



NGSOC

Next Generation Security Operations Centres

Next Generation Security Operation Centres

D6.1 Validation methodology and users identification

Report Identifier:	D6.1		
Work-package:	WP6	Task:	T6.1
Responsible Partner:	ED	Version Number:	1.0
Due Date	31/07/2025	Document Date:	09/01/2026
Distribution Security:	PU	Deliverable Type:	Report (R)
Keywords:	NG-SOC Platform, Validation, Methodology		
Project website: https://ng-soc.eu/			

Document History

Version	Content & Changes	Issue Date
0.1	Document created	15/09/2025
0.2	Document sent for review	02/10/2025
0.3	Document reviewed	07/10/2025
0.4	Document reviewed	10/12/2025
0.11	Reviews are combined	23/12/2025
0.12	Sent for Quality Assurance	28/12/2025
1.0	Quality Assurance and Submission	09/01/2026

Quality Control

	Name	Organisation	Date
Editor 1	Themis Kolyvas	ED	21/06/2025
Editor 2	Jose Maria Romero	FUNITEC	29/09/2025
Peer review 1	Apostolos Gkletos	EDGR	07/10/2025
Peer review 2	Konstantinos Maliatsos	INS	10/12/2025
Authorised by (Technical Coordinator)	Mateusz Zych	Cyentific AS	28/12/2025
Authorised by (Quality Manager)	Apostolos Gkletos	ED	07/01/2026
Submitted by (Project Coordinator)	Anastasia Garbi	ED	09/01/2026

Legal Disclaimer

NG-SOC is an EU project funded by the Digital Europe Programme (DIGITAL) under grant agreement No. 101145874. 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 NG-SOC 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.

Copyright notice

© Copyright by the NG-SOC Consortium

This document contains information that is protected by copyright. All Rights Reserved. No part of this work covered by copyright hereon may be reproduced or used in any form or by any means without the permission of the copyright holders.

Table of Contents

Table of Contents	4
List of Figures.....	5
List of Tables	6
Abbreviations	7
Executive Summary	9
1 Introduction.....	10
1.1 Overview.....	10
1.2 Relation to other tasks and deliverables.....	10
1.3 Deliverable Structure.....	10
1.4 Consortium Context and New Partners.....	11
2 Validation Methodology.....	12
2.1 Validation objectives	13
2.2 Validation Framework	13
2.3 Validation Criteria and Metrics	14
2.4 Validation Process	15
2.5 Pilot Context.....	16
2.6 Evidence & Reporting.....	16
3 Pilot Sectors and Use Cases.....	18
3.1 Overview.....	18
3.2 Pilot Sectors and Use Cases.....	18
3.3 Cross-pilot notes (interfaces & stakeholders)	21
4 Users Identification	22
4.1 User Categories	23
4.2 Supporting Users	23
4.3 User Mapping Table	24
5 Validation Phases and Link to WP6 Deliverables	25
6 Conclusion	28
REFERENCES	31
APPENDIX	32

List of Figures

Figure 1 Validation hierarchy 14

Figure 2 Validation Process Cycle 22

Figure 3 Provenance of Metrics and Targets..... 30

List of Tables

Table 1 Inputs from Deliverables 10

Table 2 User Mapping Table..... 24

Table 3 Map UR to Validation 32

Abbreviations

Acronym	Description
DoW	Description of Work
EU	European Union
EC	European Commission
GA	Grant Agreement
IDEB	Innovation, Dissemination & Exploitation Board
IPR	Intellectual Property Rights
KPI	Key Performance Indicator
UAT	User Acceptance Testing
MTTA	Mean Time To Acknowledge
MTTR	Mean Time To Resolve
ECSF	European Cybersecurity Skills Framework
MoSCoW	Must, Should, Could, Won't
FPR	False Positive Rate
SUS	System Usability Scale
SLA	Service Level Agreement
DSP	Digital Service Provider
NIS2	Directive (EU) 2022/2555 (Network & Information Security 2)
PC	Project Coordinator
PEB	Project Executive Board
PMI	Project Management Institute
PGA	Project General Assembly
QAS	Quality Assurance Supervisor
QMP	Quality Management Plan
SW, S/W	Software
TL	Task Leader
WP	Work Package
WPL	Work Package Leader
CTI	Cyber-Threat Intelligence
DMP	Data Management Plan
DPO	Data Protection Officer

DoA	Description of the Action
FUI	Federated User Interface
GDPR	General Data Protection Regulation

Executive Summary

This deliverable defines the **validation methodology and users identification framework** for the NG-SOC project. It represents the foundation of WP6, guiding how technical components, the integrated platform, and pilot activities will be validated against user, system, and regulatory requirements.

The methodology adopts **standards-based, multi-level validation** (component, system, pilot) and incorporates **KPIs** covering technical performance, usability, interoperability, and impact. It ensures traceability to requirements (D2.3), architecture (D2.4), skills development (D5.1), and exploitation plans (D7.1).

Three pilots provide the basis for validation:

- **CaixaBank** (Banking): focusing on fraud detection and automation of SOC workflows.
- **CYNET** (Academic/CSIRT Training): advancing cybersecurity capacity building through experiential learning and incident simulations.
- **ELES/INFO** (Energy): strengthening resilience and real-time risk management in critical energy infrastructures.

Users are identified across **analysts, SOC operators, risk managers, trainers, and regulators**, with specific mappings per pilot.

Validation activities explicitly address **compliance with NIS2, the Cybersecurity Act, and the Cyber Solidarity Act**, ensuring the NG-SOC solution supports EU policy goals. This deliverable also introduces ethical and GDPR safeguards for real-world pilot execution.

1 Introduction

1.1 Overview

NG-SOC aims to establish a network of next-generation, AI-enabled, and interoperable Security Operations Centres (SOCs) across the EU. The project integrates advanced SOC components, including the Behavioural Intrusion Prevention System (BIPS), NG-SIEM, NG-SOAR, CICMS, CTI sharing system, Dynamic Risk Management Engine, Penetration Testing module, Cyber Range, and training platform, into a modular architecture validated through real-world pilots.

