecosystem components namely, the ATIO, the DPA and the CTI sharing and storage modules. The relevant architecture is presented in Figure 5.

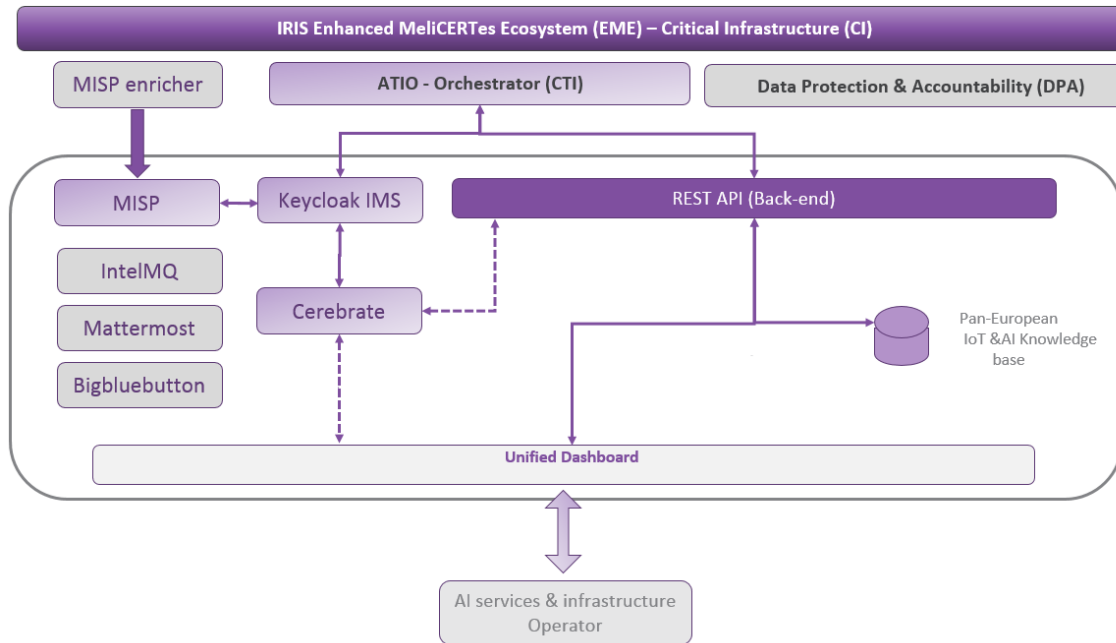


Figure 5: IRIS-EME CI operator's instance architecture

The IRIS-EME platform receives the CTI events/incidents related to novel IoT and AI-based (e.g., machine learning) threats targeting ICT systems that are detected by the IRIS platform ATA deployed tools at the Critical Infrastructure and communicated to the EME-platform through the ATIO module. The ATIO module is the interface with the IRIS platform and more specifically with the IRIS detectors (ATA tools).

In addition, the IRIS-EME platform incorporates a MISP instance, that is managed by the CTI sharing and storage component. CTI Sharing and Storage facilitates CTI enrichment which is based on correlation techniques, as described in D4.2. The enriched CTI is stored in the CTI Sharing and Storage tool which is based on the MISP platform enabling storage and dissemination of CTI in a secure and efficient manner.

Also, the IRIS-EME platform is remotely integrated with the DPA module enabling the storage of audit logs that capture the IRIS user response (mitigation action) with respect to an identified threat into the blockchain that is managed by the DPA.

3.1.2 IRIS-EME platform (CERT/CSIRT Operator instance)

The IRIS-EME platform instance that is configured for the CERTs/CSIRTs operator interconnects directly both to the CI and CERTs/CSIRTs instances of the IRIS-EME platform. Figure 6, visualises the afore-mentioned schema.

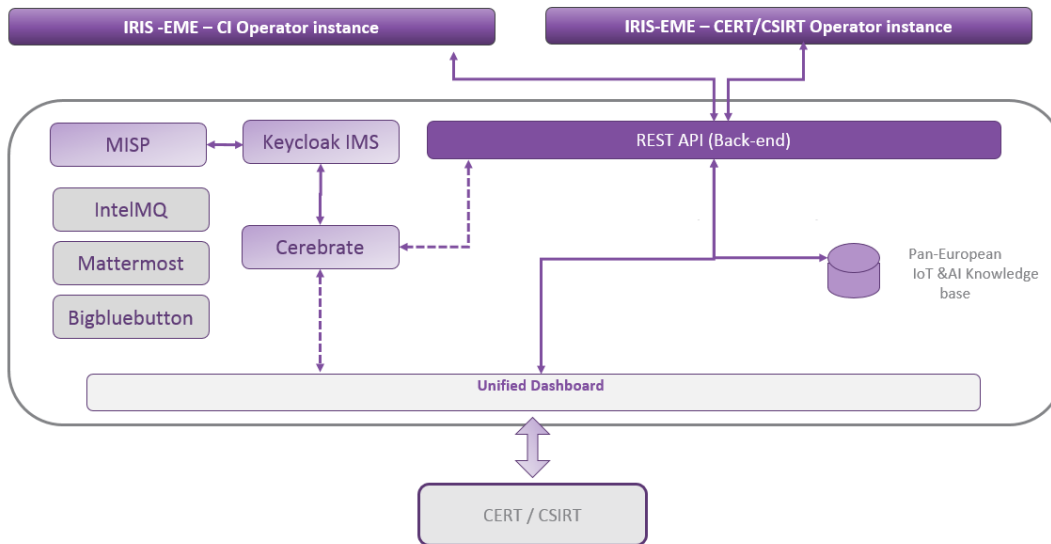


Figure 6: IRIS-EME CERT/CSIRT instance architecture

3.2 IRIS-EME platform components

The IRIS-EME platform consists of a selection of MeliCERTes CSP 2 developed components which are extended and configured to implement the target objectives and functionality. More specifically, within the system the following components are included:

Cerebrate (MeliCERTes 2): Cerebrate supports the IRIS users and organizations definitions offering a visual environment for managing IRIS user roles and entities that results to the description of sharing groups (Trust Circles). The sharing groups drive the CTI communication and sharing of the CTI data that are generated by the IRIS platform.

Keycloak IMS: Identity and access management solution that supports the secure authentication and authorization of IRIS users and services.

Unified Dashboard: Unified visual environment (dashboard). The UI facilitates the CTI information visualization and implements the operational workflows for situational awareness, information sharing, incident reporting, response and communication and collaboration for the needs of the target IRIS users. The unified dashboard integrates all the IRIS developed visual environments in a loose manner, safeguarding the coherence of the IRIS platform towards its users.

REST API and **Pan-European IoT & AI Knowledge base** to facilitate Dashboard communication with the other IRIS components and provide a continuously updated and informed storage medium for the exchanged information and knowledge base with IoT and AI aggregated threats, of the platform.

MISP: MISP instance that is managed by the CTI Sharing and Storage module (part of MeliCERTes CSP 2).



INTELMQ: An auxiliary communication channel that will support the collection and processing of security feeds through a message queuing protocol. INTELMQ is developed in the framework of MeliCERTes CSP 2.

BigBlueButton/Jitsi: An open-source multiplatform voice, video conferencing and instant messaging application for the Web platform.

Mattermost: An open-source, self-hostable online chat service with file sharing, search, and integrations. It is designed as an internal chat for participating organisations.

3.3 IRIS-EME platform implementation

The IRIS-EME platform development adheres to modular design and programming principles. The components that comprise the system are built as independent building blocks and can independently function minimizing the dependencies between the system's modules. Integrating modular applications into a unified solution allows the system to provide the required functionality that was designed for. This enables the platform to be easily integrated, but most importantly easily maintained.

The IRIS-EME developed services can be updated progressively or even replaced, as might be required in the future, without affecting the operation of the whole system. This is of great importance for the sustainability of the platform as it is envisaged to be exploited by the IRIS platform not only within the timespan of the project's duration but also well beyond that.

Moreover, the implementation of the IRIS-EME platform, as it presents a complex system that integrates multiple modules (services and applications), required well-defined interfaces, data models, data base schemas, etc. In addition, the utilization of standardized data models, such as STIX v2.1 and interfaces such as RESTful APIs reassure the integration, adoption and extensibility of the system.

The source code of the IRIS-EME platform is located within the private IRIS instance of GitLab⁵.

⁵ <https://gitlab.iris-h2020.eu/h2020-iris/iris-collaborative-secure-and-trusted-cyber-threat-intelligence-sharing/eme>



3.4 IRIS-EME platform operation

The IRIS-EME platform receives Cyber Threat Intelligence (CTI) data, that follow the Structured Threat Information Expression (STIX) v2⁶ specification, from the IRIS platform's ATIO module through its exposed REST API. The CTI information that is collected by the EME back-end follows a JSON structure. The data follow the STIX v2.1 format for interoperability purposes. More specifically the data model, contains information regarding the ATA tool that detected the event, details on the specific threat that was detected (attack or vulnerability) including event criticality and impact details and the suggested mitigation actions that are proposed through the Unified Dashboard of the EME-CI operator instance to the CI Operator, and which are generated by the IRIS RRR component. The structure of this document is presented below through an indicative example of a CTI event.

```
{
  "type": "bundle",
  "id": "...",
  "objects": [
    {
      "type": "extension-definition",
      "spec_version": "2.1",
      "id": "...",
      "created_by_ref": "...",
      "created": "...",
      "modified": "...",
      "name": "Response action definition",
      "description": "Additional properties defined for the execution of
response actions",
      "schema": "https://.....",
      "version": "1.0",
      "extension_types": [
        "property-extension"
      ],
      "detection": {
        "organisation": "...",
        "detection_name": "...",
        "detection_summary": "...",
        "source": "...",
        "classification": "...",
        "first_seen": "...",
        "last_seen": "...",
        "actor": "...",
        "confidence": "...",
        "risk_score": "...",
        "threat": "...",
        "iris_id": 012
      },
      "policies": {
        "organisation": "...",
        "action_policy": {
```

