CyberSecDome

An innovative Virtual Reality based intrusion detection, incident investigation and response approach for enhancing the resilience, security, privacy and accountability of complex and heterogeneous digital systems and infrastructures.

D6.4 - Intermediary Report on Contribution to Certification Standardisation

Editor:	Kostas Drakonakis
Beneficiary:	TUC
Version:	1.0
Status:	Final
Delivery date:	25/02/2025
Dissemination level:	PU (Public)

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

Deliverable Factsheet

Grant Agreement No.:	101120779
Project Acronym:	CyberSecDome
Project Title:	An innovative Virtual Reality based intrusion detection, incident investigation and response approach for enhancing the resilience, security, privacy and accountability of complex and heterogeneous digital systems and infrastructures.
Call:	HORIZON-CL3-2022-CS-01 (Cybersecurity)
Start date:	01/09/2023
Duration:	36 months

Deliverable Name:	D6.4 Intermediary Report on Contribution to Certification Standardisation
Related WP:	WP6 Dissemination, Exploitation and Sustainability
Due Date:	28/02/2025

Editor:	Kostas Drakonakis (TUC)
Contributor(s):	ACS, LIU, MAG, SLC, TUM, CBRL, ITML, STS, ARU, AEGIS, IMT, OTE, AIA
Reviewer(s):	Michael Kühr (TUM), Shareeful Islam (ARU)
Approved by:	All partners

Disclaimer

This document reflects the opinion of the authors only. While the information contained herein is believed to be accurate, neither the CyberSecDome consortium as a whole, nor any of its members, their officers, employees or agents make no warranty that this material is capable of use, or that use of the information is free from risk and accept no liability for loss or damage suffered by any person with respect to any inaccuracy or omission.

Executive Summary

This document reports on the CyberSecDome standardisation efforts throughout the first half of the project as per Task 6.3. Specifically, this document outlines the project's standardisation objectives and the adopted strategies to achieve them. Additionally, it documents the status of the activities planned, including the adoption of pertinent standards, liaisons with relevant standardisation bodies, establishment of cross-project synergies and participation in relevant events by the consortium partners. Moreover, the next steps and planned activities for the second half of CyberSecDome are described.

Initially, a comprehensive overview of the current standardisation landscape and relevant bodies, which are related to CyberSecDome, is provided. Then, the project's standardisation objectives and goals are outlined, followed by a high-level overview of the strategy defined by the consortium to achieve them. Moreover, an overview of the standards *already* adopted by the CyberSecDome components is provided, including relevant certifications acquired by consortium partners, highlighting the project's commitment to utilizing and extending existing, well-defined standards, policies and best practices and to producing high-quality, robust and standardisable results.

Subsequently, this deliverable describes all distinct liaisons established with appropriate standardisation bodies along with activities carried out by the consortium. These include cross-project synergies, participation in physical and virtual standardisation-focused events, such as webinars, workshops and conferences, as well as the direct involvement of partners in meetings of relevant standards' technical committees (TCs) and special interest groups (SIGs).

Finally, a brief overview of planned activities to be carried out during the second half of the project is provided, including planned publications, standards-related recommendations and best practices and the organisation of dedicated standardization-oriented workshops.

Document History

Version	Date	Author(s)	Comments
0.1	10/12/2024	Kostas Drakonakis (TUC)	ToC
0.2	25/01/2025	Kostas Drakonakis (TUC)	First draft
0.3	29/01/2025	ALL contributing partners	Input in Sections 3, 4 and 5
0.4	06/02/2025	Kostas Drakonakis (TUC)	Final version for internal review
0.5	07/02/2025	Michael Kühr (TUM), Shareeful Islam (ARU)	Peer review
0.6	14/02/2025	Kostas Drakonakis (TUC)	Integrating review comments
0.7	19/02/2025	Haris Mouratidis (SLC)	Quality check
1.0	25/02/2025	Kostas Drakonakis (TUC)	Final version ready for submission

Table of Contents

List of Figures

List of Tables

Acronyms and Abbreviations

AG	Advisory Group
ECSCI	European Cluster for Securing Critical Infrastructures
HSB	Horizon Standardisation Booster
KPI	Key Performance Indicator
NSB	National Standards Body
SIG	Special Interest Group
SDO	Standards Developing Organization
TC	Technical Committee
TG	Task Group
WG	Working Group

1 Introduction

1.1 Purpose and Scope

This deliverable aims to describe CyberSecDome's standardisation objectives and current efforts towards achieving them. It outlines the current standardisation landscape and the project's strategy for achieving the desired results. Moreover, the document highlights all relevant standards adopted by CyberSecDome components, particularly at the technical level, and also covers pertinent certifications acquired by different partners. Additionally, it describes the liaisons established with distinct standardisation and policymaking bodies, as well as cross-project synergies, and the individual activities that were carried out during the first half of the project's lifetime, paving the way for concrete contributions. Finally, the next steps for the second half of the project are laid out.

