

AENAON Open Call #1

Technical Annex

August 2026



Co-funded by
the European Union



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



AENAON



Prepared by
AENAON Consortium.

Reviewed by
AENAON Consortium.

Version control
V1.0 (Released 07 August 2026)

About

AENAON develops a Federated Digital Twin-based Cyber Range platform to improve cybersecurity preparedness and resilience of offshore wind farms across Europe. Funded by the Digital Europe Programme through the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC),

aenaon-project.eu

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

Grant Agreement No. 101249723.

Table of contents

- 1. AENAON Service Stack Overview 5**
 - 1.1 Purpose of this Technical Annex.....5
 - 1.2 AENAON Service & Tool Stack.....5
 - 1.3 Structure and Use of the Tool Profiles 6
- 2. Tool Profiles 7**
 - 2.1 Digital Twin Solution 7
 - 2.2 Penetration Testing Solution 8
 - 2.3 xBOMGuard 9
 - 2.4 Cyber Range Solution..... 10
 - 2.5 Risk Assessment Platform 11
 - 2.6 Cyber Threat Intelligence Platform 12
 - 2.7 Threat Hunting & Monitoring 13
 - 2.8 Threat Detection & Incident Response Platform..... 14
 - 2.9 Strategic Cyber Threat Intelligence Platform (SCTIP) 15



1. AENAON Service Stack Overview

1.1 Purpose of this Technical Annex

This Technical Annex provides prospective applicants with a concise overview of the cybersecurity services and tools made available through the AENAON Open Call. Its purpose is to help applicants understand the role and main capabilities of each tool, the types of activities it may support, the expected inputs and outputs, and the principal technical conditions associated with its use.

The annex is intended to support the preparation of realistic and technically credible proposals. Applicants should use the information provided to identify the tools that are relevant to their proposed use case, describe how these tools will contribute to the planned activities, and estimate the integration, configuration, data-preparation and validation effort required. The annex does not constitute detailed product documentation or a complete interface specification. More detailed technical information and onboarding guidance will be provided to selected applicants where required.

1.2 AENAON Service & Tool Stack

AENAON brings together a portfolio of complementary cybersecurity preparedness services supporting offshore wind farms and related digital infrastructures. As illustrated in Figure 1, the service stack is organised into five main service families:

- Digital Twins & Virtualisation Services;
- Vulnerability Discovery & Penetration Testing Services;
- Security Awareness & Cyber Range Services;
- Threat & Risk Assessment Services; and
- Risk/Threat Monitoring & Cyberattack Management Services.

Each service family is supported by one or more specialised tools. These tools address different aspects of cybersecurity preparedness, including infrastructure simulation, vulnerability identification, digital supply-chain visibility, scenario-based training, threat intelligence, cyber risk assessment, threat hunting, monitoring and incident-oriented analysis.

Applicants are not expected to use the complete AENAON tool stack. A proposal may focus on a single tool or combine several tools where this is justified by the proposed use case and implementation approach. The selected tools may be used to support integration, customisation, testing, validation, scenario execution, evidence generation or the assessment of an applicant-provided cybersecurity solution.



Figure 1. AENAON Service and tool stack

1.3 Structure and Use of the Tool Profiles

Section 2 presents a concise profile for each AENAON tool. Every profile follows a common structure covering:

- a high-level overview of the tool and its main function;
- examples of potential Open Call use;
- the expected deployment and access model;
- the principal inputs and outputs; and
- any important technical prerequisites, dependencies and limitations.

Applicants should review the profiles in relation to their proposed technical activities and clearly identify which tool or combination of tools they intend to use. The proposal should explain the role of each selected tool, the information or environment that the applicant will provide, the expected integration or configuration work, and the outputs or validation evidence expected from its use.

The tool profiles provide an indicative technical baseline. Actual integration requirements may vary according to the proposed scenario, the maturity of the applicant's solution, the availability and quality of relevant data, the number of systems involved and the level of customisation required. Any use of the tools must also respect applicable access-control, confidentiality, data-protection and authorised-testing requirements.