1.2 Relation to other tasks and deliverables

The purpose of D6.1 is to:

- Define a common methodology for validating NG-SOC tools and pilots.
- Identify and profile the user groups who will participate in validation.
- Establish criteria, metrics, and processes for validation activities.
- Ensure traceability between WP2 requirements, WP5 training needs, and WP6 validation results.
- Provide the foundation for subsequent WP6 deliverables (D6.2 - D6.5).

Receives inputs from:

Table 1 Inputs from Deliverables

Deliverable	Description
D1.1	provides quality assurance framework
D2.3	defines requirements forming validation criteria
D2.4	links requirements to technical components
D5.1	validation of training effectiveness
D7.1	alignment with KPIs and dissemination strategy

1.3 Deliverable Structure

This deliverable sets out the **validation methodology** and **users' identification** for NG-SOC pilots and explains how validation will be executed and accepted across WP6. The document is organised as follows:

- **Section 1 – Introduction.** Purpose and scope of D6.1, relation to other WPs/deliverables, and consortium context.
- **Section 2 – Validation Methodology.** Objectives, framework, criteria/metrics, and processes used to validate NG-SOC components and the integrated platform (component → system → pilot), including compliance aspects and evidence collection.

- **Section 3 – Pilot Sectors and Use Cases.** Overview of stakeholders and detailed sector pilots: **Banking (CaixaBank)**, **Educational/Training (CYNET/FUNITEC)**, and **Energy (ELES/INFO)**—with representative flows, validation activities, and success metrics.
- **Section 4 – Users Identification.** User categories, supporting users, and a mapping table linking roles to pilots, components exercised, evidence, and KPIs.
- **Section 5 – Validation Phases and Link to WP6 Deliverables.** Phased execution across **D6.1–D6.5** (methodology/users; integration & testing; pilots preparation/execution/success indicators; users' acceptance & validation), with inputs, activities, outputs, acceptance gates, and KPIs.
- **Section 6 – Conclusion.** Key takeaways and next steps, maintaining KPI alignment and traceability to requirements and architecture.
- **References** and **Appendix** materials (e.g., user mapping table) complete the document.

This structure ensures traceability from **requirements (D2.3)** and **architecture/interfaces (D2.4)** to **pilot evidence and acceptance (D6.4–D6.5)** under the WP6 quality and KPI framework.

1.4 Consortium Context and New Partners

Following the GA amendment, three new partners joined:

- **ELES** (Slovenian TSO) and **INFO** (SOC services for ELES), jointly leading the **energy pilot**.
- **FUNITEC** (Universitat i Tecnologia, Spain), reinforcing **training and user acceptance** in WP5 and WP6.

2 Validation Methodology

NG-SOC Objectives

- a) An interoperable CTI toolbox that can both exchange and **operationalise** machine- and human-readable CTI from multiple sources (e.g., CERT-EU, NIS Cooperation Group, EU CyCLONe). This means CTI is not only shared but also **used** in rules, detections and playbooks.
- b) Incident-response capacities aligned with good practices of the CSIRTs Network and CERT-EU, enabling interaction across established SOCs, EU actors and third parties. In practice, this is tested through end-to-end cases run across partners.
- c) Dedicated training and education in digital-infrastructure security, tailored to identified goals and delivered through multiple methods (self-paced and hands-on).
- d) AI-enhanced technologies to predict, detect and analyse threats within an open-standards, interoperable architecture to avoid vendor lock-in and enable cross-border sharing.

For all objectives: (objective → measurable objective → validation indicator)

Objective 01 — Interoperable CTI toolbox

Measurable objective. Integrate ≥3 CTI sources; exchange and operationalise CTI across NG-SIEM/NG-SOAR/CICMS using STIX 2.x/TAXII; package and execute CACAO v2 playbooks; ingest-to-distribution latency ≤5 minutes in pilots.

Validation indicators.

- ≥90% of CTI feeds active and standards conformant.
- Number of CACAO v2 playbooks imported/exported and validated.
- ≥70% of relevant alerts enriched with IoC/IoA from CTI-SS.
- SOC analyst UAT rating on CTI usefulness ≥4/5.

Objective 02 — Incident response aligned with CSIRTs/CERT-EU practices

Measurable objective. Reduce MTTA and MTTR by ≥20% through NG-SOAR automation (CACAO), CICMS workflows and NG-SIEM triggers; ≥10 validated playbooks per pilot.

Validation indicators.

- Baseline vs pilot MTTA/MTTR deltas (from CICMS case timelines).
- Number of playbooks executed successfully and % automated steps.
- % NG-SIEM alerts that open CICMS cases and trigger playbooks.
- Stakeholder satisfaction ≥4/5 with auditable evidence in CICMS.

Objective 03 — Training and education programmes

Measurable objective. Deliver an ECSF-aligned curriculum via Open edX (self-paced) and KYPO/CyberRangeCZ (hands-on); $\geq 80\%$ course completion and $\geq 75\%$ practical-exercise success across target roles.

Validation indicators.

- Role mapping to ECSF and pilot needs.
- Learning analytics: completion, assessment scores, pre/post skill uplift.
- Platform KPIs: scenario availability and range stability/usage.

Objective 04 — AI-enhanced prediction, detection and analysis

Measurable objective. Demonstrate AI-supported detection (e.g., BIPS) integrated with NG-SIEM; precision/recall ≥ 0.80 on pilot datasets; false-positive rate $\leq 10\%$; real-time JSON outputs consumed by NG-SIEM/CICMS.

Validation indicators.

- Detection quality (precision, recall, FPR (False Positive Rate)) and time-to-analysis vs baseline.
- Successful end-to-end consumption of BIPS outputs by other components.
- Operator UAT on explainability/usefulness $\geq 4/5$.

2.1 Validation objectives

The objectives are to explain **what success looks like** and **how we will prove it**:

- Ensure compliance with user and system requirements (D2.3) and keep MoSCoW (Must, Should, Could, Won't) priorities traceable to tests.
- Verify that each component meets its specification and integrates as designed (D2.4 architecture & interfaces).
- Assess usability, scalability, interoperability, and alignment with NIS2 and EU policy goals during pilots.
- Provide measurable outcomes using project KPIs (e.g., MTTR reduction, requirements coverage, user satisfaction).