1.2 Contribution to other Deliverables

This deliverable serves as the basis for identifying standards adopted by CyberSecDome components, which can further aid in identifying opportunities for standardisation contributions. By outlining the liaisons established with relevant entities, it facilitates the dissemination of pertinent results and the engagement of relevant stakeholders and standardisation bodies. As such, deliverables focusing on different CyberSecDome components can benefit by proposing amendments, extensions and/or modifications of existing standards and, most importantly, communicating the contributions to the appropriate bodies. Moreover, the different standardisation-focused activities described in this document also serve as significant dissemination channels, contributing to related deliverables (D6.2 and D6.3). Lastly, D6.5 *"Final Report on Contribution to Certification Standardisation"* will build upon this deliverable, outlining the steps and contributions towards standardisation for the second half of the project.

1.3 Structure of the Document

This document has the following structure:

- Section 1 briefly describes the purpose and scope of the deliverable.
- Section 2 outlines the current standardisation landscape, including relevant bodies, and describes CyberSecDome's standardisation objectives and strategy.
- Section 3 compiles and presents all standards currently adopted by the CyberSecDome platform and components, as well as pertinent certifications acquired by consortium partners.
- Section 4 describes the established bonds and liaisons with relevant standardisation bodies and the individual events and activities carried out so far.
- Section 5 delineates planned activities and next steps for the second half of the project.

2 Standardisation Strategy

2.1 Standardisation Landscape

The cybersecurity standardisation landscape comprises several distinct entities, such as National Standards Bodies (NSBs), non-governmental organizations (e.g., ISO), dedicated working groups (WGs) and special interest groups (SIGs), as well as policy making bodies (e.g., ENISA). It is therefore imperative to identify such bodies that are pertinent to CyberSecDome's objectives, so as to promptly and effectively identify potential pathways and opportunities for achieving the project's standardisation goals, as detailed in 2.2. In the following we outline the most prominent international and European such standardisation bodies.

The **European Committee for Standardization (CEN)** and the **European Committee for Electrotechnical Standardization (CENELEC)** are the two major European organizations that develop and publish standards to enhance safety, interoperability, and innovation within Europe. Prominent standards and guidelines include EN 17640 on fixed-time cybersecurity evaluation methodology for ICT products and EN 18031-1, TS 50701 covering security requirements and recommendations on various sectors (e.g., radio equipment and railways).

The **European Telecommunications Standards Institute (ETSI)** is an independent, non-profit organization responsible for developing global standards and defining requirements and recommendations in telecommunications, information technology, and electronic communications, with a focus on cybersecurity through its CYBER TC. Relevant standards include TR 103 305-1 on critical security controls, TR 104 003 on vulnerability disclosure, TR 103 937 on cyber resiliency and supply chain management and EN 303 645 on security recommendations for consumer IoT products.

The **European Union Agency for Cybersecurity (ENISA)** is the agency dedicated to achieving a high, common level of cybersecurity across Europe. This is achieved through concrete advisories to the European Commission and EU member states on cybersecurity issues, aiding in the development of EU-wide policies, strategies and regulations. Crucially, ENISA publishes reports, guidelines and recommendations on various cybersecurity topics, such as risk management, data protection and incident response (e.g., [1], [2], [3]), as well as adhering to emerging regulations such as the NIS 2 directive [4].

The **Organization for the Advancement of Structured Information Standards (OASIS)** is a nonprofit, global consortium that aims at developing open and transparent standards on multiple fronts, such as artificial intelligence, emergency management and cybersecurity. Several standards and the associated TCs focus on different security matters, with a special focus on threat information sharing through the Threat Actor Context and Cyber Threat Intelligence TCs (Structured Threat Information Expression, Trusted Automated Exchange of Intelligence Information). Moreover, the Collaborative Automated Course of Action Operations (CACAO) TC works towards the implementation of a unified standard for implementing course of action playbooks for cybersecurity operations.

The **Forum of Incident Response and Security Teams (FIRST.org)** is a global nonprofit organization that brings together incident response and security teams to foster collaboration and improve cybersecurity worldwide. Among its various activities, FIRST develops frameworks, guidelines and best practices, such as the Common Vulnerability Scoring Systems (CVSS) and the Exploit Prediction Scoring System (EPSS) for vulnerability scoring, triaging and prioritization, as well as the Traffic Light Protocol (TLP) for information sharing.

The **International Organization for Standardization (ISO)** is an independent, non-governmental international organization that develops and publishes global standards across a wide range of industries and sectors, including a plethora of standards pertinent to cybersecurity and incident management. Similarly, the **International Electrotechnical Commission (IEC)** also develops standards for electronic and related technologies and often cooperates with ISO on standard development over common areas of interest. Such standards include the well-known ISO/IEC 27001, 27002, 27005, 27017, 27018, 27023 and 27035, establishing requirements and providing guidelines for a wide range of cybersecurity aspects, such as implementing and maintaining an information security management system (ISMS), information security controls and risk management in general contexts and in cloud services, as well as incident management.