⁶ <https://docs.oasis-open.org/cti/stix/v2.1/csprd01/stix-v2.1-csprd01.html>



```

    "contain": {
      "isolate": "enabled",
      "block_service": "enabled",
      "shutdown": "enabled"
    },
    "harden": {
      "install_patches": "enabled",
      "disable_service": "enabled",
      "implement_access_control": "enabled"
    },
    "recover": {
      "restore": "enabled",
      "reconfigure": "enabled"
    }
  },
  "criticalities": {
    "organisation": "...",
    "asset_ip": "...",
    "asset_device": "...",
    "criticality": "1"
  },
  "playbook_actions": {
    "type": "playbook",
    "playbook_id": "",
    "spec_version": "cacao-2.0",
    "playbook_standard": "CACAO",
    "name": "playbook name",
    "created_by": "RRR",
    "created": "...-06-14T14:29:22.24089Z",
    "modified": "...",
    "playbook_valid_from": "...",
    "playbook_valid_until": "...",
    "organization_type": "...",
    "asset": "...",
    "risk_score": "...",
    "playbook_impact": "...",
    "playbook_severity": "...",
    "playbook_priority": "...",
    "playbook_type": "...",
    "workflow_start": "3",
    "workflow": [
      {
        "id": 2,
        "impacted_actor": "...",
        "action": "Isolate Host",
        "description": "It is recommended that the host is isolated
from the network to prevent further compromise and impact .",
        "execution_api": "",
        "action_impact": 10
      },
      {
        "id": 3,
        "impacted_actor": "...",
        "action": "Block Host Service",
        "description": "It is recommended that the affected service
is blocked on the host",

```



```

        "execution_api": "",
        "action_impact": 5
    },
    {
        "id": 4,
        "impacted_actor": "...",
        "action": "Shutdown host",
        "description": "It is recommended that the host is shutdown
",
        "execution_api": "",
        "action_impact": 10
    }
]
}}}}

```

Then, the IRIS-EME platform visualizes the CTI event through the EME-CI Unified Dashboard to the IRIS-user and communicates to the eligible IRIS-EME platform instances at national, regional or Pan-European level (included in the respective Trust Circle/Sharing Group of the CI Operator). The CTI information sharing process is orchestrated by the *Cerebrate* component which keeps the IRIS-EME platform instances synchronised. The relevant communication channels are dictated by the Sharing Group defined within the Cerebrate module. The Sharing Group signifies a group of organizations, either CERTs/CSIRTs or CI operators or both that share a common interest or incentive in sharing CTI data, and in the context of IRIS for timely sharing and reporting a detected incident and thus supporting further joint communication and collaboration for its effective management through applicable response actions – this is of utmost importance especially in the cases that new IoT and AI relevant threats and attacks are encountered. In addition to the Sharing Groups, the Cerebrate instance holds information about the individuals and organisations. The functionality of cerebrate is described in Section 3.4.2.

3.4.1 Keycloak IMS

The functionalities supported by the IRIS-EME platform and are related to the provision of Authentication, Authorization and Accounting (AAA) services have been implemented by using the open source software Keycloak⁷, which provides an identity and access management solution and offers OAuth 2.0 authorization framework, SAML 2.0 standard and OpenID Connect for identity management.

⁷ <https://www.keycloak.org/>

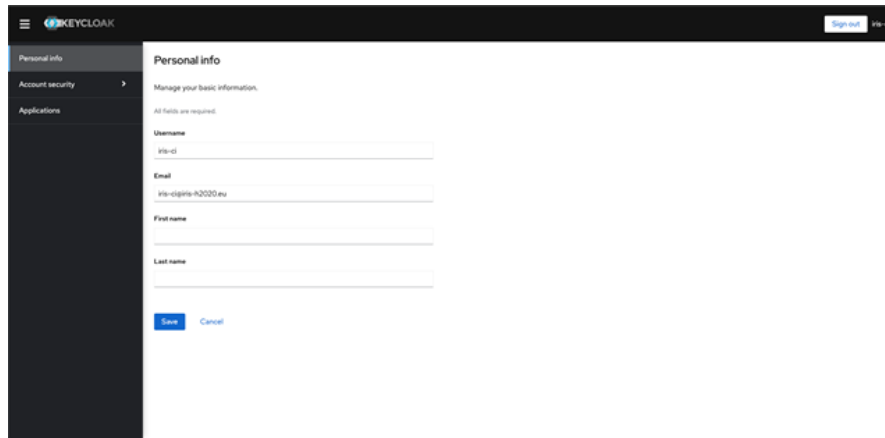


Figure 7: IRIS-EME platform Keycloak IMS

The REST API that the IRIS-EME platform exposes is protected by the Keycloak service. Figure 8, illustrates the process that the ATIO follows in order to be able to reach the IRIS-EME platform. More specifically, the ATIO contacts the Keycloak IMS using the service credential and requests the access token. Upon receiving the access token, the ATIO module incorporates the token into the request that makes towards the IRIS-EME REST API. Once Keycloak validates the token, the request is granted and the ATIO module is able to proceed with the request.

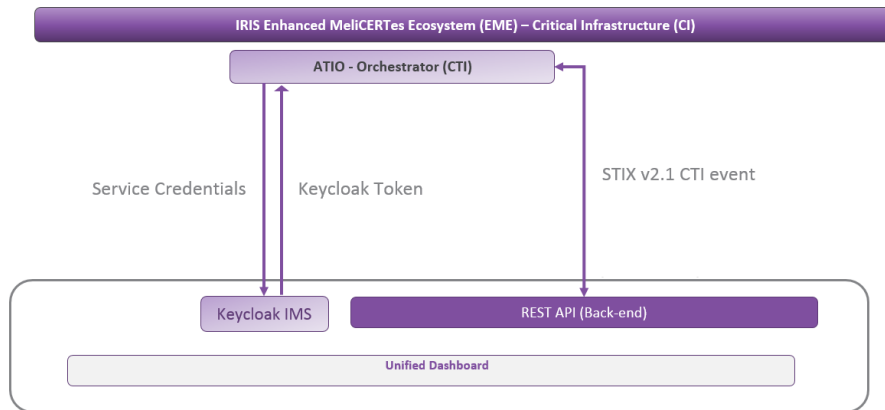


Figure 8: IRIS-EME Keycloak operation via ATIO

Moreover, Keycloak IMS enables single sign on for the IRIS-EME platform user. The user login in the dashboard through the Keycloak is illustrated in Figure 9.

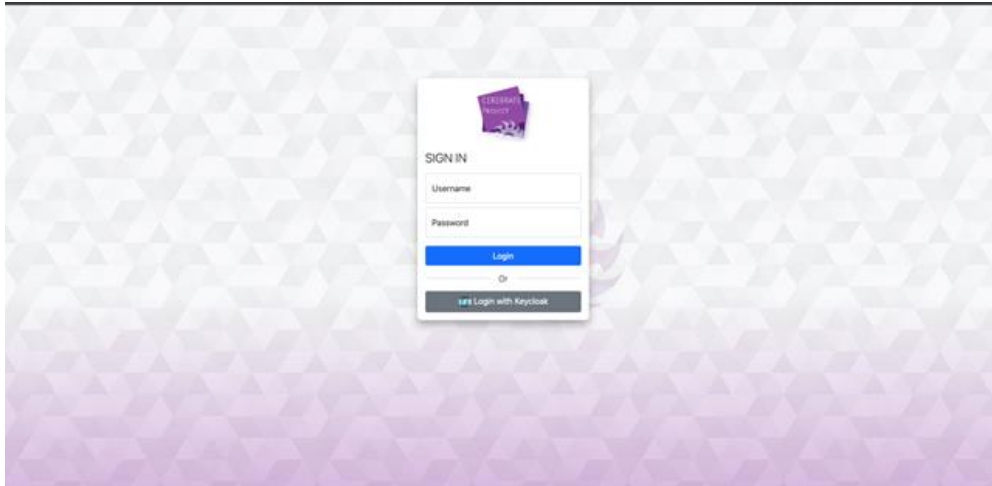


Figure 9: IRIS-EME Keycloak login page

3.4.2 MeliCERTes 2 - Cerebrate

Cerebrate⁸⁹ is the central component of the MeliCERTes ecosystem, providing directory services, information sharing as well as orchestration services for the local tools it interconnects with. All of the local tool components of MeliCERTes are autonomous and can work without Cerebrate, with the latter providing services to facilitate the management and configuration of the connected tools. The architecture provides a high level of resilience without sacrificing each organisation's abilities to pick and choose the components they wish to run based on their specific needs.

More specifically, Cerebrate provides for:

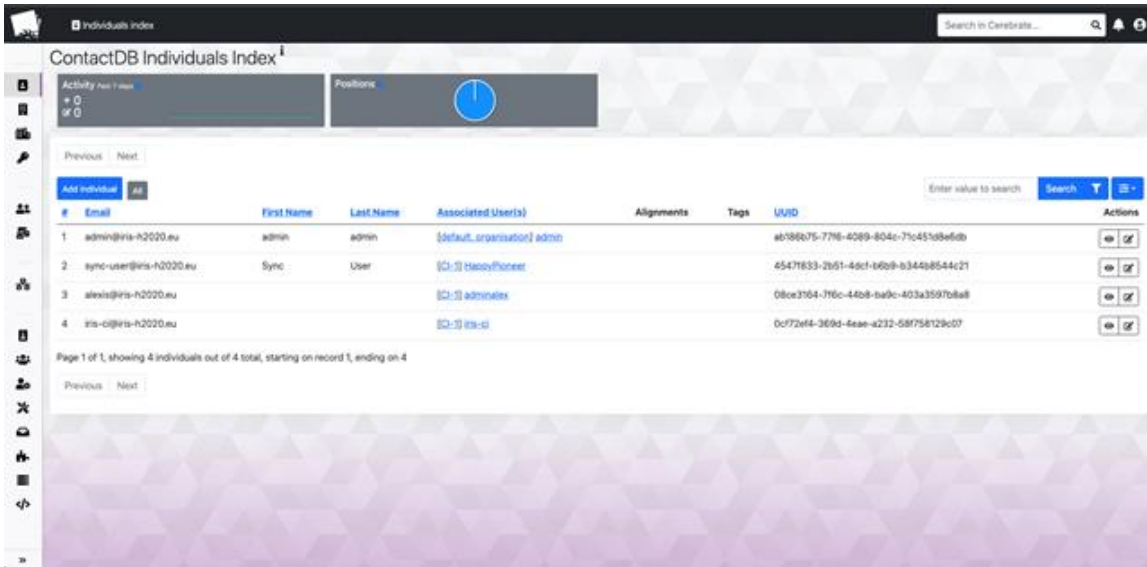
- Advanced repository to manage individuals and organisations;
- Key store for public encryption and signing cryptographic keys (e.g. PGP);
- Distributed synchronisation model where multiple Cerebrate instances can be interconnected amongst organisations and/or departments;
- Management of individuals and their affiliations to each organisation;
- Advanced API and CLI to integrate with existing tools (e.g. importing existing directory information);
- Dynamic model for creating new organisational structures;
- Local tooling interconnection to easily connect existing tools with their native protocols;