How this will be evidenced: Requirements $\rightarrow$ test cases $\rightarrow$ pilot scenarios are linked in a simple traceability view (Requirement ID $\rightarrow$ Component(s) $\rightarrow$ Test/Scenario $\rightarrow$ KPI). Evidence comes from logs, CICMS audit trails, NG-SOAR playbook records, and training analytics.

2.2 Validation Framework

We validate at **three levels**, combining technical verification and user acceptance, aligned to WP6 tasks T6.2–T6.3.

1. **Component-level testing.** Unit/integration tests per module (BIPS, NG-SIEM, NG-SOAR, CICMS, CTI-SS, DRME, Pen-Test, Cyber Range, Open edX). Purpose: check each asset against its specs and interfaces before integration. Example: NG-SOAR can import/export CACAO v2 and validate schemas.

2. **System-level validation.** End-to-end data-flow tests in a pilot-like environment exercising the **Interfaces Model** (e.g., BIPS → NG-SIEM → CICMS → NG-SOAR, including CTI enrichment). Purpose: verify orchestration and performance with realistic loads.
3. **Pilot-level validation (UAT).** Sector-specific scenarios in Banking, Education/Training and Energy to observe real workflows, constraints, and regulations. Purpose: ensure usefulness and acceptance in operational contexts.

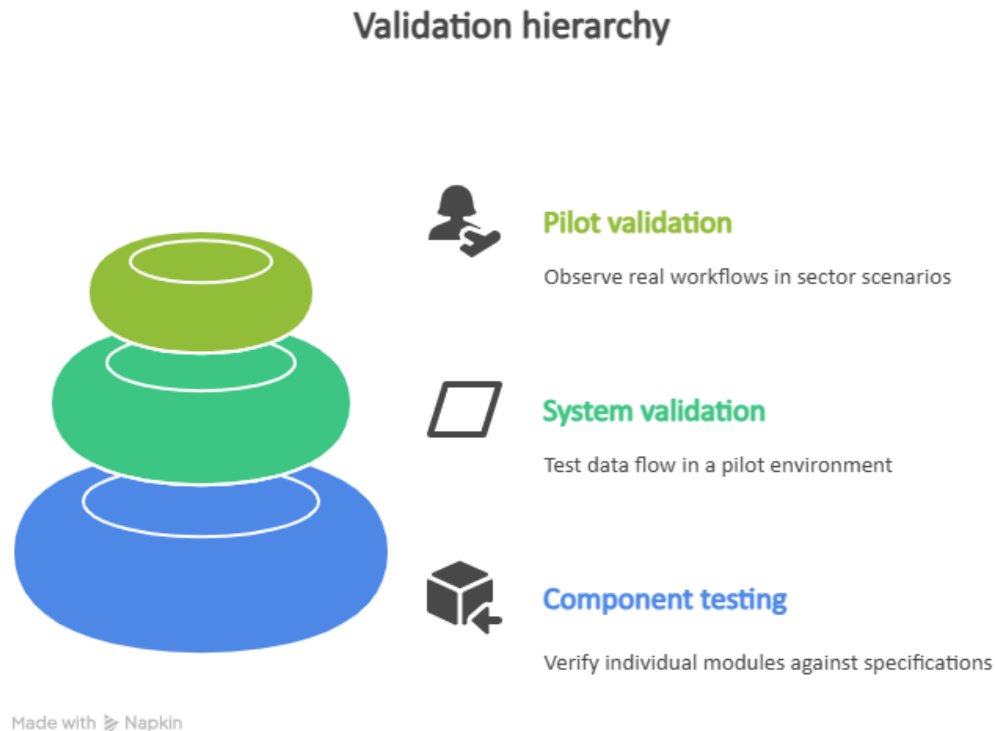


Figure 1 Validation hierarchy

Security & compliance checks (GDPR, NIS2) are embedded in CICMS case artefacts (roles, access control, audit trails) and in documentation packages produced per release [12][13].

Environment & Governance. Builds are promoted to “stable” only after integration tests pass; binaries and docs are distributed via the consortium repository; issues are tracked centrally to close the loop between tests and fixes.

2.3 Validation Criteria and Metrics

Security & resilience

- Detection quality (precision/recall/FPR for BIPS/analytics), alert enrichment rate, MTTA/MTTR; playbook execution success and error rates. *Measured with component logs, NG-SIEM indices, and CICMS timelines.*

Usability & user acceptance.

- SUS (System Usability Scale)/UAT (User Acceptance Testing) questionnaires per role (analysts, incident responders, trainers). *Collected after pilot sessions and major releases.*

Interoperability with open standards

- Conformance to STIX/TAXII and CACAO; ability to exchange playbooks/incident data via MISP/CTI-SS and to orchestrate actions via NG-SOAR ↔ CICMS. *Checked through schema validation and end-to-end exchanges.*

Performance & scalability.

- Ingest/processing latency, throughput, stability under pilot loads; evidence that BIPS/NG-SIEM/CICMS operate real-time per interface specs.

Training impact.

- Completion and pass rates on Open edX; success in CyberRangeCZ scenarios; pre/post skill uplift aligned to ECSF. *Captured via platform analytics and assessment exports.*

Operational impact.

- % of alerts auto-triaged by NG-SIEM/NG-SOAR (CACAO playbooks) and BIPS; CICMS is used only for case handling & reporting. Measured as: reduction in manual effort (minutes/alert), % cases created/updated in CICMS with complete audit trail, and SLA compliance. Baseline: pre-pilot process without NG-SOAR auto-triage.

Project-level KPIs.

- Requirements coverage (≥90%), integrated-system success, user satisfaction (≥80% “satisfactory”), and integration problem resolution time—used as acceptance gates.

2.4 Validation Process

User-based stream. Role-specific UAT (analyst, responder, trainer) using **structured SUS/UAT surveys** (Likert 1–5). **Optional** think-aloud sessions and short debrief meetings, **as feasible and agreed with pilot owners**. Notes are captured only at the aggregate level and fed back into the backlog.

Sampling & data collection.