The **National Institute of Standards and Technology (NIST)** is an agency that promotes innovation and industrial competitiveness by developing and advancing standards and best practices in various sectors. While NIST is a US based standardisation institute, it is internationally recognized for its contributions to cybersecurity through well known, exemplary publications, such as the NIST Cybersecurity Framework (CSF) [5] and the NIST SP 800 Series, which offer detailed guidelines on information security controls (SP 800-53 [6]) and incident management (NIST SP 800-61 [7]).

The **Internet Engineering Task Force (IETF)** is an open, global community of network designers, engineers, researchers, and other professionals dedicated to developing and promoting technical standards for the internet, through a multitude of affiliated WGs on different security aspects. These include key transparency, lightweight authenticated key exchange, Web authorization protocols, transport layer security (TLS) and more.

2.2 CyberSecDome Approach towards Standardisation

The CyberSecDome project has a clear commitment to disseminating its results, innovations and key insights to relevant bodies and organisations, with the goal of contributing to the overall standardisation landscape, particularly in regard to digital infrastructure resilience, as well as incident management and response.

Specifically, CyberSecDome has identified and established the following standardisation objectives:

1. Establish liaisons with relevant bodies, as well as cross-project standardisation-focused synergies via presentations and workshops, participation in technical committees' (TCs) and working groups' (WGs) meetings, and proposal of recommendations and best practices.
2. Regularly interact with standardisation and policy-making bodies (e.g., ENISA, OASIS TCs, FIRST) in relevant fields, such as incident management and response.
3. Identify, monitor and, where applicable, adopt and adhere to existing standards, in an effort to pinpoint gaps and potential areas for improvement.
4. Raise awareness and promote the project's results, key innovations and insights, as well as collect feedback for fine tuning project outcomes.

From the early stage of the project, the partners in T6.3 solicited the consortium's input for identifying existing bonds and activities with relevant standardisation bodies and entities, to foster potential opportunities for further liaisons and interactions. These liaisons constitute the cornerstone for achieving the entirety of the aforementioned objectives, since they serve as channels that enable direct engagements and interactions for disseminating project results and proposing recommendations and best practices extracted from CyberSecDome's advancements. Moreover, the individual standardisation-related activities carried out by consortium partners through the first half of the project were monitored and tracked through live spreadsheet files in the project's repository. These activities served both educational and informative purposes on standardisation matters (e.g., attending pertinent workshops and conferences), as well as results' dissemination via actively participating through presentations.

Another major avenue for increasing the project's impact and engaging in further meaningful interactions is the formation of and participation in cross-project synergies. For the first half of the project, this was achieved by joining the European Cluster for Securing Critical Infrastructures (ECSCI), comprising 47 European projects, which promotes such synergies and collaborations and offers a multitude of related events for dissemination. Another major advancement was CyberSecDome's initiative to form a cross-project cluster with similar-topic projects (SYNAPSE, PHOENI2X) and jointly apply for the Horizon Standardisation Booster (HSB) services, which include a series of consultation sessions with an appropriate standardisation expert and the organisation of a joint standardisation-focused workshop.

Additionally, consortium input was gathered through shared files for collecting both relevant and *already adopted standards* by CyberSecDome components, as well as specific certifications acquired by partners. Apart from highlighting the project's commitment to achieving high-quality, interoperable and sustainable results, this was a crucial step in identifying potential opportunities for improvement and contributions through the continuous monitoring and surveying of these standards.

Overall, these activities aim to achieve the standardisation objectives set by the consortium as part of T6.3. Additionally, establishing such steady bonds with standardisation bodies and cross-project collaborations allows for the achievement of the pertinent key performance indicator (KPI), which dictates that the CyberSecDome project should make at least three recommendations and/or propose best practices on the topic of incident investigation and response. Specifically, as the technical work in the project continues to progress, this is planned to be achieved by authoring and disseminating whitepapers and/or policy briefs on various CyberSecDome innovations and approaches, as well as extracting best practices and key insights from the project's advancements.

3 Adopted Standards

CyberSecDome strives to achieve sustainable, high-quality and exploitable results. Crucially, the technical specifications and user requirements defined in D2.2 "*Architecture and Technical Specifications of CyberSecDome*" clearly dictate that the CyberSecDome platform should have the following key properties, among others:

1. ***Scalability***. Design the CyberSecDome system to be scalable, supporting the integration of additional tools and the expansion to cover more digital infrastructures.
2. ***Interoperability.*** Achieve interoperability among the CyberSecDome tools and with existing digital infrastructure systems, ensuring seamless data exchange and collaboration.
3. ***Compliance.*** Ensure all CyberSecDome tools and processes comply with relevant cybersecurity standards, regulations (e.g., GDPR), and ethical guidelines.

One prominent approach to aid in the realization of these properties is the identification and adoption of relevant standards, policies and sets of best practices in different components, modules or even entire pipelines of the system. Specifically, exploiting well-established, existing standards, guidelines, and best practices fosters interoperability, extensibility, compliance with relevant guidelines and quality assurance.