In Figure 10 below, the IRIS-EME Cerebrate instance is presented. More specifically, this view describes the users that are registered in a particular IRIS-EME platform instance

⁸ <https://melicertes.github.io/docs/>

⁹ <https://doc.cerebrate-project.org/>

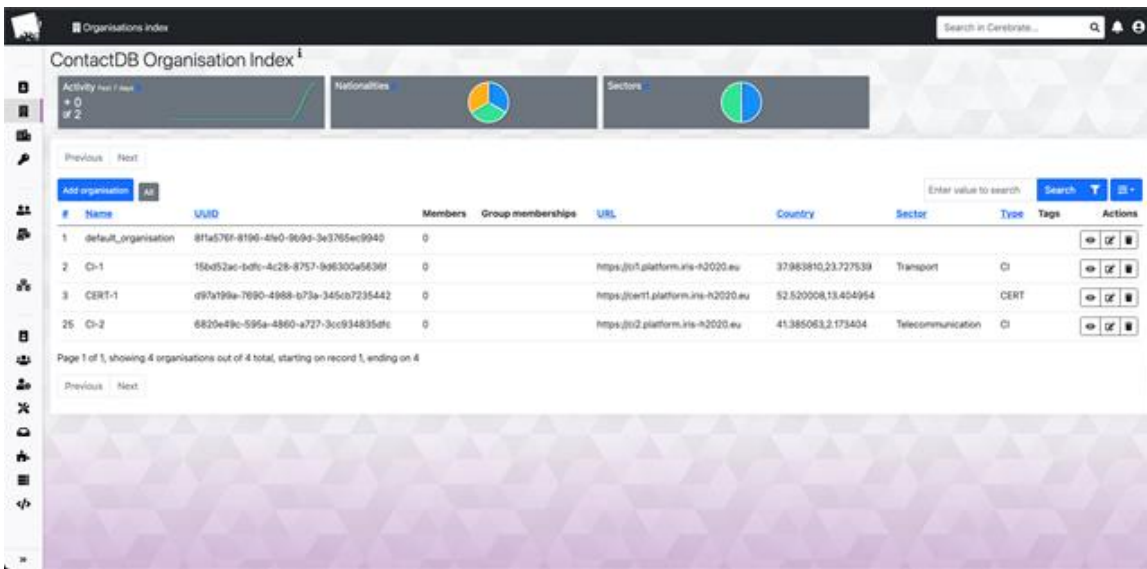
deployment. The particular snapshot is taken from the Cerebrate that is located within (Critical Infrastructure 1) CI-1 IRIS-EME platform instance deployment.



#	Email	First Name	Last Name	Associated User(s)	Alignments	Tags	UUID	Actions
1	admin@iris-h2020.eu	admin	admin	[default_organisation] admin			ab786b75-77b6-4089-804c-75c455b8e6db	[edit] [delete]
2	sync-user@iris-h2020.eu	Sync	User	[CI-1] taseovffloster			45471833-2b51-4dct-b6b9-b344b8544c21	[edit] [delete]
3	alexia@iris-h2020.eu			[CI-1] alexiaalex			08ce3704-7f6c-44b8-ba9c-403a3597b8a8	[edit] [delete]
4	iris-ci@iris-h2020.eu			[CI-1] iris-ci			0c772ef4-369d-4ee4-a232-58756129c07	[edit] [delete]

Figure 10: IRIS-EME platform's Cerebrate view of individual registered users

Figure 11, describes the organisations that are available in the Cerebrate instance. More specifically, the organisations which are visible here are members of one or more Sharing groups (Trust Circles) that the particular organisations, namely CI-1, participate in.



#	Name	UUID	Members	Group memberships	URL	Country	Sector	Type	Tags	Actions
1	default_organisation	811a57ef-819d-4fe0-969d-3a3765ec9940	0							[edit] [delete]
2	CI-1	15cd52ac-bdfc-4c28-8757-9a6300a5636f	0		https://ci1.platform.iris-h2020.eu	37983810,23,727539	Transport	CI		[edit] [delete]
3	CERT-1	097a199a-7690-4968-b73a-345cb7235442	0		https://cert1.platform.iris-h2020.eu	52,520008,13,404954		CERT		[edit] [delete]
25	CI-2	6820e49c-595a-4860-a727-3cc934835dfc	0		https://ci2.platform.iris-h2020.eu	41,385063,2,173404	Telecommunication	CI		[edit] [delete]

Figure 11: IRIS-EME platform's Cerebrate view of individual registered organisations

Figure 12 illustrates the Sharing Groups that the CI-1 organisation participates in. Here the name of that Sharing Group is CERT-1, however it could have been assigned any other name.

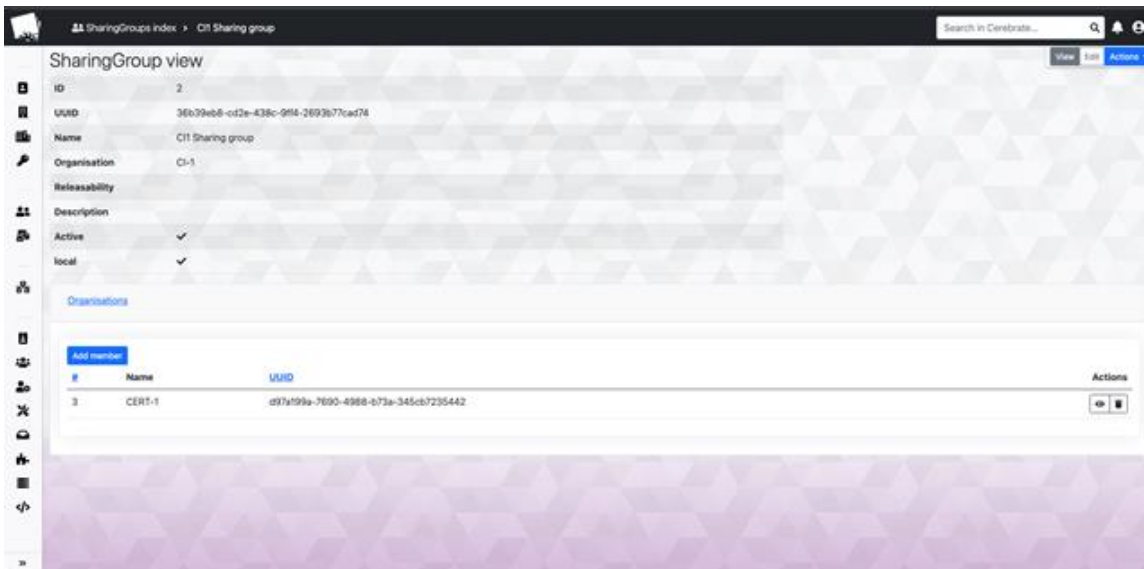


Figure 12: IRIS-EME platform's Cerebrate view of available Sharing Groups

Figure 13 presents the broods that are active for that particular Cerebrate instance. Broods in Cerebrate allow for cerebrate-instance to cerebrate-instance synchronisation.

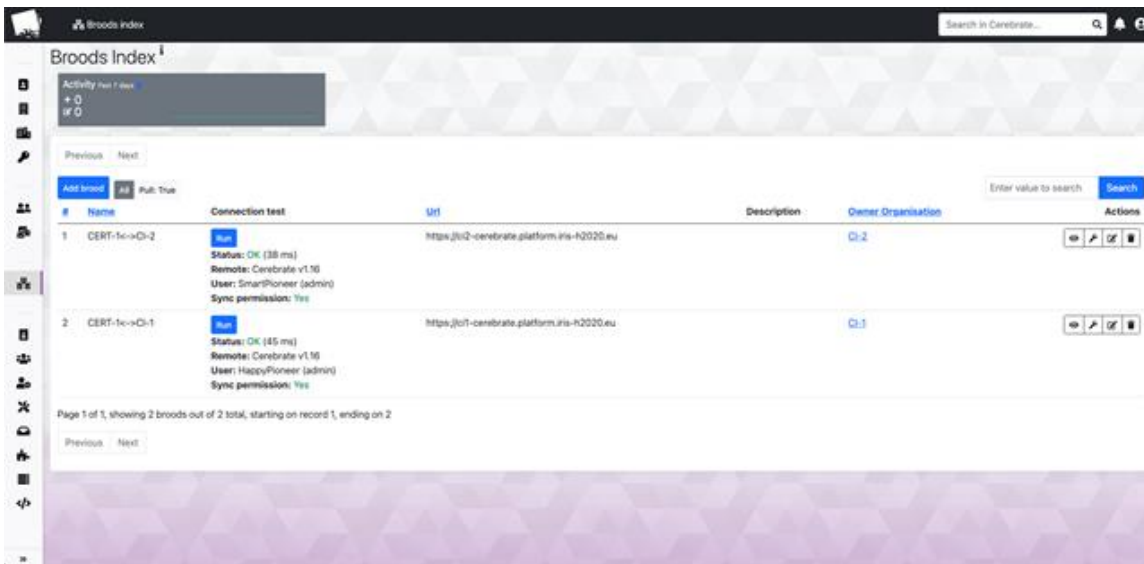
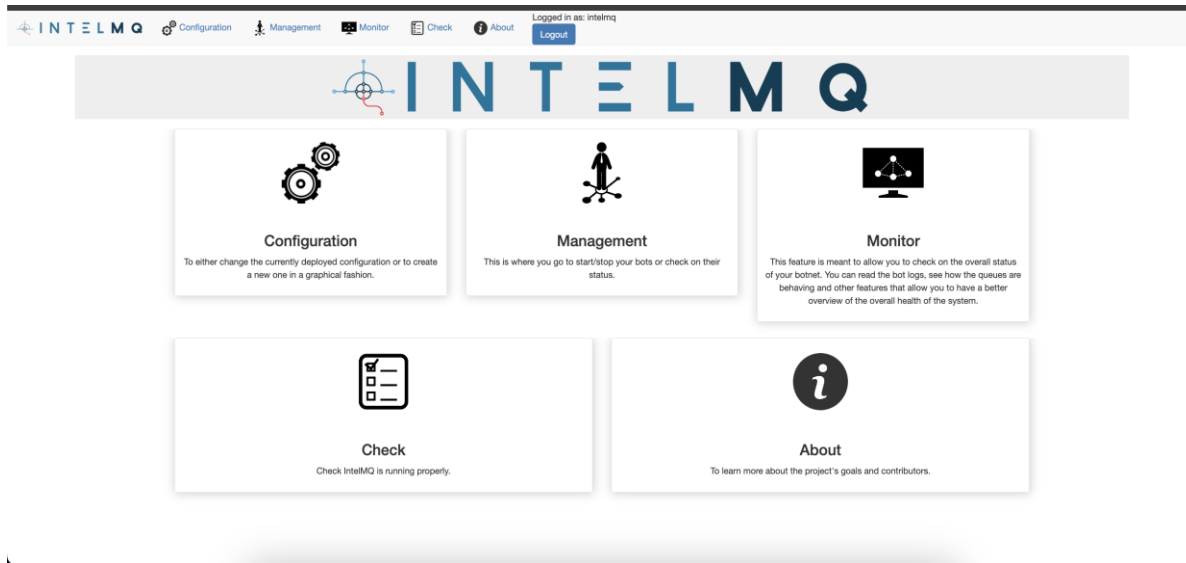


Figure 13: IRIS-EME platform's Cerebrate view of the Broods that allow for data synchronisation among instances of Cerebrate

3.4.3 INTELmq

IntelMQ is a solution for IT security teams (CERTs & CSIRTs, SOC's abuse departments, etc.) for collecting and processing security feeds (such as log files) using a message queuing protocol. Its main goal is to give to Incident Responders an easy way to collect & process threat intelligence thus improving the Incident handling processes of CERTs. The IRIS-EME

platform has incorporated INTELMQ as an additional means of interaction between the extended list of IRIS stakeholders and in a much more timely manner (once an incident is actually detected).