To obtain stable metrics while respecting pilot constraints, we adopt the following **default sampling targets** (to be **confirmed and, if needed, adjusted** by each pilot during D6.4 readiness reviews):

- **Alert timing/performance analyses:** about **200 alerts** per analysis **or** at least **one full week** of normal operations (whichever is larger).
- **Training analytics:** about **20 trainees** per course/cohort to derive meaningful completion and uplift statistics.
- **UAT cadence:** minimum of **one complete UAT round per pilot per major release**. These targets come from D6.1’s measurement approach and WP7’s KPI cadence; these are **targets, not hard commitments**, and may be scaled up/down based on volume, risk and data-protection constraints.

Acceptance thresholds (pilot targets to be confirmed in D6.4 readiness reviews).

Ownership: *Component Lead proposes → Pilot Owner validates → WP6 Lead approves.*

- **CTI (interoperability & operationalisation).** **Target:** **≥90%** CTI feeds operational and standards-conformant; **≤5-minute** ingest-to-distribution latency in pilots; **≥60–70%** of relevant alerts enriched with IoC/IoA.
Why: 90% sets a high but reachable bar with redundancy; 5 minutes matches near-real-time SOC needs; 60–70% reflects typical relevance rates once noisy alerts are filtered.
- **Incident Response (automation & coordination).** **Target:** **≥15–20%** reduction in **MTTA/MTTR** versus pilot baseline; **≥9** CACAO playbooks validated (or **≥3** per pilot); **≥50%** of automated steps are executed without error.
Why: 15–20% is a material improvement recognised in WP KPIs; playbook counts ensure functional coverage;
- **Training & Education (ECSF-aligned).** **Target:** course **completion ≥80%**; scenario **success ≥70–80%**; measurable **pre/post skill uplift** for target roles (Open edX/CyberRangeCZ analytics).
Why: Standard thresholds for training effectiveness and statistical sufficiency of cohorts.
- **AI-enhanced detection (e.g., BIPS).** **Target:** precision/recall **≥0.80** on pilot datasets; false-positive rate **≤10%** at target thresholds; **real-time JSON outputs ingested by NG-SIEM/NG-SOAR; cases then created/updated in CICMS for handling and reporting.**
Why: 0.80/≤10% is an accepted balance between reliability and alert fatigue; real-time intake tests end-to-end integration.

Quality and risk hooks. Project KPIs (WP6/WP7) are reviewed at each milestone; deviations are documented per QMP, with corrective actions tracked to closure.

Ethics & GDPR. Pilots use minimum-necessary data; access is role-based; audit trails are part of acceptance; consent/notice templates are included where users participate in training/UAT. Evidence is captured within CICMS or linked repositories.

2.5 Pilot Context

- **Banking (CaixaBank).** Fraud/anomaly detection, workflow automation, CTI-driven playbooks—tests cross-component orchestration under tight SLAs (Service Level Agreements).
- **Education/Training (CYNET).** Data protection and capacity building—proves Open edX + CyberRangeCZ integration and measures skill uplift.
- **Energy (ELES/INFO).** SCADA/OT resilience—validates DRME, Pen-Test module and NG-SOAR actions in critical-infrastructure contexts.

2.6 Evidence & Reporting

- **Evidence pack.** Test logs; CTI conformance reports (STIX/TAXII and CACAO schema validation); CICMS audit trails (cases, tasks, artefacts); NG-SOAR playbook execution records; Open edX and CyberRangeCZ analytics exports.

- **Reports & dashboards.** Per-pilot KPI dashboards and a cross-pilot view with variance vs baseline; requirements-coverage reports (target $\geq 90\%$); narrative summaries of UAT findings and lessons learned for the next iteration.

3 Pilot Sectors and Use Cases

3.1 Overview

Users include **primary end-users (pilots)**, **secondary stakeholders** (regulators, CSIRTs, law-enforcement authorities, academia), and **indirect beneficiaries** (citizens, SMEs, EU cybersecurity community). Primary pilots are: **CaixaBank** (Banking), **CYNET** (Academic/Training), and **ELES/INFO** (Energy). These pilots validate the integrated NG-SOC platform and its components against sectoral needs and NIS2 obligations.

Cross-cutting components exercised in pilots include **BIPS**, **NG-SIEM**, **NG-SOAR**, **CICMS**, **CTI-SS**, **DRME**, **Pen-Test**, **CyberRangeCZ**, and **Open edX**, with interfaces specified in D2.4.

3.2 Pilot Sectors and Use Cases

3.2.1 Banking Sector — CaixaBank

Use case title: Real-time fraud detection and incident response.

Why this matters: Finance is an NIS2/DORA-regulated, high-volume environment; the pilot focuses on detecting subtle transaction anomalies, triaging large alert volumes, and automating response.

Scope & data sources (illustrative): Payment channel telemetry, host/network logs (Windows Event Logs, syslog, NetFlow), CTI indicators, and case/audit artefacts in CICMS.

Process flow (end-to-end):

1. **BIPS** analyses network/host streams; flags anomalies; publishes JSON alerts into NG-SIEM (Kafka→OpenSearch).
2. **NG-SIEM** correlates alerts with CTI and business context; exposes cases/alerts via APIs and dashboards.
3. **CICMS** opens/merges a case, builds a timeline, stores evidence, and coordinates tasks across teams.
4. **NG-SOAR** triggers CACAO v2 playbooks (isolate host, block IP, notify fraud unit, collect artefacts), with executions logged.

Validation activities:

- Interface conformance (BIPS↔NG-SIEM, NG-SIEM↔CICMS, CICMS↔NG-SOAR) per D2.4 Interfaces Model.
- CTI operationalisation: STIX/TAXII ingestion and case enrichment through MISP.
- Performance under load: ingest latency and correlation throughput in “SOC-like” conditions.

Success metrics — pilot-agreed targets (to be confirmed at D6.4 readiness)

Ownership: *Component Lead proposes → Pilot Owner validates → WP6 Lead approves*. Figures below are **example targets**; the final **pilot-agreed target** must be filled in by CaixaBank for this pilot.

- **Detection & triage.**

Example target: ≥20% reduction in MTTA/MTTR; ≥60–70% of relevant alerts enriched with CTI; BIPS precision/recall ≥0.80 and FPR ≤10%.