During the first half of the project, when the main technical progress and advancements of CyberSecDome were carried out, the technical partners particularly focused on and pursued the identification and exploitation of relevant standards, where applicable, to achieve the aforementioned goals. In the following table, all pertinent standards and best practices adopted by CyberSecDome are outlined, along with a description highlighting the use, goal and importance of the standard/guidelines, the associated tasks and components they are used in, as well as the specific partners adopting them.

Table 1: Standards, best practices and guidelines adopted by CyberSecDome.

Standard / Best practices	Description	Partner	Associated components	Associated tasks
NIST SP 800-92 Guide to Computer Security Log Management [8]	This publication seeks to assist organizations in understanding the need for sound computer security log management by providing practical, real-world guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise	ACS	Incident Investigation	T3.3, T4.5
NIST SP 800-61 R2 Computer Security Incident Handling Guide	This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively by providing guidelines for incident handling, particularly for analysing incident-related data and determining the appropriate response to each incident.	ACS	Incident Investigation	T3.3, T4.5
FIRST.ORG Common	CVSS provides a way to capture the principal characteristics of a vulnerability and produce a	LiU	Automated pen-testing	T3.4

Standard / Best practices	Description	Partner	Associated components	Associated tasks
Vulnerability Scoring System (CVSS)	numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.			
MITRE[14] Common Vulnerabilities and Exposures (CVE)	The mission of the CVE Program is to identify, define, and catalogue publicly disclosed cybersecurity vulnerabilities, so as to foster coordination and prioritization for vulnerability handling.	LiU, MAG, SLC	Automated Pen-Testing, Dynamic Risk Assessment	T3.4
MITRE Common Platform Enumeration (CPE)	CPE is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets.	MAG, SLC	Dynamic Risk Assessment	T3.4
MITRE Common Weakness Enumeration (CWE)	CWE is a community-developed list of common software and hardware weaknesses that could contribute to the introduction of vulnerabilities.	LiU	Automated Pen-Testing	T3.4
MITRE ATT&CK	MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.	LiU	Automated Pen-Testing	T3.4
FIRST.ORG Exploit Prediction Scoring System (EPSS)	EPSS is a data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild.	MAG, SLC	Dynamic Risk Assessment	T3.4
ISO 28000	ISO 28000 focuses on aspects critical to manage and assure security risks by providing a best practice framework to reduce them.	MAG, SLC	Dynamic Risk Assessment	T3.4
NIST FIPS PUB 180-4: Secure Hash Standard (SHS) [9]	This standard specifies hash algorithms that can be used to generate digests of messages. The digests are used to detect whether messages have been changed since the digests were generated.	TUM	Dynamic and Adaptive Incident Response	T3.5

Standard / Best practices	Description	Partner	Associated components	Associated tasks
OASIS Structured Threat Information Expression (STIX) V2.1	STIX is a language and serialization format used to exchange cyber threat intelligence (CTI) with clear object representations and descriptive relationships.	CBRL	Threat Intelligence Sharing	T4.3
OASIS Trusted Automated Exchange of Intelligence Information (TAXII) V2.1	TAXII is an application layer protocol for the secure communication of cyber threat information in a simple and scalable manner, over HTTPS and by defining a restful API.	CBRL	Threat Intelligence Sharing	T4.3
FIRST.ORG Traffic Light Protocol (TLP)	TLP was created to facilitate greater sharing of potentially sensitive information and more effective collaboration, through a set of predefined labels to indicate the sharing boundaries of information.	CBRL	Threat Intelligence Sharing	T4.3
IEEE P3652.1 - Guide for Architectural Framework and Application of Federated Machine Learning [10]	Focuses on federated learning (FL) architecture and best practices for secure, privacy-preserving FL. A blueprint for data usage and model building across organizations and devices while meeting applicable privacy, security and regulatory requirements is provided in this guide.	ITML	AI Knowledge Sharing (following specific guidelines)	T3.1, T4.4
Open Neural Network Exchange (ONNX)	ONNX is an open format built to represent machine learning models. ONNX defines a common set of operators - the building blocks of machine learning and deep learning models - and a common file format to enable AI developers to use models with a variety of frameworks, tools, runtimes, and compilers, fostering interoperability.	ITML	AI Knowledge Sharing, Intrusion Detection and Protection	T3.1, T3.2, T4.4
OpenAPI Specification	A standard for creating and documenting APIs, enabling seamless integration of services.	ITML	AI Knowledge Sharing	T3.1, T4.4