3.5 Interfaces and data models

The REST API that is exposed by the back-end services of the IRIS-EME platform is described in Figure 14. The interfaces can be distinguished in 4 categories, namely: CERT, CI, Synchronisation and Vulnerability scanning requests. More specifically:

- CERT associated endpoints correspond to the API calls that facilitate the communication of the IRIS detected threats towards the IRIS-EME CERT instances.
- CI associated endpoints corresponds to the API calls that facilitate the collection of the CTI threat identified by the IRIS platform by the IRIS-EME platform (CI instance), several filtering and aggregation related functionalities that are provided by the IRIS-EME CI unified dashboard.
- Synchronization endpoints facilitate the synchronization of the information, namely the CTI threat including IRIS users' input (response action), that is communicated by an IRIS-EME CI instance towards the IRIS-EME CERT instances.
- Finally, vulnerability-scanning endpoint supports the vulnerability scanning functionality that is provided through the IRIS-EME CI dashboard. The relevant functionality is described in section 3.9.3.



cert			^
GET	/cert/cis	cert_cis_list	🔒
GET	/cert/threats	cert_threats_list	🔒
GET	/cert/threats/aggregate	cert_threats_aggregate_list	🔒
ci			^
GET	/ci/policy/settings	ci_policy_settings_list	🔒
PUT	/ci/policy/settings/{id}	ci_policy_settings_update	🔒
PATCH	/ci/policy/settings/{id}	ci_policy_settings_partial_update	🔒
GET	/ci/threats	ci_threats_list	🔒
POST	/ci/threats	ci_threats_create	🔒
GET	/ci/threats/aggregate	ci_threats_aggregate_list	🔒
POST	/ci/threats/event	ci_threats_event_create	🔒
PUT	/ci/threats/{threat_id}/playbook	ci_threats_playbook_update	🔒
PATCH	/ci/threats/{threat_id}/playbook	ci_threats_playbook_partial_update	🔒
synchronization			^
POST	/synchronization/eme/threat	synchronization_eme_threat_create	🔒
PATCH	/synchronization/eme/threat	synchronization_eme_threat_partial_update	🔒
vulnerability-scanning			^
POST	/vulnerability-scanning	vulnerability-scanning_create	🔒

Figure 14: IRIS-EME platform's REST API

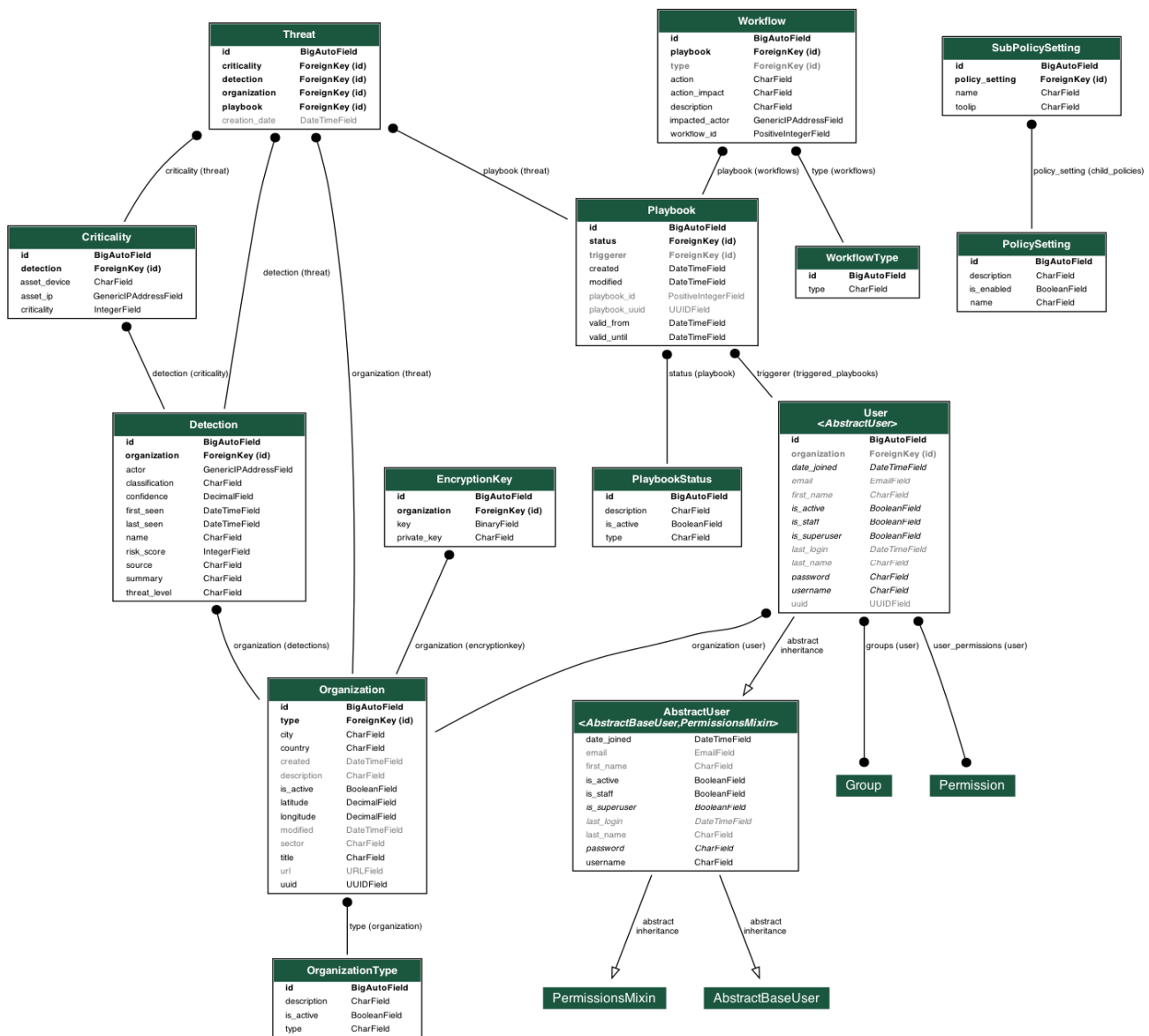
The IRIS-EME platform's backend services exposed through the above-mentioned API utilise a cache architecture with Redis¹⁰. Redis is an in-memory datastore that supports and facilitates caching session data. Redis allows to reduce the load on a primary database while speeding up database reads.

¹⁰ <https://redis.io/>

3.6 IRIS-EME platform Database Schema

Figure 15 presents the IRIS-EME platform's database schema. A database schema refers to the logical and visual configuration of the entire relational database. The database objects are often grouped and displayed as tables, functions, and relations. A schema describes the organization and storage of data in a database and defines the relationship between various tables. The CTI threat data that are visualized in IRIS-EME CI and CERT dashboards are structured (following STIX v2.1 format) and are stored in IRIS-EME platform's distributed relational DB.

Figure 15: IRIS-EME platform's Database Schema





Threat DB table corresponds with the CTI event that is detected by the IRIS platform and is communicated to the IRIS-EME platform and is associated with the following tables:

- Unique ID: Characterizes in a unique manner the CTI event
- Criticality: Describes the criticality of the asset that is targeted by the adversary.
- Detection: Describes the associated CTI event findings, including the threat corresponding Risk, threat level threat summary etc.
- Playbook: Contains information on the mitigation actions that are suggested by the system to the IRIS user. The mitigation actions (one or more) are called Workflows.
- Organization: Holds details about the particular organization that is affected.

User DB table corresponds with the IRIS user. Each group of users adhere to one or more groups that are enabled with a specific set of permissions. In addition, through the DB schema it is evident that one or more users can be associated with one Organization. Finally, a User can trigger one or more playbooks (one for each CTI threats that need to be mitigated by the IRIS platform).

Finally, the Policy DB table holds information that describe the automated responses (one or more) that a user can enable through the IRIS-platform. Then according to each IRIS user's selection regarding the automated response policies that consents to, the IRIS-platform is able to automatically respond (accepting the suggested workflows), thus saving crucial time in view of the mitigation of a detected CTI threat.

3.7 IRIS-EME Unified Dashboard – SIEM

The IRIS-EME platform's unified dashboard application, hereinafter EME-UI, is designed to provide to the IRIS stakeholders (IRIS users) with real-time AI and IoT related Cyber Threat Intelligence (CTI) data that are generated by the IRIS platform's ATA tools' detection mechanisms, on the one hand, enhancing thus their situational awareness, and allow on the other hand to customize both the information sharing and the automated response policies, invoke the relevant operational workflows and execution of the backend IRIS services, and enable the online communication and collaboration among the need to know stakeholders in a Sharing Group/Trust Circle. It further provides a series of advanced information visualization capabilities, as well as information filtering and clustering.

The dashboard application per se is implemented as a full-stack Node.js and JavaScript application utilising the Vue.js framework. The EME-UI is containerized and Kubernetes compliant thus inherently taking advantage of the benefits of Cloud Native computing, guaranteeing increased availability, while assuring efficiency and security.