2. Tool Profiles

2.1 Digital Twin Solution

Service family: Digital Twins & Virtualisation Services Provider: ZELUS
--

Tool overview

A distributed industrial control system simulation and digital twin platform for offshore wind farms, leveraging OPC UA and TCP fieldbus communication to replicate turbine operations, electrical infrastructure, and environmental conditions. By combining real-time sensor data, historical operational data, weather information, and performance metrics, the digital twin provides a dynamic representation of the physical wind farm, enabling monitoring, predictive maintenance, energy optimisation, and improved operational decision-making.

Potential Open Call use

The Digital Twin Solution can support open call applicants seeking to test, validate, or demonstrate cybersecurity approaches within a representative, simulated offshore wind farm environment. It enables the safe execution of attack scenarios, threat simulations, and security control assessments without risk to live operational assets. Applicants developing solutions in areas such as intrusion detection, vulnerability assessment, incident response, or OT/ICS security can use the platform as a realistic testbed to prototype, evaluate, and validate their approaches against simulated industrial conditions.

Deployment & Access

The platform is deployed as a containerised service using Docker, and can be hosted on-premises or within a private cloud environment. Access is provided through a web-based interface for dashboards and reporting, alongside programmatic access via OPC UA endpoints and REST APIs for integration with external tools and analytics pipelines. Credentials and network access details are issued upon onboarding. The environment can be provisioned on request and configured to reflect specific wind farm topologies or operational scenarios relevant to the applicant's use case.

Inputs & Outputs

The digital twin requires turbine operational parameters, industrial control system configurations, OPC UA and TCP fieldbus data, real-time sensor measurements, weather information, and historical operational records to accurately simulate wind farm behavior and support monitoring, optimization, and predictive maintenance. Based on these inputs, it produces real-time operational insights, simulated system states, performance metrics, anomaly detection results, and predictive maintenance information, which are presented through dashboards, reports, and analytical tools to support wind farm monitoring, energy optimization, asset management, and operational decision-making.

Technical prerequisites, dependencies, limitations

The digital twin requires a Docker environment hosting its Python-based simulation platform, supporting libraries, and communication services. It depends on OPC UA and TCP fieldbus interfaces, wind turbine and ICS models, operational data sources, and network connectivity to accurately simulate and monitor offshore wind farm operations.

2.2 Penetration Testing Solution

Service family: Vulnerability Discovery & Penetration Testing Services Provider: ZELUS

Tool overview

Automated Security Assessment Toolkit (ASAT) is an extensible platform for orchestrating network and web security scans and storing their results in a graph database. It runs Nmap, Nikto, ADEnum, Kerbrute, and FFuF behind a single REST API, executes each scan in an isolated Docker container, and persists in hosts, services, and findings in Neo4j for correlation and reporting.

Potential Open Call use

ASAT can support open call applicants seeking to perform structured security assessments as part of vulnerability discovery, penetration testing, or attack surface mapping use cases. It enables applicants to rapidly enumerate assets, identify exposed services, and surface known vulnerabilities across target environments through a single orchestrated interface. Teams developing solutions in areas such as threat detection, risk scoring, or remediation workflow automation can leverage ASAT's Neo4j-backed findings as a structured data source, using the correlated graph output to prototype and validate their approaches against realistic assessment results.

Deployment & Access

ASAT is deployed as a containerised application stack using Docker, comprising the Python-based orchestration platform, integrated security tools, and a Neo4j graph database instance. It can be hosted on-premises or within an isolated private network environment. Access is provided through a web-based dashboard for scan management and reporting, and via a REST API for programmatic integration with external pipelines or tooling. User credentials and network access details are issued upon onboarding. The environment can be scoped and configured to reflect specific assessment scenarios relevant to the applicant's use case.

Inputs & Outputs

ASAT requires authenticated user credentials to access the platform dashboard, together with project identification details, target IP addresses or network ranges, and scan configuration parameters, including tool-specific flags and custom scan options for non-default assessments. These inputs enable ASAT to define the assessment scope, configure security scanning workflows, and execute targeted vulnerability analysis. Based on the collected data, ASAT generates structured security assessment results, including discovered assets, services, vulnerabilities, and findings from integrated security tools. It correlates this information within a graph database to enhance attack surface visibility, support risk analysis, and facilitate remediation planning, while also producing customizable assessment reports that can be exported in PDF format for documentation, analysis, and stakeholder communication.