Standard / Best practices	Description	Partner	Associated components	Associated tasks
IETF PCAP Capture File Format	A structured file format used by tcpdump, and other programs using libpcap, to read and write network traces.	TUC	Intrusion Detection and Protection	T3.2
Center for Internet Security (CIS) Benchmarks Level 1	The CIS Level 1 benchmark provides basic, foundational security controls that are relatively straightforward to implement without causing significant disruptions to business operations. It's primarily intended for environments where the primary goal is to establish a basic level of security with minimal complexity.	OTE	Pilot lab	T5.1, T5.2
OpenXR	OpenXR is a royalty-free, open standard that provides a common set of APIs for developing XR applications that run across a wide range of AR and VR devices. This reduces the time and cost required for developers to adapt solutions to individual XR platforms while also creating a larger market of easily supported applications for device manufacturers that adopt OpenXR	IMT	VR interface	T4.1

To provide a more holistic view, we also visually demonstrate the adopted standards over the CyberSecDome architecture, as defined in D2.2, in Figure 1. Overall, the use of predefined standardised metrics, tools, specifications, as well as following best practices and guidelines, span all core components of the CyberSecDome platform, further improving system-wide extensibility, interoperability and compliance with industry-level requirements.

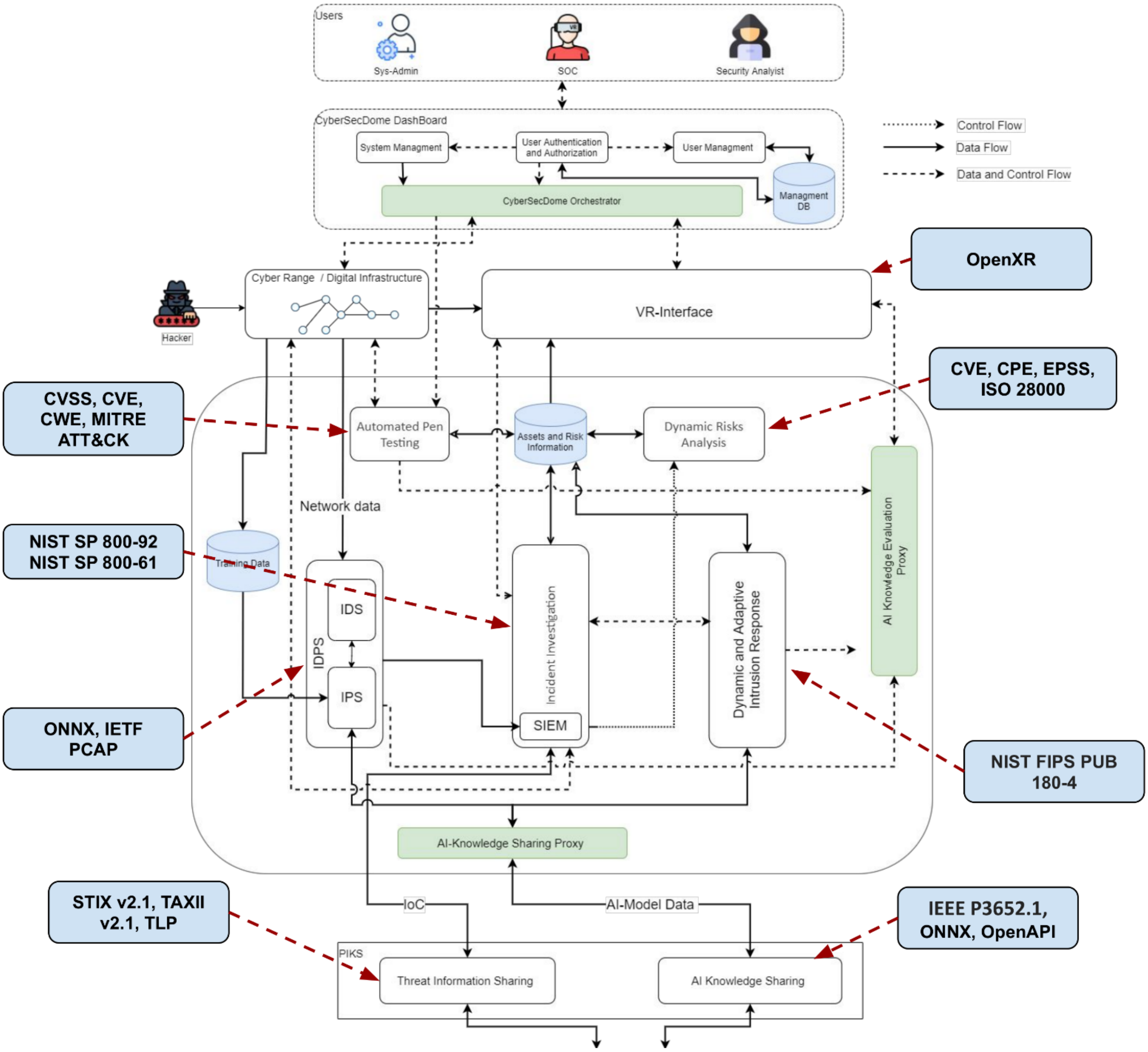

Figure 1: Adopted standards in CyberSecDome.

3.1 Acquired Certifications

Apart from the direct use of standards in various components and tasks, the technical partners have also acquired highly recognized and demanding certifications related to information technology, security, privacy and quality management, ensuring adherence and compliance to industry-level requirements and showcasing commitment to high-quality products and services. We outline the CyberSecDome partners' certifications in the following table.