Pilot-agreed target: To be decided.

Evidence: CICMS timelines; NG-SIEM/CTI logs; BIPS evaluation report.

- **Automation.**

Example target: ≥10 CACAO playbooks validated per pilot (or ≥3 per use case); ≥80% of automated steps execute without error; [% of NG-SIEM alerts auto-opening CICMS cases].

Pilot-agreed target: To be decided.

Evidence: NG-SOAR execution logs; CICMS case creation records.

- **Usability (analysts/fraud unit).**

Example target: UAT ≥4/5; key findings recorded in CICMS timelines and pilot report.

Pilot-agreed target: To be decided.

Evidence: SUS/UAT questionnaires; CICMS artefacts; workshop minutes (aggregate only).

Note: “Example target” expresses a recommended level derived from WP6/WP7 practice; each pilot **must confirm or adjust** the value in “Pilot-agreed target” before execution.

Validation focus (as required): NG-SIEM, NG-SOAR, BIPS, CTI.

3.2.2 Educational Framework — CYNET

Use case title: Protecting student data and network integrity (capacity-building & incident rehearsal).

Why this matters: The academic network (DSP under NIS2) blends technical risk with human factors; the pilot uses training-first validation to raise readiness and test processes safely.

Scope & platforms: **CyberRangeCZ** for hands-on scenarios (isolated sandboxes via OpenStack; scoring, orchestration, telemetry), and **Open edX** for self-paced modules and learning analytics.

Process flow (training-centered scenario):

1. Instructors configure phishing/ransomware/IR scenarios in **CyberRangeCZ**; trainees execute in isolated environments with telemetry captured.
2. **Open edX** delivers pre-work and post-assessments; completion/score data exported for analytics.
3. Selected scenarios feed alerts to **NG-SIEM/CICMS** to rehearse triage/documentation; optional **NG-SOAR** playbooks illustrate automation.

Validation activities:

- Platform readiness (scenario deployment, stability, telemetry capture) in CyberRangeCZ.
- Course delivery/analytics exports in Open edX (API/CSV/OLX inputs; LMS telemetry).
- UAT with trainers/trainees; linkage to ECSF roles via WP5 mapping.

Success metrics — pilot-agreed targets (to be confirmed at D6.4 readiness)

Ownership: *Component Lead proposes → Pilot Owner validates → WP6 Lead approves.* The values below are **example targets**; the final **pilot-agreed target** must be completed by CYNET/FUNITEC for this pilot.

- **Training outcomes.**

Example target: Course completion $\geq 80\%$; scenario success $\geq 70-80\%$; measurable **pre/post skill uplift** per ECSF-mapped role

Pilot-agreed target: To be decided.

Evidence: Open edX analytics exports (completion, grades); CyberRangeCZ telemetry/score files; assessment reports.

- **Process rehearsal.**

Example target: At least **one end-to-end exercise** documented in CICMS (alerts → case → actions → closure), with **UAT $\geq 4/5$** from trainers/trainees.

Pilot-agreed target: To be decided.

Evidence: CICMS timelines and artefacts; SUS/UAT questionnaires; debrief minutes (aggregate only).

Note: “Example target” provides guidance derived from WP6/WP7 practice. Each pilot **confirms or adjusts** the value in “Pilot-agreed target” prior to execution.

Validation focus (as required): Cyber Range, Training Platform, CICMS.

3.2.3 Energy Sector — ELES/INFO

Use case title: Securing critical infrastructure and SCADA systems.

Why this matters: The pilot targets OT/SCADA-adjacent risks (data manipulation, unauthorised access, injection attacks) in a **controlled testbed** replicating live conditions — a deliberate choice to de-risk validation before scaling.

Scope & data sources: Simulated grid telemetry, application logs, OT-app interfaces; threat scenarios driven by current CTI; coordinated response via NG-SOAR and case evidence in CICMS.

Process flow (two representative paths):

A. Data-manipulation detection — BIPS flags anomalies in grid/OT telemetry → **NG-SIEM** correlates with CTI and context → **DRME** updates risk posture → **CICMS** coordinates investigation → **NG-SOAR** executes containment (e.g., block malicious sources, request operator checks).

B. Injection/unauthorised access — Pen-Test module simulates attack paths; alerts flow to **NG-SIEM/CICMS**; **NG-SOAR** semi-automates mitigation; results feed improvements to controls and procedures.

Validation activities

- Testbed execution of scenarios with full artefact capture (logs, timelines, actions).
- DRME and BIPS behaviour under realistic load; NG-SOAR playbooks for OT-adjacent triage/containment.

Success metrics (examples)

- **Threat detection:** BIPS precision/recall around ≥ 0.80 with $\approx \leq 10\%$ FPR (per component specification).
- **Operational response:** MTTA/MTTR improvements vs baseline; documented CICMS audit trails; number of NG-SOAR playbooks validated.

- **Security posture:** reductions in high/critical findings from Pen-Test iterations; DRME risk updates reflected in cases.

Validation focus (as required): Dynamic Risk Engine (DRME), Pen-Test Module, NG-SOAR.

3.3 Cross-pilot notes (interfaces & stakeholders)

- **Interfaces Model:** Detailed APIs and data exchanges for **BIPS**, **NG-SIEM**, **NG-SOAR**, **CICMS** ensure pilots exercise real integrations (REST/TLS, JSON schemas, playbook exchange).
- **Stakeholders & roles:** Platform admins, SOC analysts/responders, DFIR, Pen-Testers, and CTI specialists are identified with responsibilities per pilot.

4 Users Identification

This section identifies **who participates in validation**, **why** they are needed, and **what evidence** they provide. It creates a clear link between **roles** → **responsibilities** → **components exercised** → **evidence produced**, which is required for: (i) requirements traceability (D2.3), (ii) access control and GDPR accountability during pilots, and (iii) users' acceptance in D6.5.

How it is used: The role catalogue below informs UAT sampling, access provisioning, and the **User Mapping Table (4.3)**. Each pilot completes the mapping before execution so that responsibilities and decision rights are unambiguous.