Technical prerequisites, dependencies, limitations

ASAT requires a Docker environment hosting its containerized Python application, Neo4j database, and integrated security tools. It operates with modest resource requirements and depends mainly on network access to authorized targets and correct container configuration.

2.3 xBOMGuard

Service family: Vulnerability Discovery & Penetration Testing Services Provider: CILIX

Tool overview

xBOMGuard is a platform providing xBOM-driven cyber asset intelligence. It transforms structured BOM evidence into component, version, supplier and dependency views, enriches them with vulnerability and exploitability intelligence, and supports contextual prioritisation, blast-radius analysis and reporting.

Potential Open Call use

Applicants may analyse a product or representative offshore-wind software stack, identify vulnerable, outdated or unsupported components and dependency paths, prioritise testing or remediation, and generate exposure summaries for penetration-testing or risk-assessment activities.

Deployment & Access

CILIX will host and operate xBOMGuard for the supported Open Call activities. Selected beneficiaries will receive controlled browser access to a project-scoped workspace and will not need to deploy the platform. Where justified, authorised machine-to-machine exchange may use the documented REST API with scoped credentials. Self-managed deployment, source code, deployment artefacts, direct database or raw-graph access, and internal APIs are not included.

Inputs & Outputs

- **Inputs:** CycloneDX JSON BOMs are preferred. SPDX JSON, structured inventories, SARIF findings, purl/CPE identifiers and optional lifecycle, criticality or VEX/OpenVEX evidence may also be used where supported.
- **Outputs:** dashboards; component and dependency inventories; enriched findings; priority bands and reason codes; project, release and supplier views; blast-radius and posture summaries; JSON outputs; PDF/CSV reports; and applicable CycloneDX or SARIF exports.

Technical prerequisites, dependencies, limitations

- **Limitations:** results depend on the completeness and currency of the supplied evidence. Physical or OT assets are represented only where provided as structured evidence. xBOMGuard does not replace active discovery, penetration testing, monitoring or incident response; a matched vulnerability indicates potential exposure, not confirmed exploitation.
- **Data handling:** sensitive or operational data should only be submitted where authorised and in accordance with the applicable security and confidentiality conditions. Representative or synthetic BOMs may be used where operational evidence cannot be shared.
- **Licensing:** xBOMGuard is proprietary CILIX background. Access is limited to the agreed Open Call activities. Extensions, unsupported integrations, dedicated deployments or continued use outside that scope require prior agreement with CILIX.

2.4 Cyber Range Solution

Service family: Security Awareness & Cyber Range Services Provider: ZELUS
--

Tool overview

A cyber range and training platform (Cyber Range & IC RTP) that orchestrates scenarios and executes training exercises for wind farm operators, working alongside a Digital Twin & Virtualization component to provide realistic, virtualized infrastructure for exercises.

Potential Open Call use

The Cyber Range solution can support open call applicants seeking to design, deliver, or evaluate security training and awareness programmes targeting wind farm operators or OT personnel. It provides a realistic, risk-free environment for testing exercise content, detection rule effectiveness, and incident response playbooks. Applicants developing solutions in areas such as operator readiness assessment, security awareness measurement, or exercise automation can use the platform to run structured training campaigns and collect telemetry for performance evaluation and continuous improvement.

Deployment & Access

The platform is deployed in conjunction with the Digital Twin & Virtualisation component, which provides the underlying emulated infrastructure for each exercise environment. It can be hosted within a private or isolated network environment and is accessible to participants through role-based operator accounts. Exercise scenarios are configured and launched by platform administrators, with access credentials and environment details issued upon onboarding. Scenario complexity and scope can be adjusted to align with the specific training objectives of the applicant's use case.

Inputs & Outputs

The training platform requires exercise and training requests, operator access details from Wind Farm Operators, and detection rules and incident scenarios provided by the Threat Detection & Incident Response component. Using these inputs, it sends scenario environment requests to the Digital Twin component to instantiate realistic training exercises for operators and generates exercise telemetry and outcome data that can be used by other platform components for performance evaluation, analysis, and continuous improvement.