Table 2: Partners' certifications

Certification	Description	Certified partners
ISO/IEC 27001:2013	Defines requirements an information security management system (ISMS) must meet, providing companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.	MAG, OTE, ITML
ISO/IEC 27701:2019	Defines requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization,	OTE
ISO/IEC 20000-1:2018	Specifies requirements for an organization to establish, implement, maintain and continually improve an information technology service management system (ITSM), including the planning, design, transition, delivery and improvement of services to meet the service requirements and deliver value.	AIA
ISO 9001:2015	Specifies requirements for quality management in organisations, on how to establish, implement, maintain, and continually improve a quality management system (QMS). It aims to assist organisations in promoting products and services that meet customer and applicable statutory and regulatory requirements. It helps businesses to improve their performance and demonstrate their commitment to quality.	AIA

4 Liaison and Standardisation Activities

As mentioned in Section 2.2, CyberSecDome aspires to propose best practices and key insights extracted during its development and disseminate them to relevant standardisation and policymaking bodies as concrete recommendations. To achieve this, we plan to leverage the liaisons established with different bodies, TCs and SIGs, as well as CyberSecDome partners' involvement in their activities, such as workshops and meetings. Specifically, direct involvement with such entities opens up prominent standardisation pathways and provides significant opportunities for shaping existing or future standards. We outline all established liaisons in Table 3.

Table 3: CyberSecDome standardisation liaisons

Relevant body	Standard / Committee	Description	Partner	Role / Activity
OASIS	Cyber Threat Intelligence (CTI) TC	The TC aims to support and standardise automated information sharing for cybersecurity situational awareness, real-time network defense, and sophisticated threat analysis.	TUC	TUC personnel is a TC member
OASIS	Threat Actor Context (TAC) TC	The TC aims to enabling semantic interoperability of threat actor contextual information via a common knowledge framework and standardised vocabularies.	TUC	TUC personnel is a TC member
OASIS	Collaborative Automated Course of Action Operations (CACAO) TC	The TC aims to define the standard for implementing course of action playbooks for cybersecurity operations.	TUC	TUC personnel is a TC member
FIRST.ORG	Traffic Light Protocol (TLP)	TLP was created to facilitate greater sharing of potentially sensitive information and more effective collaboration, through a set of predefined labels to indicate the sharing boundaries of information.	TUC	TUC personnel is a contributor
FIRST.ORG	Automation SIG	Aims to provide a forum where members active in the field of Incidence Response (IR) automation can exchange best practices, document knowledge and compile a list of IR automation tools, among others.	TUC	TUC personnel is participating

Relevant body	Standard / Committee	Description	Partner	Role / Activity
FIRST.ORG	Common Vulnerability Scoring System (CVSS)	CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.	TUC	TUC personnel is closely monitoring the developments of this standard
FIRST.ORG	Exploit Prediction Scoring System (EPSS)	EPSS is a data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild.	TUC	TUC personnel is closely monitoring the developments of this standard
RISC-V Foundation	Shadow Stack and Landing Pads TG	Contributing to the official specification document for enabling architectural support for Control Flow Integrity in RISC-V architecture.	TUC	TUC personnel is the chair of the TG
ENISA	-	The European Union Agency for Cybersecurity, ENISA, contributes to EU cyber policy and enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, among others.	TUC	Prof. Ioannidis was part of ENISA AG and TUC personnel occasionally participate to a number of ENISA WGs (latest one Enhancing SOCs)
OWASP	-	The Open Worldwide Application Security Project is an online community that produces freely available articles, methodologies, documentation, tools, and technologies in the fields of IoT, system software and web application security.	ARU	ARU is leading the Cambridge chapter of OWASP
ISC2	-	The International Information System Security Certification Consortium, or ISC2, is a non-profit organization which	ARU	ARU is leading and coordinating cyber security emerging

Relevant body	Standard / Committee	Description	Partner	Role / Activity
		specializes in training and certifications for cybersecurity professionals.		knowledge area defined by ISC2

It is important to note that several of these liaisons are directly coupled with the standards already adopted by CyberSecDome. For instance, TUC is participating in OASIS' *Cyber Threat Intelligence* (CTI) TC, which produced the STIX and TAXII standards, and also contributed to FIRST's *Traffic Light Protocol* (TLP) standard, all leveraged by CBRL in Task 4.3. TUC is also a member of OASIS' *Threat Actor Context* (TAC) and *Collaborative Automated Course of Action Operations* (CACAO) TCs, as well as FIRST's newly established *Automation* SIG, which are tightly connected with CyberSecDome's threat intelligence and incident response (DAIR) components, respectively. As such, these liaisons present excellent opportunities to both closely monitor the developments of these standards, as well as to identify gaps and lacks of standards from their direct usage in CyberSecDome. In particular, these liaisons constitute direct channels for disseminating project results, recommendations and best practices, further contributing in the shaping of related standards and, overall, maximising the project's impact. Crucially, CACAO is currently undergoing revisions and reformations towards its newer version (v2.1), where TUC is actively participating through multiple TC meetings, which we outline in the next subsection. Similarly, FIRST's *Automation* SIG aims at documenting and disseminating common best practices for automation in the context of incidence response, closely aligning with CyberSecDome's standardisation objectives, and therefore constitutes a great candidate for further project contributions.