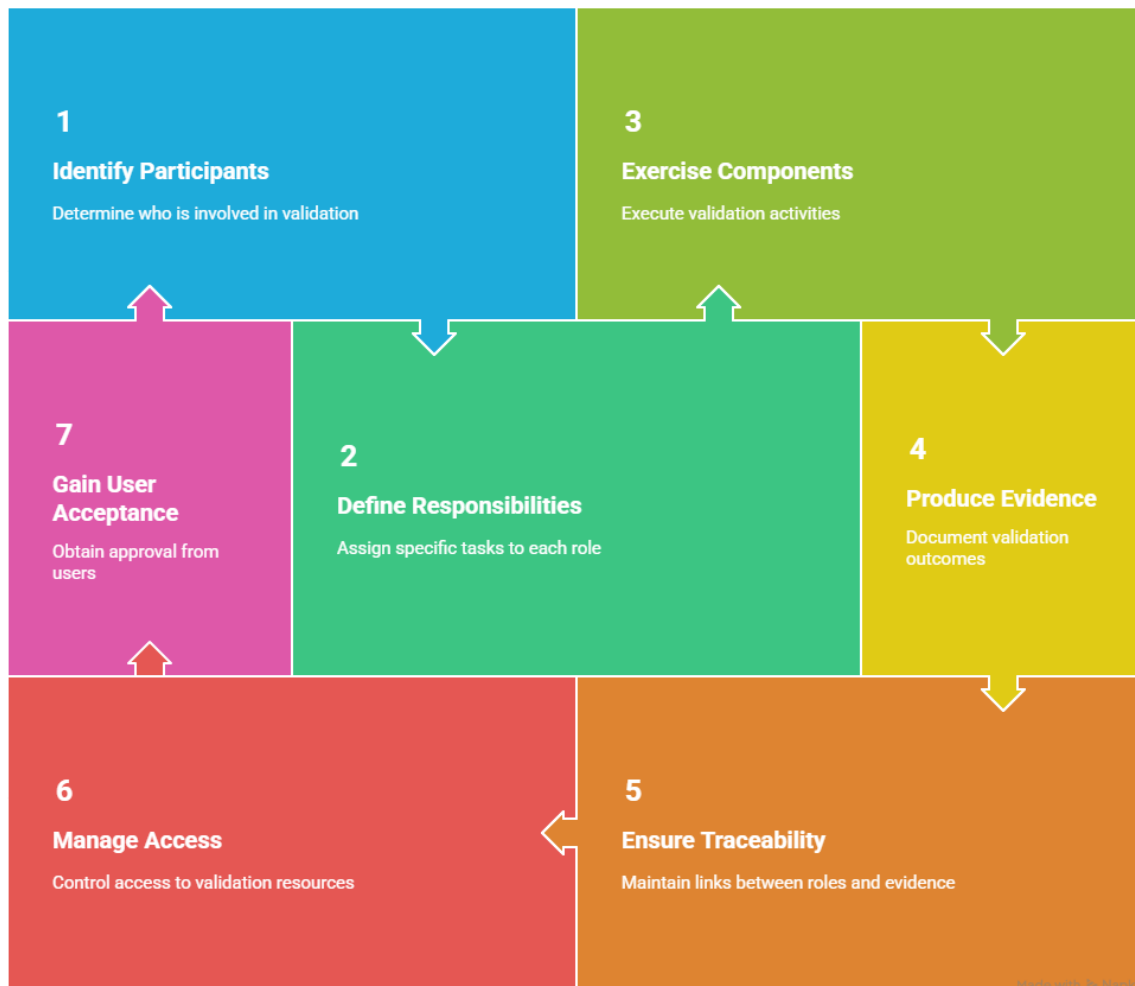


Figure 2 Validation Process Cycle

4.1 User Categories

- **SOC Analysts** — Monitor, triage and investigate alerts; correlate with CTI; initiate/execute playbooks; document timelines and evidence in CICMS. These are primary operators of NG-SIEM/NG-SOAR/BIPS and heavy CICMS users.
- **CISOs and Security Managers** — Define policy, risk appetite and acceptance criteria; approve response plans; consume dashboards and reports for governance and NIS2 compliance. (Aligned with ECSF role taxonomy used in WP5).
- **IT Administrators** — Maintain platforms, identities and integrations (Kubernetes, APIs, RBAC/SSO); support log/telemetry onboarding needed for pilots and validation.
- **Penetration Testers** — Execute semi-automated tests to identify exploitable weaknesses; provide findings as validation evidence and to exercise DRME/NG-SOAR workflows.
- **Incident Responders** — Coordinate end-to-end incidents; lead containment/eradication/recovery; ensure CICMS case quality and audit trails; validate MTTA/MTTR improvements.
- **Trainers and Trainees** — Design and deliver curricula (Open edX) and hands-on scenarios (CyberRangeCZ); collect learning analytics to demonstrate skills uplift aligned to ECSF.

Note: D2.3 identifies and describes these roles (e.g., CISO, Incident Responder, CTI Specialist, Risk Manager, Pen-Tester, System Administrator/Operator) as the basis for requirements and pilot participation.

4.2 Supporting Users

Who they are: Organisations and roles that **enable** validation but are **not** the primary operational SOC users.

- **CYNET/FUNITEC (facilitators).** Provide and operate training/exercise platforms; design/import scenarios; export analytics; help run UAT. *They do not grade academic work nor act as teachers for end-users; their role is facilitation and evidence provision.*
- **European CSIRTs/ENISA/regulators (observers/advisers).** Provide good practice input on interoperability/compliance; may participate in table-tops or surveys; do **not** make pilot acceptance decisions.
- **Customer/user groups where relevant.** Provide contextual feedback (e.g., business units or operators) to assess usability and workflow impact.

What they provide / What they do not.

- *Provide:* platform readiness evidence, scenario definitions, analytics exports, UAT instruments and minutes (aggregate).
- *Do not provide:* final acceptance decisions (owned by Pilot Owners/CISOs) nor operational staffing of SOC shifts.