3.8 Implementation

The EME-UI layout has a fixed navigation sidebar on the left side that enables the user to navigate through the various views of the application. The IRIS logo is placed on the top side, while the username of the IRIS-user along with a configuration icon is placed on the top right corner. When clicking on the icon, a menu pops up that gives the options to log out, visit the home page or view user profile details. This design is consistent in both EME UI flavours that are implemented and which are tailored for the CI operator and for the CERT/CSIRT cybersecurity expert respectively.

3.9 EME-CI UI

The IRIS-EME platform instance that is configured for the CI operator, as mentioned in Section 3.1, incorporates a visualisation environment that is tailored to the CI operator specific needs. Hereinafter, the EME-CI UI collects the CTI events that the ATIO module sends to the IRIS-EME platform and visualises them to the IRIS user that resides on the side of a Critical Infrastructure. Once the CI operator authenticates via the Keycloak login page (Section 3.4.1), then the IRIS user accesses the home page of the dashboard.

3.9.1 EME-CI UI Homepage

The Homepage of the EME-CI UI is presented in Figure 16. It can be distinguished in 5 thematic groups:

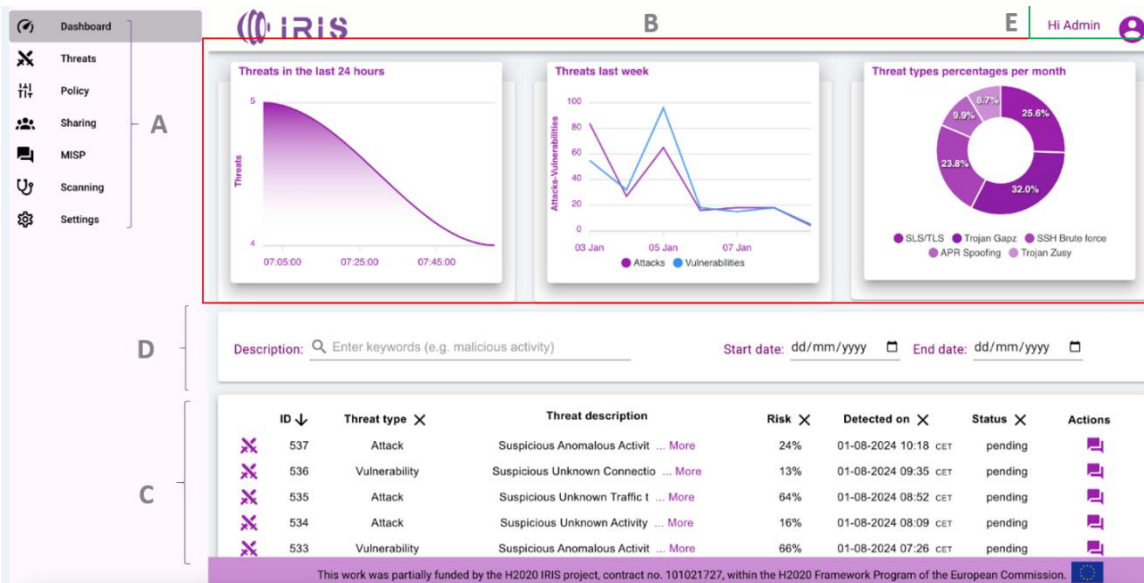


Figure 16: IRIS EME-CI Homepage

Group A: Showcases the side menu item. It holds menu items that navigate the user to other webpages.

- **Threats:** Leads to the Threats webpage which is the detailed view of the incidents reflected in the homepage in **Group C**.



- **Policy:** Leads the user to the Policy webpage where the CI operator is able to set the policies that allow to automate the response on his/her behalf for a given CTI threat (event).
- **Sharing:** Leads the CI operator to the Cerebrate instance that holds the contact details of individuals, organizations, sharing groups and more.
- **MISP:** Leads the operator to the deployed MISP instance that belongs to the organization that the operator affiliates with.
- **Scanning:** Leads to a window through which the user can trigger a Vulnerability Scanning to a specific IP address. Details on the VDM component that is responsible for executing the scan can be found in Deliverable D3.1
- **Settings:** this window, at the time of writing this Deliverable, is not yet used.

Group C: Holds the table of the detected threats that are collected over time. Each line in the table contains brief details on a particular event collected by the IRIS platform. For each event, the following properties are present:

- ID of the event
- Threat type (Can either be attack or vulnerability)
- Threat description (brief description)
- Risk (the identified risk)
- Detected on (the date that was first seen)
- Status (pending if the CI operator has not provided his/her input yet, approved in case that the user accepted the suggested mitigation actions or declined in case the user refused to apply the suggested actions.
- Actions correspond to a communication mechanism that the IRIS platform operator has in order to notify the Sharing group that he/she participates in

The events that are listed in this table can be sorted in ascending or descending order.

Group D: Allows for searching within the CTI events stored in the above-mentioned table about a particular keyword or to limit the CTI event aggregates to a specific time-window.

Group B: Contains 3 charts that present the amount of threats in the last 24 hours or within the last week. The circle chart on the right depicts statistics of the captured events based on the Threat description keywords.

Group E: Illustrates the name of the user who accesses the dashboard and upon pressing the icon, the user is able to logout from the dashboard.

3.9.2 EME-CI UI Policy

Here the IRIS-EME CI operator is able to distinguish the automated response policies that he/she prefers to enforce (if any). Contain, Harden and Recover categories correspond to the response actions (mitigation actions) that are suggested by the IRIS backend RRR component. More details on the classification of these response actions can be found in Deliverable D3.3.

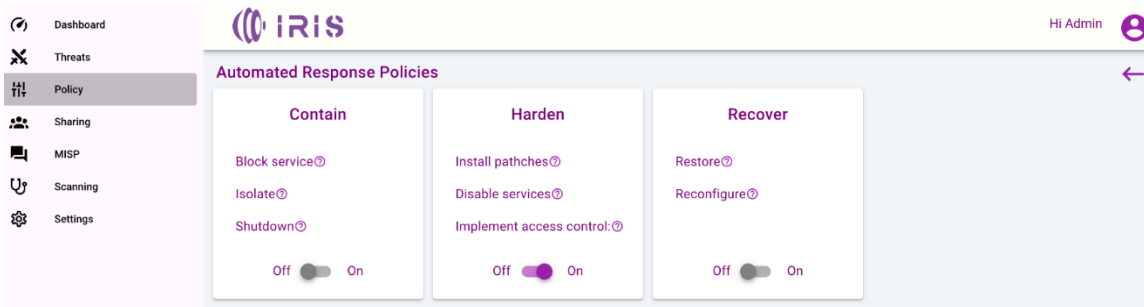


Figure 17: IRIS-EME CI Policy view

Upon hovering the mouse over a *question mark* icon. The explanation of the particular response action is provided. In Figure 18, the relevant feedback is presented.

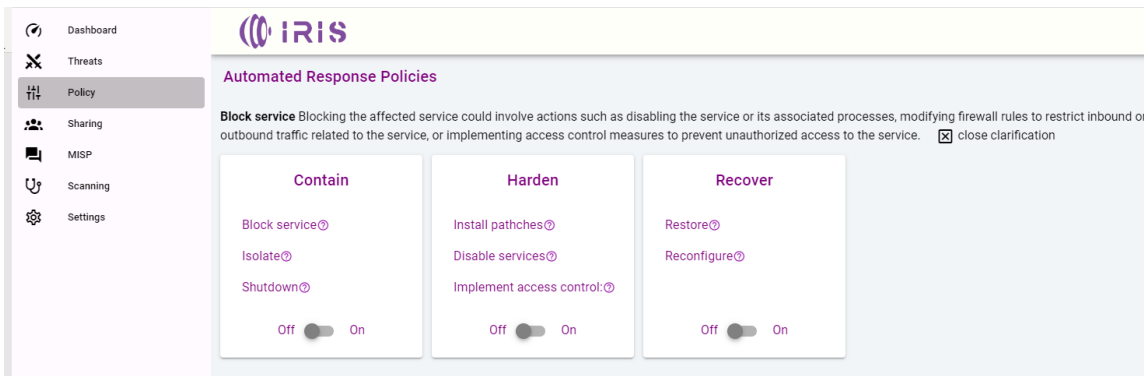
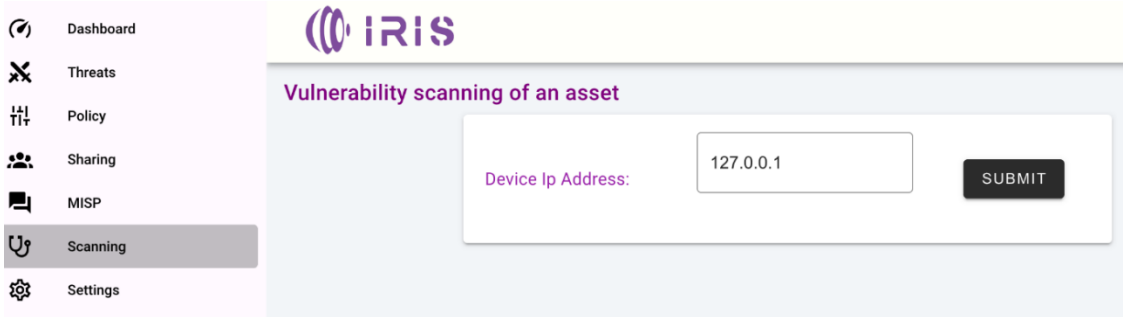


Figure 18: IRIS-EME CI policy explanation

3.9.3 EME-CI UI Scanning

The Scanning view of the IRIS-EME CI UI allows the CI operator to trigger a Vulnerability Scanning for a CI's asset. In the relevant field, the user should declare the desired IP address. Once the Submit button is pressed the procedure is triggered. Once it concludes the potential results will be visible either to the dashboard's homepage table or in the *Threats* view.



3.9.4 IRIS-EME CI UI Threats

The Threats view is illustrated in Figure 19. The main window is separated in two columns. The first one on the right presents the detected events' detailed information. The one on the left offers filtration and aggregation options for the presented threats.