4.1 Synergies

Another avenue for boosting the project's standardisation impact is by forming synergies with other related projects and initiatives. Such cross-project synergies can foster joint standardisation efforts, such as compiling best practices and recommendations and organizing workshops. We outline the current CyberSecDome synergies in the following table.

Table 4: Cross-project synergies and liaisons.

Project / Cluster	Description	Involved partners
SYNAPSE	The SYNAPSE project aims to protect Essential and Important Entities, considered in the NIS2 Directive, from the increasing cyber threats. To this end, SYNAPSE relies on three pillars, Situational Awareness, Incident Response, and Preparedness Capabilities. Several CyberSecDome partners are participating in SYNAPSE and MAG is leading the standardisation efforts of the project.	MAG, CBRL, STS, AEGIS
PHOEN2IX	A Cyber Resilience Framework providing Artificial Intelligence (AI) – assisted orchestration, automation & response capabilities for business continuity and recovery, incident response, and information exchange, tailored to the needs of Operators of Essential Services (OES) and of the EU Member State (MS) National Authorities entrusted with cybersecurity.	AEGIS

Project / Cluster	Description	Involved partners
EU-CIP	Establish a novel pan European knowledge network for Resilient Infrastructures, which will enable policy makers to shape and produce data-driven evidence-based policies, while boosting the innovation capacity of Critical Infrastructures (CI) operators, authorities, and innovators (including SMEs).	AIA
ECSCI	The main objective of the ECSCI cluster is to create synergies and foster emerging disruptive solutions to security issues via cross-projects collaboration and innovation, including the promotion of and contribution to relevant standardisation efforts.	ALL

In more detail, CyberSecDome joined the European Cluster for Securing Critical Infrastructures (ECSCI), a cluster aiming to establish and promote cross-project synergies, collaboration and innovation on various fronts, including dissemination and standardisation efforts. Importantly, ECSCI (recently, in cooperation with the EU-CIP project) often organizes various events that are entirely focused on current standardisation matters, or incorporate relevant key insights and presentations. Crucially, CyberSecDome has officially expressed interest and is planned to participate in such upcoming events, in order to disseminate project results and its standardisation efforts.

Moreover, CyberSecDome has taken the initiative to form a cross-project collaboration cluster with the same-call SYNAPSE project (HORIZON-CL3-2022-CS-01-01, GA 101120853) and the PHOENI2X project (HORIZON-CL3-2021-CS-01-01, GA 101070586), which also incorporate incident investigation and response capabilities and innovations. Specifically, CyberSecDome assembled and coordinated the cluster projects so as to jointly apply for and leverage pertinent services provided by the Horizon standardisation Booster (HSBooster), a platform dedicated to supporting Horizon Europe projects in enhancing and valorising project results through standardisation. In more detail, the cluster prepared a unified application for a dedicated workshop on the current standardisation landscape specifically on the common topic of incident investigation and response, organized by HSBooster and led by an appropriate standardisation expert allocated for our cluster. At the time of writing, CyberSecDome and the other participating projects have engaged in fruitful consultancy meetings with the allocated standardisation expert, so as to identify and align project needs, objectives and expectations in a collaborative effort to effectively co-organise the final standardisation-focused workshop and ensure a successful and insightful event for all participants.

4.2 Individual Activities

By leveraging the liaison ties and cross-project synergies described previously, the CyberSecDome partners have participated in several different individual standardisation activities, disseminating project results where possible, as well as monitoring the developments of related standards (e.g., OASIS CACAO, FIRST’s Automation SIG) and policies and identifying further opportunities to enhance the project’s standardisation efforts and impact. Individual standardisation activities are monitored through regularly updated boilerplate files in the project’s repository.