Technical prerequisites, dependencies, limitations

Digital Twin & Virtualization component (for the emulated infrastructure/environment), inputs from Threat Detection & Incident Response for realistic exercise scenarios.

2.5 Risk Assessment Platform

Service family: Threat & Risk Assessment Services Provider: PRIVACT
--

Tool overview

The Risk Assessment Platform delivers AENAON's Threat and Risk Assessments (TRA) Services, assessing risks and threats to offshore-wind digital infrastructures through automated threat and vulnerability analysis. It draws on open vulnerability repositories (CVE/NVD, OSV) and threat feeds and aligns with IACS standards such as ISA/IEC 62443. Knowledge-graph models capture component dependencies and simulate threat propagation to reveal critical points, cascading effects and cyber-physical impact, assessing both individual and cascading risk.

Potential Open Call use

Applicants may model a representative offshore-wind infrastructure, assess individual and cascading risks, prioritise them and generate threat scenarios and mitigation strategies. It provides threat-modelling and risk-scoring baselines through project-scoped service accounts where appropriate.

Deployment & Access

PRIVACT hosts and operates the platform; beneficiaries receive controlled access to a project-scoped workspace and need not deploy it. Where justified, machine-to-machine exchange uses the documented REST API with scoped credentials. Source code, self-managed deployment and internal interfaces are excluded.

Inputs & Outputs

- **Inputs:** an asset portfolio and system model; prioritised software/component exposure from xBOMGuard; and cyber and strategic threat-intelligence feeds (CTI/SCTIP), including open vulnerability repositories such as CVE/NVD and OSV.
- **Outputs:** threat modeling; risk scores and prioritisation; individual and cascading risk paths; knowledge-graph risk models; threat and risk scenarios with mitigation strategies; and risk-assessment reports.

Technical prerequisites, dependencies, limitations

- **Limitations:** results depend on the completeness and currency of the supplied portfolio, xBOMGuard exposure and CTI/SCTIP inputs. It delivers risk analysis, modelling and prioritisation - not active discovery, penetration testing, monitoring or incident response; a modelled risk is potential, not confirmed, exposure.
- **Data handling:** sensitive data should be submitted only where authorised and in line with the applicable conditions; representative or synthetic models may be used otherwise.
- **Licensing:** a proprietary PRIVACT-operated service for the agreed Open Call activities; use beyond that scope requires prior agreement with PRIVACT.

2.6 Cyber Threat Intelligence Platform

Service family: Threat & Risk Assessment Services Provider: ENDOSCOPE
--

Tool overview

CTIP is an AI-assisted Cyber Threat Intelligence platform operated by ENDOSCOPE. It supports Threat and Risk Assessment services by enabling structured threat information sharing, situational awareness and knowledge sharing across the AENAON workflows. The platform ingests Cyber Threat Intelligence data and Indicators of Compromise through CTI feeds and dedicated ingestion endpoints. It enriches and correlates the collected information with contextual metadata generated through ENDOSCOPE-managed ETL and enrichment processes, transforming raw threat data into actionable intelligence that can be consumed by analysts and other AENAON components. The platform provides Role-Based Access Control, standard CRUD functionality, CTI feed management, and custom ingestion and enrichment endpoints developed to address pilot-specific AENAON requirements.

Potential Open Call use

CTIP can support future Open Call pilots by supplying the Threat Intelligence data required by their Threat and Risk Assessment activities and downstream AENAON workflows.

Deployment & Access

ENDOSCOPE will host and operate CTIP for the supported Open Call activities. Selected beneficiaries will receive controlled API access to an organization workspace and will not need to deploy the platform. Where justified, authorised machine-to-machine exchange will use the documented REST API with scoped credentials. Self-managed deployment, source code, deployment artefacts, direct database and internal APIs are not included.

Inputs & Outputs

- **Inputs:** CTIP accepts structured Cyber Threat Intelligence data through its REST/JSON interfaces and CTI ingestion mechanisms.
- **Outputs:** enriched Indicators of Compromise; contextual metadata associated with submitted indicators; structured REST/JSON responses; results produced through pilot-specific enrichment endpoints; CTI data prepared for consumption by downstream AENAON workflows.