4.3 User Mapping Table

Table 2 User Mapping Table

Pilot / Partner	User Groups	Roles in Validation	Link to WP2 Requirements
CaixaBank	SOC team, fraud unit	Pilot execution, tool validation	Banking/Finance requirements (D2.3)
CYNET	CSIRT staff, trainers	Training validation, awareness	Academia requirements (D2.3)
ELES/INFO	Operators, OT security teams	Energy pilot execution	Energy requirements (D2.3)
FUNITEC	Trainers, evaluators	User acceptance validation	Cross-pilot

How is this table used. It links *who* participates to *what they validate* and *how proof is gathered*: roles and sectors from **D2.3**; components and interfaces from **D2.4** (NG-SIEM↔CICMS, NG-SOAR↔CICMS, CTI); training/user-skills evidence from **D5.1**; and overall WP6 framing from **D6.1**.

5 Validation Phases and Link to WP6 Deliverables

Overview. Validation is organised as a phased pipeline across WP6 deliverables. **D6.1** establishes the method and users; **D6.2/D6.3** integrates and tests components against the architecture; **D6.4** prepares and executes pilots and gathers success indicators; **D6.5** concludes user acceptance and final validation. Traceability is maintained to **D2.3** (requirements, MoSCoW, role mapping) and **D2.4** (architecture, interfaces), under the quality gates and KPI cadence defined in **D1.1 (QMP)**.

D6.1 — Validation methodology and users identification (foundation)

Scope & purpose. Define a standards-based, multi-level validation approach (component → system → pilot) and identify the user groups and stakeholders who will participate.

Key inputs.

- **D2.3** user & system requirements (templates, MoSCoW, pilot linkage, role taxonomy).
- **D2.4** architecture & *Interfaces Model* (what to validate and how components interact).
- **D1.1 QMP** (release policy, repositories, KPI cadence, risk handling).

Activities. Define criteria/metrics and instruments (questionnaires, logs, playbook records, audit trails); map users to pilots and components; align with NIS2/ENISA good practice and ECSF; plan evidence capture.

Outputs. Validation plan (levels, roles, instruments), users catalogue and pilot mapping, evidence model, linkage to WP7 KPIs.

Acceptance gate. WP6/WPL approval that methodology, roles and evidence model are in place to proceed to integration & testing (D6.2/D6.3).

D6.2 / D6.3 — Integration & Testing (from components to integrated platform)

Scope & purpose. Build and verify the **integrated NG-SOC platform** by exercising component interfaces and data flows prior to pilots (BIPS, NG-SIEM, NG-SOAR, CICMS, CTI-SS, DRME, Pen-Test, CyberRangeCZ, Open edX).

Key inputs.

- D6.1 plan & user mappings (what to test and who observes/accepts).
- D2.4 *Interfaces Model* and sequence diagrams (BIPS→SIEM→CICMS→SOAR; CTI via STIX/TAXII; CACAO playbooks).
- D2.3 requirements to derive test cases and coverage.
- QMP release & repo rules (stable release after integration tests; binaries & docs in Nexus; issue tracking).

Activities.

- Component-level tests (APIs, schemas, security controls) and **system-level** end-to-end runs in a pilot-like environment.
- Interoperability checks: STIX/TAXII CTI exchange, CACAO playbook import/export/execution, RBAC/SSO flows.
- Performance checks: ingest/processing latency, throughput and stability under representative loads.
- Defect management and re-tests via the shared ticketing system.

Outputs.

- Tested integration build(s) promoted to “stable”, with user/technical documentation.
- Requirements coverage report with cross-references to D2.3 IDs.

Acceptance gates & KPIs (as defined in the project QMP/D1.1 and the WP7 KPI catalogue)

- **KPI-6.1 — Integrated system success rate.** ≥80% one month before delivery and **100% at delivery**; **integration issue resolution time ≤15 days.** *Project-level gate used at D6.2/D6.3 readiness and confirmed at D6.5.*
- **KPI-6.2 — System requirements coverage.** ≥90% of D2.3 requirement IDs covered by tests/evidence; any deviations **documented and justified.** *Project-level gate checked at D6.3 and consolidated at D6.5.*

Source/provenance. Thresholds above are **fixed at the project level** and come from:

- the **Quality Management Plan (QMP, D1.1)** — release/issue rules, integration success, and resolution times; and
- the **WP7 KPI catalogue (e.g., D7.1/D7.2)** — definitions for “integrated-system success”, “requirements coverage”, and “user satisfaction”.

Evidence. Test logs; interface conformance reports; playbook run logs; CTI exchange traces; issue-tracker closure reports; release notes and binaries.

Note. These gates are **not negotiated at the pilot level**. Pilots may add **pilot-specific targets** (e.g., MTTR reduction, CTI enrichment) elsewhere, but KPI-6.1 and KPI-6.2 remain as project acceptance thresholds.

D6.4 — Pilots preparation, execution, and success indicators (sector validation)

Scope & purpose. Prepare environments and data, execute sector scenarios (Banking, Educational/Training, Energy), and capture **success indicators** across technical and user dimensions.

Key inputs.

- Stable integrated platform from D6.2/D6.3; pilot scenarios and roles from D6.1; D2.3 requirements relevant to each pilot; D2.4 interfaces.

Activities.

- Pilot readiness: access control, datasets, runbooks, risk/ethics checks; rehearsal in controlled testbeds if needed.
- Pilot execution: end-to-end incidents with **CICMS** timelines and **NG-SOAR** CACAO playbooks; CTI enrichment via STIX/TAXII; optional training-centred runs (Open edX + CyberRangeCZ).
- UAT cycles with analysts/responders/managers; SUS/UAT questionnaires; workshops and interviews.

Outputs.

Per-pilot success-indicator pack (metrics, evidence, lessons learned) and cross-pilot synthesis.

Acceptance gates & KPIs (QMP).

- **KPI-6.3** ≥80% of users rate platform performance “satisfactory” or better; **KPI-6.4** MTTR reduction >15% for simulated multi-vector attacks (or pilot baseline); participation metrics per pilot (**KPI-6.6**).

Evidence. CICMS audit trails (cases, tasks, artefacts), NG-SOAR playbook executions, NG-SIEM alert streams, CTI exchange logs, Open edX/CyberRange analytics, where applicable.