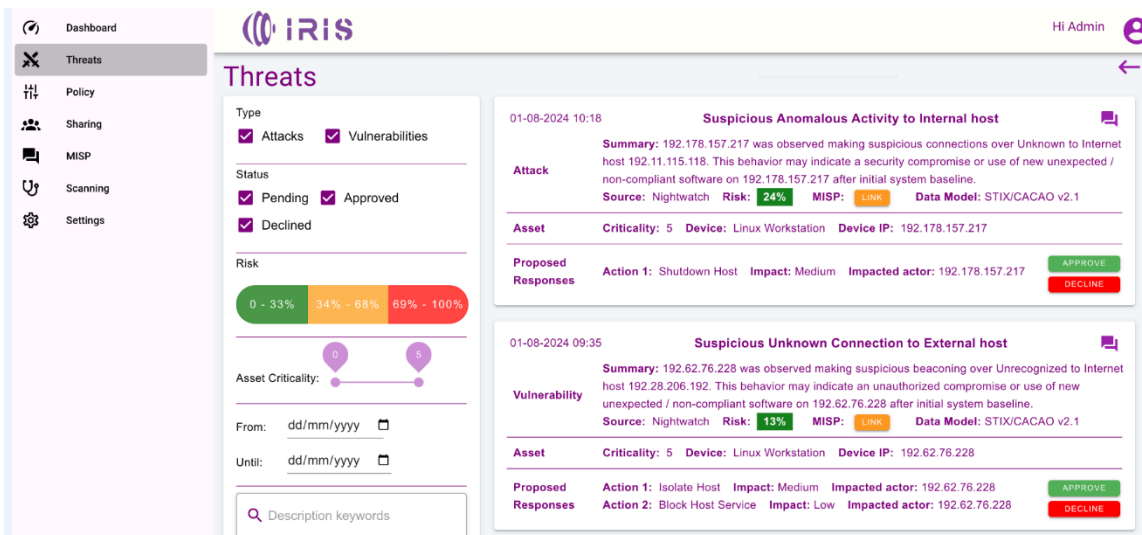


Figure 19: IRIS-EME CI UI Threat view

The events are listed in the relevant webpage of the EME dashboard – “Threats”. A detected threat can either be an attack or a vulnerability. For each threat that is detected by the IRIS platform and subsequently presented by the EME dashboard, various information regarding the *threat*, the *asset* and the *proposed responses* are presented to the user as illustrated in Figure 19. More specifically:

Attack Summary: Presents the detailed description of the threat.

Source: Contains the detector device.

Risk: Describes the identified risk for a specific threat.

MISP: Holds the MISP URL of the specific threat.

Data Model: the associated data model structure of the communicated event.

Asset: Contains information on the affected asset such as the *Criticality* (level of importance), the *name* of the device and its IP address.

Proposed Responses: Presents the suggested mitigation actions to be applied to the affected sub-system.

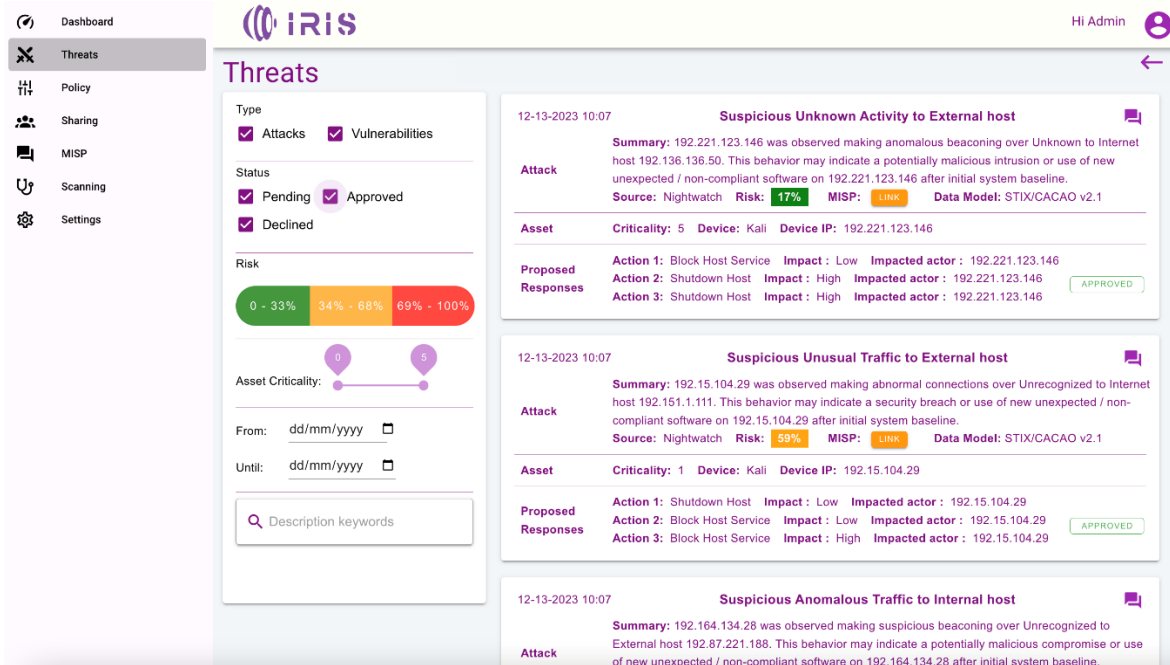


Figure 20: IRIS-EME CI UI Threats view (approved)

In addition, on the left part of the *Threats* view, the user can filter the events that are aggregated here based on their type, status, risk level, asset criticality, their date or aggregated given a particular keyword. By default, the events are organized by date.

An important part of the Threat sharing and response workflow of the IRIS framework concerns the user's feedback to a particular threat. Once the CTI events (threats) are received by the EME ecosystem and the dashboard, the system considers the *Policies'* preferences that are configured by the user. According to that, a proposed response can either be automatically communicated to the supported infrastructure or a user feedback is needed to be provided in order for the system to proceed dispatching the response to the affected system through ATIO. In case of the former the *Proposed Responses* are automatically approved by the system as indicated in Figure 20. If the user feedback is needed then the collected event listing is presented as in Figure 19. Then the user is able to either approve or decline the *proposed responses*.

Finally, once the detected CTI event is *resolved* (Figure 20), the relevant information is communicated to the CERTs and CSIRTs authorities that participate within the same Sharing group as the Critical Infrastructure that is affected. At the same time, the event is communicated to the ATIO and from there to the affected infrastructure.

Moreover, EME offers enhanced collaboration and communication capabilities that aim to support the EME user for addressing a detected threat effectively and efficiently. Thus, in case that the user would require some assistance from the CERTs/CSIRTs authorities, then

he/she is able to communicate with the cybersecurity authorities using the purple messaging icon that is embedded in every CTI listing.

3.10 EME-CERT UI

The IRIS-EME platform instance that is configured for the CERTs/CSIRTs operator, as mentioned in Section 3.1, incorporates a visualisation environment that is tailored to the CERT/CSIRT operator specific needs, hereinafter EME-CERT UI. The IRIS-EME platform that resides on the CERT/CSIRT establishments collects the events that are dispatched/shared by the IRIS-EME instances that are located on the CI premises and visualises them through the dashboard to the CERT/CSIRT operator.

3.10.1 EME-CERT UI Homepage

Once the events are communicated to the CERTs/CSIRTs deployed IRIS-EME platforms the associated operator can overview the collected threats through the homepage of the dashboard as presented in Figure 21 and Figure 22. The first figure illustrates the upper part of the dashboard, whilst the second figure presents the bottom part of the dashboard.

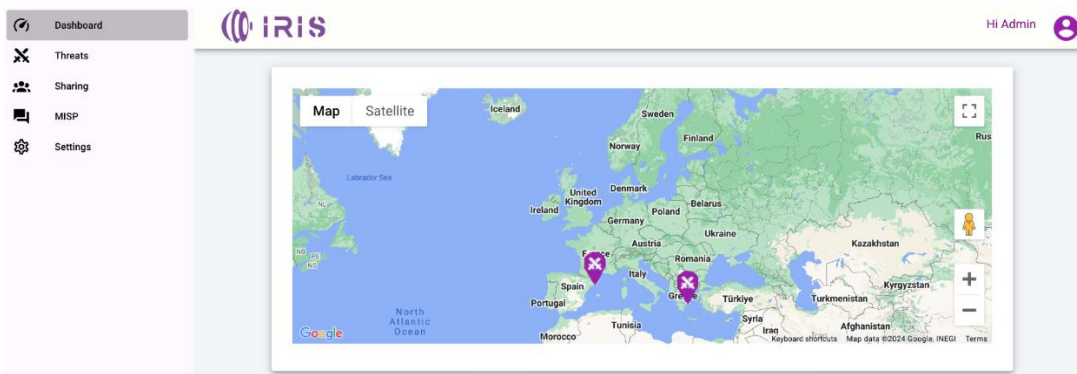


Figure 21: IRIS-EME CERT UI Homepage (upper part)

Figure 21 presents the map on which the CERT/CSIRT can observe the location of the events at Pan-European, national or regional level.

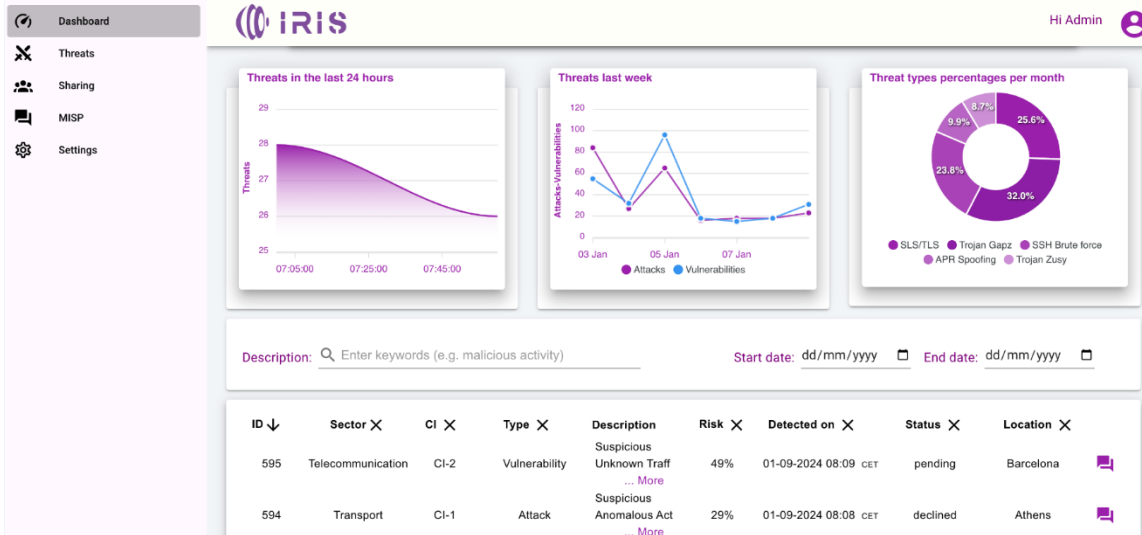


Figure 22: IRIS-EME CERT UI Homepage (bottom part)

Figure 22 presents the bottom part of the screen. Here the user similarly to the IRIS-EME CI UI, is able to review the statistics of the threats that were captured for the last 24 hours or 7 weeks and a classification of the threats based on their type. On the left, the menu item is similar to the one described in Section 3.9.1.