Technical prerequisites, dependencies, limitations

- **Limitations:** CTI feeds are curated and updated periodically rather than continuously. Consequently, the platform's results reflect the information available from the configured sources at the time of the request and should be assessed together with other relevant Threat and Risk Assessment evidence.
- **Data handling:** sensitive or operational data should only be submitted where authorised and in accordance with the applicable security and confidentiality conditions.
- **Licensing:** CTIP is proprietary ENDOSCOPE background. Access is limited to the agreed Open Call activities. Additional integrations, dedicated deployments, unsupported endpoints, broader access rights or continued use outside the agreed scope require prior agreement with ENDOSCOPE.

2.7 Threat Hunting & Monitoring

Service family: Risk/Threat Monitoring & Cyberattack Management Services Provider: CILIX

Tool overview

The CILIX Threat Hunting & Monitoring Workbench is a hosted prototype for preparing and documenting hypothesis-driven hunts. It translates exposure, vulnerability, risk and CTI/TTP context into structured investigation objectives, Kestrel-compatible huntbooks and reusable hunt packs for representative IT, OT and digital supply-chain scenarios.

Potential Open Call use

Open Call participants may design pilot-specific hunt scenarios, map assets, vulnerabilities, indicators and MITRE ATT&CK techniques to investigation steps, generate Kestrel-compatible hunt packs and document findings. Packs may be executed through an external Kestrel runtime when connectors and telemetry are available; otherwise representative or synthetic data may support sample workflows.

Deployment & Access

The workbench will be hosted and operated by CILIX as a standalone online service for the supported Open Call activities. Selected beneficiaries will receive managed browser-based workspace access and will not be required to deploy the workbench locally. Exchange with other tools is primarily manual or file-based. Generated hunt packs may be exported for execution through a separately configured, compatible Kestrel runtime. The external runtime, relevant connectors and access to suitable telemetry are required only where live or representative hunt execution forms part of the proposed use case. Connection to live operational telemetry is subject to explicit prior authorisation.

Inputs & Outputs

- **Inputs:** Manual or agreed CSV/JSON input; a hunt hypothesis; asset, exposure, vulnerability and risk context; IoCs, TTPs and CTI/STIX 2.1 information where available; and compatible logs or telemetry for execution.
- **Outputs:** Structured hypotheses and investigation steps; Kestrel huntbooks and hunt packs (.hf); Markdown/PDF reports; analyst findings; and JSON/CSV result summaries where available. Execution records depend on the external runtime and connected data sources.

Technical prerequisites, dependencies, limitations

- **Limitations:** Results depend on data coverage and connector compatibility. The workbench does not collect telemetry and is not a production SIEM/SOAR, EDR, SOC/MDR or 24/7 service. It provides no automated response or incident management.
- **Licensing:** The workbench is a proprietary CILIX prototype. Access is provided for the agreed AENAON Open Call activities. Source code and self-managed deployment are not included. Exported Kestrel-compatible hunt packs may be used in approved external runtime environments, subject to the applicable runtime licences, access permissions and security conditions. Hunt hypotheses, IoCs, TTPs, hunt packs and execution results may contain sensitive security information and must be handled accordingly.

2.8 Threat Detection & Incident Response Platform

Service family: Risk/Threat Monitoring & Cyberattack Management Services Provider: PRIVACT

Tool overview

The Threat Detection & Incident Response Platform provides the functional capabilities for threat detection and for monitoring risk and incidents. It brings network and endpoint activity together into a single monitoring and analysis environment, enriched with asset context and threat-intelligence, supports correlation among assets, vulnerabilities and threats so that suspicious activity is detected, alerted and investigated. It allows review of the existing attack surface and the effectiveness of control actions against identified risks, supporting informed decision-making and an effective incident-response workflow. The platform underpins AENAON's Risk Monitoring and Cyberattack Management (RMCM) Services.