Table 5: Standardisation activities

Hosting organization	Activity description	Date	Partner
Saviynt, iC Consult	Attending webinar "Unlocking NIS2 Compliance – How Identity Security Ensures Regulatory Readiness".	27/02/2024	TUC
CEN, CENELEC, ETSI, ENISA	Attending ENISA-ESOs 8th Cybersecurity Standardisation Conference.	05/03/2024	TUC
ARU, ISC2	Hosted webinar "CISSP certification process and examination". The event was delivered by CISSP academic partnership lead and hosted at ARU to discuss CISSP examination process and certification.	12/03/2024	ARU
OASIS	Participation in CACAO TC Working Call meetings, closely monitoring the standard's developments.	21/11/2023, 05/12/2023, 16/01/2024, 26/03/2024, 09/04/2024, 28/05/2024, 16/07/2024, 30/07/2024, 17/09/2024	TUC
FIRST.org	Attending the 36th Annual FIRST Conference (Japan).	09/06/2024 - 14/06/2024	TUC
FIRST.org	Participation in Automation SIG meetings.	05/09/2024, 11/06/2024	TUC
EU-CIP / ECSCI	Attending 1st EU-CIP Knowledge Hub and Innovation Management Services Webinar.	21/05/2024	TUC
EU-CIP / ECSCI	1st Annual Conference on Critical Infrastructure Resilience: "Reinventing Resilience" – co-organised with the ECSCI cluster.	20/9/2023 - 21/9/2023	AIA
Home Office Emerging Technology Threats	Risks and Opportunities of Technology-Harm Convergence organised by Home Office's Science & Technology unit (within Homeland Security Group).	03/10/2024	ARU

Hosting organization	Activity description	Date	Partner
EU-CIP / ECSCI	Attending webinar "Fortifying the Future: How EU R&D Projects can Shape Standards and Policies in Critical Infrastructure Protection".	10/12/2024	TUC
FIRST.org	Presentation in 2025 TF-CSIRT Meeting & FIRST Regional Symposium Europe on the topic of "Joint Incident Response in the Face of Cross-Country Threat Actors".	14/01/2025	TUC

5 Planned Activities and Next Steps

Here we outline the activities currently planned for the second half of CyberSecDome, building upon the work carried out and the liaisons and synergies established during the first half of the project, as described in this deliverable.

Table 6: Planned activities.

Hosting organization	Activity description	Date	Partner
HSBooster, CyberSecDome, SYNAPSE, PHOENI2X	A cross-project workshop, co-organised by CyberSecDome, providing key insights on projects' objectives and approaches towards standardisation, as well as covering standardisation-related topics on the field of incident investigation and response by a dedicated standardisation expert allocated by HSBooster.	20/03/2025	ALL
Design, Automation and Test in Europe (DATE) Conference	Peer-reviewed paper presentation [11]	03/2025	TUM
ECSCI	Presenting CyberSecDome in the 3rd ECSCI (European Cluster for Securing Critical Infrastructures) Workshop on Critical Infrastructure Protection and Resilience.	04/2025	MAG

Additionally, CyberSecDome will continuously and actively participate in OASIS' *CACAO* TC and FIRST's *Automation* SIG meetings, described in 4.2, monitoring the developments of the relevant standards, policies and best practices, while also disseminating project results where applicable. Moreover, CyberSecDome partners are continuously monitoring relevant events held by associated organisations (e.g., ECSCI, FIRST, ESOs), so as to attend, participate and disseminate project outcomes whenever possible.

Moreover, the consortium is planning to author, publish and disseminate a series of conference papers [11], whitepapers and policy briefs on different CyberSecDome components (e.g., dynamic and adaptive incident response) or combinations of components (e.g., intrusion detection and prediction), outlining key insights, challenges, best practices and standardisable-related outcomes, serving as concrete recommendations that could aid in the shaping of existing and future standards. This is planned as a continuous effort starting from M18 till the end of the project.

Finally, CyberSecDome has officially expressed interest in participating in an open access book on various topics on AI for critical infrastructure protection and resilience, as well as cybersecurity, organised by the ECSCI cluster and involving several other EU projects. Specifically, CyberSecDome will contribute by authoring a dedicated chapter on the innovations, security services, best practices and recommendations it provides. According to ECSCI's guidelines, the open access book is planned for publication for the 2nd quarter of 2025.

References

[1] ENISA (2024). Best Practices for Cyber Crisis Management.

[2] ENISA (2023). Good Practices for Supply Chain Cybersecurity.

[3] ENISA (2009). Good Practice Guide on Information Sharing.

[4] ENISA (2024). IMPLEMENTING GUIDANCE NIS2.

[5] NIST (2024). The NIST Cybersecurity Framework (CSF) 2.0.

[6] NIST (2020). Security and Privacy Controls for Information Systems and Organizations.

[7] NIST (2012). Computer Security Incident Handling Guide.

[8] NIST (2006). Guide to Computer Security Log Management.

[9] NIST (2015). Secure Hash Standard (SHS).

[10] IEEE (2021). 3652.1-2020. Guide for Architectural Framework and Application of Federated Machine Learning.

[11] M. Hamad, M. Kuehr, H. Mouratidis, E.M. Kalogeraki, C. Gizelis, D. Papanikas, A. Bountioukos-Spinaris, C. Skandylas, E. Raptis, A. Alexopoulos, G. Chrysos, M. Marmpena, S. Politi, K. Lieros, N. Papagiannopoulos, I. Xanthopoulos, S. Papastergiou, S. Ioannidis, M. Asplund, M. Pahl and S. Steinhorst, "CyberSecDome – Framework for Secure, Collaborative, and Privacy-aware Incident Handling for Digital Infrastructures", *Proceedings of the Design, Automation and Test in Europe (DATE) Conference*, March 2025.