Finally, at the bottom part of the screen, the CERT/CSIRT operator is able to review the collected threats. Each row holds one threat that was communicated by a specific Critical Infrastructure. For each threat the following properties are provided:

- ID of the threat
- The sector that the organisation belongs
- The CI name (corresponds to the organisation name)
- The type of the threat
- The brief description of the threat
- The associated Risk
- The date and time that it was detected
- The status and the associated location that the organisation locates in.

3.10.2 IRIS-EME CERT UI Threats

Figure 23 describes the threat view of the IRIS-EME CERT UI. Here the operator is able to review additional details, similarly to the CI operator UI Threats view (Section 3.9.4.) Here, a small differentiation is that the CI organisation particular details are included in each CTI threat event card.

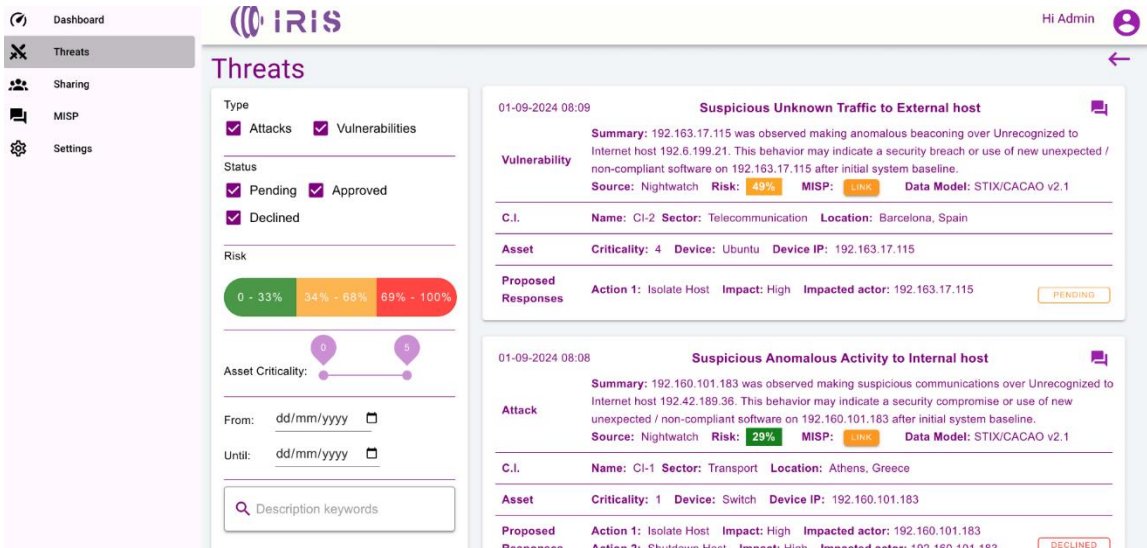


Figure 23: IRIS-EME CERT UI Threats view

One major capability that this view offers to the CERT/CSIRT operator is the fact that the status of each attack is visible also to the CERT/CSIRT side user. The status gets updated in the CERT/CSIRT side once a mitigation action is (or not) performed by the CI operator on his/her end. This way the CERT/CSIRT authority is aware of the exact status of each threat that is detected by the IRIS platform and subsequently is handled by the CI operator.

3.11 Applications integrated in IRIS-EME UI

The IRIS-EME unified dashboard aims to unify all the IRIS components' visual environments into one unified dashboard and present a single entry point to the IRIS Platform functions to its target users. For now, these dashboards are partially integrated in the IRIS-EME UI. The final updates of the IRIS-EME UI will be described in D6.4 that will describe the final version of the integrated IRIS platform.

3.11.1 ATIO - Workflow Manager (OWM) - UI

In IRIS, ATIO is implemented through the *Shuffle* software [1], an open-source solution of a security-oriented automation solution for the CERT/CSIRT community.

It is especially oriented in order security operations centres to share automatically their processes towards detections in a standardized way, while it remains focused to an entirely open ecosystem, that includes open products, open workflows and open standards.

Panel Grid

In Figure 24 the Panel Grid of workflows as part of the Orchestrator Workflow Manager (OWM) UI is shown.

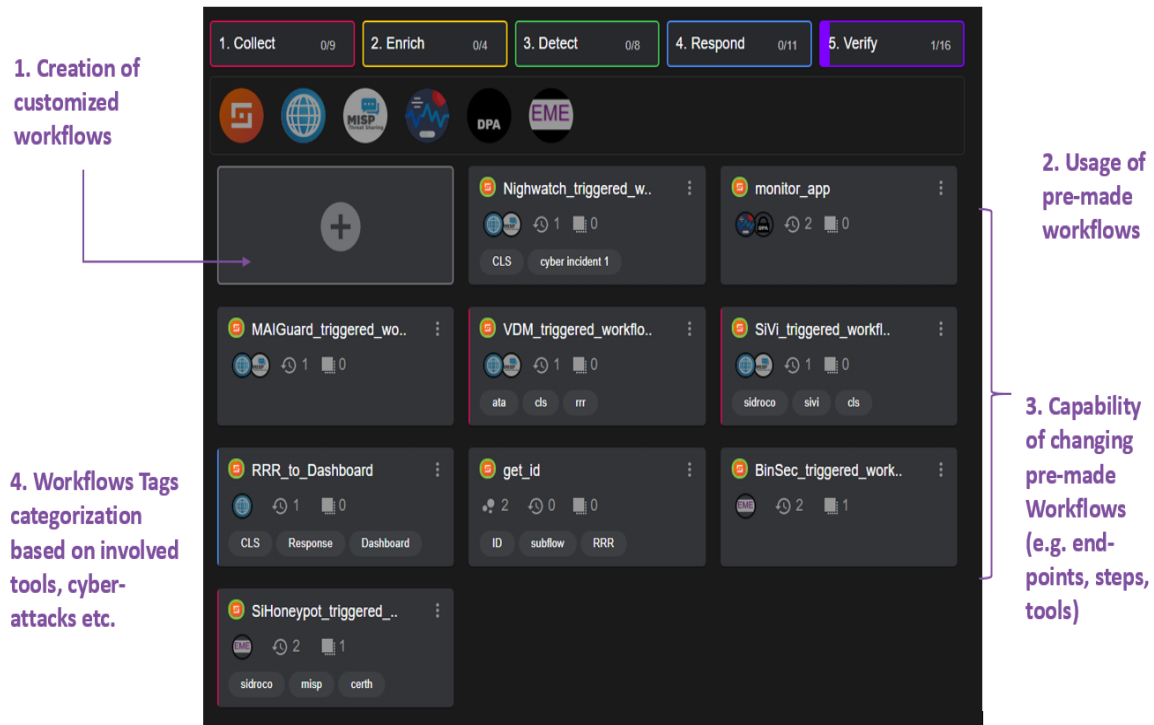


Figure 24: ATIO Orchestrator Workflow Manager (OWM) listing organisations workflows

3.11.2 MISP application - UI

MISP [2] is an open source software with a large community of MISP users creating, maintaining and operating communities of users or organizations sharing information about threats or cyber security indicators worldwide. The IRIS-EME platform incorporates a MISP instance that can be operated by the IRIS user (this is also part of MeliCERTes 2).

The MISP instance is fed with CTI data communicated by the ATIO. The MISP instance IRIS associated data is managed by the IRIS CTI sharing and storage module. More information regarding the operation and functionality provided by the MISP instance can be found within Deliverables D4.1 and D4.2. Figure 25 presents the IRIS-EME instance login page.

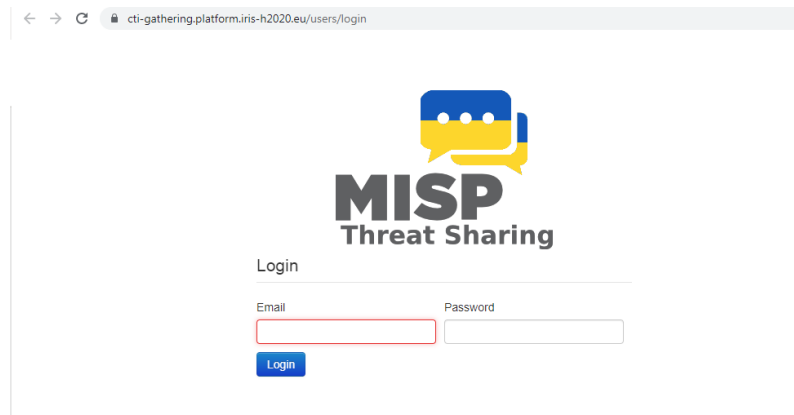
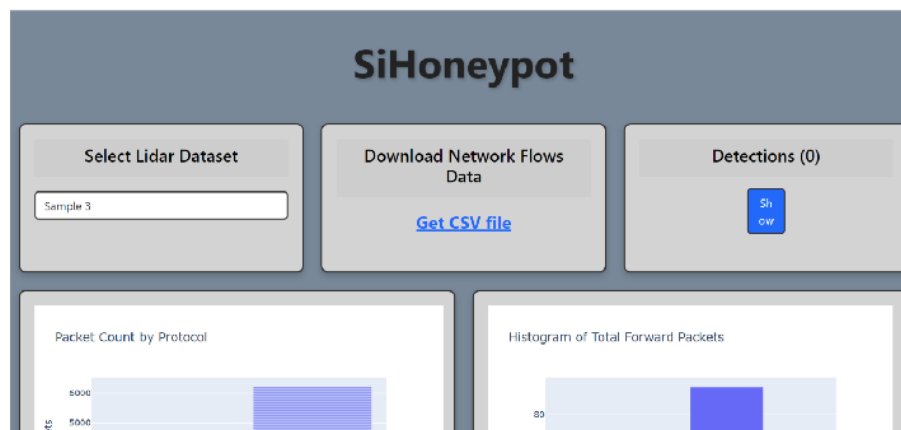


Figure 25: IRIS-EME MISP instance login page

3.11.3 SiHoneypot – UI

SiHoneypots is a specialized tool designed to deploy Honeypots associated with modern embedded devices, sensors, and industrial hardware. This tool effectively "traps" malicious actors, capturing pertinent information related to the deployed attacks. SiHoneypots actively supports the acquisition of threat intelligence and facilitates sharing through established message formats. SiHoneypots are part of the AI threat analytics and detection engine of the IRIS Automated Threat Analytics (ATA) module.