Potential Open Call use

Applicants may use the platform to monitor a representative environment, detect threats across network and endpoint activity, and investigate and document incidents. It can also be used to review the attack surface, assess how effective existing controls are against identified risks, and demonstrate a detection-to-response workflow. It can draw on the outputs of other AENAON tools - such as exposure, vulnerability and threat-intelligence context - to inform detection and prioritisation.

Deployment & Access

PRIVACT will host and operate the platform for the supported Open Call activities. Selected beneficiaries will receive controlled access to a project-scoped workspace and will not need to deploy the platform. Monitoring of live operational data is subject to prior authorisation and to the applicable access and confidentiality conditions. Self-managed deployment, source code and internal interfaces are not included.

Inputs & Outputs

- **Inputs:** network and endpoint activity (from live monitoring or representative data), threat-intelligence indicators, and asset and criticality context.
- **Outputs:** prioritised alerts, monitoring dashboards, investigation records and cases, summary reports and evidence.

Technical prerequisites, dependencies, limitations

- **Limitations:** the platform is used for detection and monitoring; it identifies and helps investigate potential threats but does not carry out prevention or automated response, and is not a 24/7 managed monitoring service. The quality of detection depends on the coverage and currency of the data, indicators and asset context provided; an alert indicates activity that requires review, not confirmed compromise.
- **Data handling:** monitoring data and incident information may be sensitive and should be provided and handled only where authorised and in line with the applicable security, confidentiality and data-protection conditions. Representative data may be used where operational data cannot be shared.
- **Licensing:** the platform is provided as a proprietary PRIVACT-operated service for the agreed Open Call activities. Extensions, dedicated deployments or continued use beyond that scope require prior agreement with PRIVACT.

2.9 Strategic Cyber Threat Intelligence Platform (SCTIP)

Service family: Risk/Threat Monitoring & Cyberattack Management Services Provider: ENDOSCOPE

Tool overview

The Strategic Cyber Threat Intelligence Platform (SCTIP) is an ENDOSCOPE-operated platform supporting Risk/Threat Monitoring and Cyberattack Management activities within AENAON. SCTIP analyses evolving attack surfaces and transforms technical and operational findings into structured, actionable Cyber Threat Intelligence reports. For the supported pilot scenario, the platform produces customised reports focused on offshore wind farm environments, their exposed assets, relevant threats, vulnerabilities, adversary tactics, techniques and procedures, and recommended mitigation priorities.

Potential Open Call use

SCTIP can support Open Call pilots by producing pilot-specific Threat Intelligence reports based on their operational context, asset scope and identified security concerns.

Deployment & Access

SCTIP is hosted and operated by ENDOSCOPE as a cloud-based service. No local deployment, installation or infrastructure provisioning is required from consortium partners, pilot organisations or Open Call participants. Selected beneficiaries will receive controlled API access to an organization workspace and will not need to deploy the platform. Where justified, authorised machine-to-machine exchange will use the documented REST API with scoped credentials. Self-managed deployment, source code, deployment artefacts, direct database and internal APIs are not included.

Inputs & Outputs

- **Inputs:** SCTIP uses information supplied by the pilot and relevant AENAON services through its REST/JSON interfaces to prepare customised Threat Intelligence reports.
- **Outputs:** SCTIP produces customised Threat Intelligence reports and structured intelligence outputs that may include: identification of relevant threat actors or adversary profiles, where supported by available evidence; agreed report or data exports for RAP, TDIR and the CLX workbench; API-based JSON responses; applicable tactics, techniques and procedures.

Technical prerequisites, dependencies, limitations

- **Limitations:** Threat Intelligence reports are based on the information and intelligence available at the time of generation. Changes to the pilot environment, newly disclosed vulnerabilities, emerging threat actors or updated intelligence may affect the relevance of previously generated findings.
- **Data handling:** sensitive or operational data should only be submitted where authorised and in accordance with the applicable security and confidentiality conditions.
- **Licensing:** Use of SCTIP is limited to the agreed consortium, pilot or Open Call activities. Additional integrations, dedicated deployments, continuous monitoring services, operational incident-response support or continued use outside the agreed scope require prior agreement with ENDOSCOPE.



Co-funded by
the European Union



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Partners



SIEMENS



Contact

AENAON Consortium
info@aenaon-project.eu