4 IRIS-EME PLATFORM DEPLOYMENT AND VALIDATION

4.1 IRIS-EME platform installation

The Installation procedure of the IRIS-EME platform is driven by HELM¹¹ charts. The associated instructions are available within the project's GitLab page¹². All of the EME developed components are containerized and are Kubernetes compliant. The associated K8s configuration files have been also authored and are available in the IRIS GitLab.

HELM chart is a package that contains all the necessary resources to deploy an application to a Kubernetes cluster. This includes YAML configuration files for deployments, services, secrets and config maps that define the desired state of the application.

In the framework of IRIS project, the installation procedure for the IRIS-EME platform will be greatly simplified. At the time of writing these lines the following components, Figure 26, are being deployed as HELM charts.

Environmental variable	Description
Django Backend	The backend
Django Backend's PostgreSQL	Backend's database
Django Backend's Redis	Backend's caching server
Cerebrate	Cerebrate web
Cerebrate's MariaDB	Cerebrate database
Unified Dashboard	Dashboard for the EME backend (client)
Keycloak	Authentication system

Figure 26: Integrated into HELM charts components of IRIS-EME platform (so far)

In order to deploy the chart in a Kubernetes cluster the following commands, as presented in Figure 27 have to be executed:

¹¹ <https://helm.sh/docs/topics/charts/>

¹² <https://gitlab.iris-h2020.eu/h2020-iris/iris-collaborative-secure-and-trusted-cyber-threat-intelligence-sharing/eme/eme-charts>



```
cd eme
export NAMESPACE="eme-test"
export RELEASE_NAME="eme-test"

helm upgrade --install \
  --namespace ${NAMESPACE} --create-namespace \
  --timeout 20m30s -f values.yaml ${RELEASE_NAME} .
```

If you add new dependency in the `Chart.yaml` run:

```
helm dependency update
```

and then

```
helm dependency build
```

Figure 27: Installation process for the IRIS-EME platform deployment

4.2 IRIS-EME platform deployments

The IRIS-EME platform has been deployed in three (3) isolated namespaces of the IRIS Kubernetes cluster where it has been unit tested for its offered functionalities. The scenario here concerns the deployment of two (2) CI operated EME-platform instances, Figure 29 and Figure 30, and one (1) CERT operated EME-platform instance, Figure 28.

Pods(iris-cert1)[8]										
NAME+	PF	READY	RESTARTS	STATUS	CPU	MEM	%CPU/R	%CPU/L	%MEM/R	%MEM/L IP
iris-cert1-cerebrate-platform-6b876bccc7-hh7t2	●	1/1	0	Running	1	71	n/a	n/a	n/a	n/a 10.244.3.181
iris-cert1-database-0	●	1/1	0	Running	11	104	4	n/a	40	n/a 10.244.6.225
iris-cert1-django-75c9b85c4c-8f4st	●	1/1	0	Running	194	4847	n/a	n/a	n/a	n/a 10.244.3.212
iris-cert1-keycloak-0	●	1/1	0	Running	6	652	n/a	n/a	n/a	n/a 10.244.3.67
iris-cert1-mariadb-0	●	1/1	0	Running	6	107	n/a	n/a	n/a	n/a 10.244.3.160
iris-cert1-postgresql-0	●	1/1	0	Running	16	47	6	n/a	18	n/a 10.244.3.164
iris-cert1-redis-master-0	●	1/1	0	Running	36	36	n/a	n/a	n/a	n/a 10.244.3.105
iris-cert1-unified-dashboard-66558d9fbd-5cf97	●	1/1	0	Running	1	29	n/a	n/a	n/a	n/a 10.244.3.207

Figure 28: CERT-1 deployment

Pods(iris-ci1)[8]										
NAME+	PF	READY	RESTARTS	STATUS	CPU	MEM	%CPU/R	%CPU/L	%MEM/R	%MEM/L IP
iris-ci1-cerebrate-platform-66d9c8489c-k5pm9	●	1/1	0	Running	1	70	n/a	n/a	n/a	n/a 10.244.3.169
iris-ci1-database-0	●	1/1	0	Running	9	96	3	n/a	37	n/a 10.244.3.122
iris-ci1-django-5cc4fd4787-x9g96	●	1/1	0	Running	11	3501	n/a	n/a	n/a	n/a 10.244.3.201
iris-ci1-keycloak-0	●	1/1	0	Running	4	624	n/a	n/a	n/a	n/a 10.244.3.247
iris-ci1-mariadb-0	●	1/1	0	Running	5	105	n/a	n/a	n/a	n/a 10.244.3.161
iris-ci1-postgresql-0	●	1/1	0	Running	11	47	4	n/a	18	n/a 10.244.3.163
iris-ci1-redis-master-0	●	1/1	0	Running	17	32	n/a	n/a	n/a	n/a 10.244.3.119
iris-ci1-unified-dashboard-5fb59c8474-7xkwj	●	1/1	0	Running	1	37	n/a	n/a	n/a	n/a 10.244.5.6

Figure 29: CI-1 deployment

Pods(iris-ci2)[8]										
NAME+	PF	READY	RESTARTS	STATUS	CPU	MEM	%CPU/R	%CPU/L	%MEM/R	%MEM/L IP
iris-ci2-cerebrate-platform-78679fc5f7-pkgh7	●	1/1	0	Running	1	75	n/a	n/a	n/a	n/a 10.244.3.178
iris-ci2-database-0	●	1/1	0	Running	8	95	3	n/a	37	n/a 10.244.3.130
iris-ci2-django-7cb8b68bf9-dzdzc	●	1/1	0	Running	10	3368	n/a	n/a	n/a	n/a 10.244.3.184
iris-ci2-keycloak-0	●	1/1	0	Running	4	675	n/a	n/a	n/a	n/a 10.244.3.248
iris-ci2-mariadb-0	●	1/1	0	Running	5	113	n/a	n/a	n/a	n/a 10.244.3.137
iris-ci2-postgresql-0	●	1/1	0	Running	14	52	5	n/a	20	n/a 10.244.5.254
iris-ci2-redis-master-0	●	1/1	0	Running	11	12	n/a	n/a	n/a	n/a 10.244.4.187
iris-ci2-unified-dashboard-64fc74b457-f12sj	●	1/1	0	Running	1	32	n/a	n/a	n/a	n/a 10.244.3.193

Figure 30: CI-2 deployment



Within each deployment, core modules of the IRIS-EME platform have been deployed.

4.3 Testing

The IRIS-EME platform has been rigorously unit tested on premise in accordance with the integration and testing methodology described within Deliverable D6.2. The Security tests and the integration tests with the rest of the components of the IRIS platform have been conducted in the IRIS cluster and thoroughly documented within Deliverable D6.3 that presents the 1st release of the integrated IRIS platform.

4.4 Future plans

The future development plan for the IRIS-EME platform concerns:

- The integration, into the IRIS-EME unified dashboard, of the visual environments of the CTI sharing and storage component, of the ATIO (shuffle) and the GUI of the SiHoneypots framework.
- To integrate all of the IRIS-EME ecosystem components into a unified master HELM chart that will allow for a holistic installation and configuration of the IRIS-EME platform via a custom script. The process so far, is partially achieved as backend integration of all components and services was prioritized.
- Any optimisations or improvements that may be received as feedback through the demonstration of the IRIS-EME platform in the 1st round of the IRIS pilot associated activities.



5 CONCLUSIONS

The IRIS-EME ecosystem design, implementation, functional and operational characteristics have been thoroughly detailed in this Deliverable. The IRIS-EME ecosystem addresses a large user base, involving not only CERTs/CSIRTs, but also stakeholders providing services, and operating infrastructures that capitalize on IoT and AI driven technologies (such as in smart city relevant services and infrastructures). Through the unified UI experience offered to the IRIS users by the IRIS-EME dashboard, the IRIS-EME platform successfully manages to provide to the extended range of IRIS stakeholders an effective, efficient as well as intuitive user experience that promotes CTI collaboration, sharing and swift response on a timely manner to the need to know only stakeholders.



6 REFERENCES

- [1] SHUFFLE, "Shuffle Automating Security Industry," [Online]. Available: <https://shuffler.io/>.
- [2] MISP Project, [Online]. Available: <https://www.misp-project.org/>. [Accessed 04 05 2022].
- [3] SHUFFLE, "Shuffle Apps," [Online]. Available: <https://shuffler.io/docs/apps>.
- [4] Consortium, IRIS, "D2.2 User and Technical Requirements," 2022.
- [5] Consortium, IRIS, "D2.6 IRIS platform and reference architecture -final version," 2023.
- [6] Consortium, IRIS, "D4.3 APIs for advanced threat intelligence orchestration," 2022.
- [7] OASISS OPEN, "CACAO Security Playbooks Version 2.0," 2023. [Online]. Available: <https://docs.oasis-open.org/cacao/security-playbooks/v2.0/csd01/security-playbooks-v2.0-csd01.html>.
- [8] OASIS Committee Specification 01, "STIX™ Version 2.1," Edited by Bret Jordan, Rich Piazza, and Trey Darley. 20 March 2020, [Online]. Available: <https://docs.oasis-open.org/cti/stix/v2.1/cs01/stix-v2.1-cs01.html>. Latest stage: <https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1..>
- [9] Organization for the Advancement of Structured Information Standards (OASIS), "STIX™ Version 2.1, Committee Specification 0.1," March 2020. [Online]. Available: https://docs.oasis-open.org/cti/stix/v2.1/cs01/stix-v2.1-cs01.html#_1j0vun2r7rgb.
- [10] IRISConsortium, "IRIS D3.1_IRIS risk and vulnerability assessment module," 2023.
- [11] STIX, "<https://oasis-open.github.io/cti-documentation/stix/intro>," [Online].
- [12] MeliCERTes, "The Cyber Security Platform MeliCERTes," [Online]. Available: <https://github.com/melicertes>.
- [13] Keycloak, "<https://www.keycloak.org>," [Online]. Available: <https://www.keycloak.org>.
- [14] IETF OAuth Working Group, "OAuth 2.0," [Online]. Available: <https://oauth.net/2/>.
- [15] OASIS, "SAML Version 2.0 Errata 05," 2012. [Online]. Available: <http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.html>.
- [16] OpenID, "Welcome to OpenID Connect," 2020. [Online]. Available: <https://openid.net/connect/>.