D6.5 — Pilots users' acceptance and validation (final acceptance)

Scope & purpose. Consolidate acceptance results, verify that pilot-level thresholds are met, close deviations, and produce the final validation statement and recommendations.

Key inputs. D6.4 success-indicator packs; unresolved issues from D6.2/D6.3; D2.3 requirement coverage report; QMP KPIs.

Activities.

- Acceptance review boards per pilot (pilot owners, component leads, WP6/WPL); verify thresholds and sign-off criteria.
- Root-cause and corrective actions for any unmet KPIs; update of playbooks, interfaces or training as needed.

Outputs.

- **Final Validation Report:** requirements coverage $\geq 90\%$; KPI outcomes; UAT results; compliance & ethics evidence; lessons learned and exploitation inputs (link to WP7).

Acceptance gates & KPIs (close-out).

- Integrated system success = **100%** at delivery (KPI-6.1); coverage $\geq 90\%$ (KPI-6.2); user satisfaction $\geq 80\%$ (KPI-6.3).

Evidence. Signed acceptance minutes, consolidated dashboards, traceability matrix (D2.3 IDs → tests → pilot evidence), release documentation.

How the phases connect (traceability and governance)

- **Traceability chain:** D2.3 requirement IDs (with MoSCoW and role/pilot tags) → D6.2/D6.3 test cases and interface checks → D6.4 pilot scenarios & UAT → D6.5 acceptance decision.
- **Architecture anchor:** D2.4's *Interfaces Model* and sequence diagram guide end-to-end tests and pilot data flows (BIPS→SIEM→CICMS→SOAR; CTI via STIX/TAXII; CACAO playbooks).
- **Quality gates:** QMP defines release, repository and issue-management rules, and the KPI cadence used as acceptance thresholds.
- **WP7 linkage:** D6.1 and the KPI catalogue ensure that validation metrics roll up into the project-level evaluation and impact framework.

6 Conclusion

This deliverable establishes the **foundation of WP6** by (i) defining a standards-based, multi-level validation methodology (component → system → pilot) and (ii) identifying the users and stakeholders who will participate in pilots and acceptance. It anchors validation to **requirements in D2.3** (with MoSCoW priorities and role/pilot tags) and to the **architecture & Interfaces Model in D2.4**, ensuring every acceptance claim can be traced from requirement → test → pilot evidence.

What this enables now.

- A clear **traceability chain** from D2.3 requirement IDs to D6.2/D6.3 integration tests, to D6.4 pilot scenarios and UAT, and finally to D6.5 acceptance decisions. The D2.3 templates (User/System requirements with Pilot, Use-case, and Role fields) and D2.4 sequence/interaction views are the backbone of this linkage.
- A common **evidence model**: interface conformance reports, CTI exchanges (STIX/TAXII), CACAO playbook execution logs, CICMS timelines/audit trails, performance traces from NG-SIEM/BIPS, and learning analytics from Open edX/CyberRangeCZ.

Next steps across WP6.

- **D6.2/D6.3 (Integration & Testing)**: integrate BIPS, NG-SIEM, NG-SOAR, CICMS, CTI-SS, DRME, Pen-Test, CyberRange and Open edX according to D2.4 interfaces; promote only **stable releases** (post-integration tests) to the consortium repository with full user/technical documentation and tracked issues.
- **D6.4 (Pilots: preparation, execution, success indicators)**: run sector scenarios (Banking, Academic/Training, Energy), collect success indicators and UAT evidence with the roles mapped in this deliverable.
- **D6.5 (Users' acceptance & validation)**: consolidate metric results, confirm thresholds, close deviations, and issue the final acceptance statement.

KPI alignment and acceptance thresholds.

Validation outcomes will be continuously checked against the **WP6 KPI set** defined in the project QMP (D1.1), including: **KPI-6.1** integrated-system success (≥80% one month pre-delivery; **=100% at delivery**) and integration issue resolution time (≤15 days); **KPI-6.2** requirements coverage (≥90% with explained deviations); **KPI-6.3** user satisfaction (≥80% "satisfactory" or better); **KPI-6.4** MTTR reduction (>15% for simulated multi-vector attacks); **KPI-6.6** participation metrics. These gates are used at D6.2/D6.3 (readiness), D6.4 (pilot success), and D6.5 (final acceptance).

Governance and quality controls.

Releases, repositories, and issue tracking (e.g., Jira/GitHub/FusionForge) follow D1.1 rules; component tests, integration tests, and pilot usage tests are explicitly scheduled under the QMP so that defects discovered in pilots trace back to requirements and interfaces. KPI monitoring is **bi-annual** at the project level and continuous at the WP6 level during pilots.

Users and ethics.

The user catalogue and mappings in this deliverable define who participates in which pilot, with roles spanning analysts, responders, managers, admins, trainers, and trainees; this supports targeted UAT and training KPIs while embedding GDPR-compliant evidence captured via CICMS audit trails and pilot documentation.

Sustainability and impact.

By building validation around open standards (STIX/TAXII, CACAO) and auditable artefacts (playbooks, case timelines, logs), the project creates **repeatable** assessments aligned with NIS2 and EU good practices. Results and lessons learned feed the **WP7 impact framework** and dissemination/exploitation actions, ensuring that improvements (e.g., playbook tuning, interface hardening, role-based training) are measurable and transferable.

Bottom line.

This D6.1 gives NG-SOC a **practical, testable path** from **design (D2.3/D2.4)** to **pilot acceptance (D6.5)** with clear responsibilities, instruments, and KPIs. Executing D6.2–D6.5 under these controls will yield **evidence-driven acceptance** and provide a robust basis for exploitation and scale-out across EU SOC communities.

Note

Provenance of metrics and numerical targets

- **Project acceptance gates.** **KPI-6.1** (integrated-system success $\geq 80\%$ one month before delivery, $=100\%$ at delivery; integration-issue resolution ≤ 15 days) and **KPI-6.2** (requirements coverage $\geq 90\%$ with documented deviations) are **fixed at project level** by the **Quality Management Plan (D1.1/QMP)** and the **WP7 KPI catalogue**. They are checked at D6.2/D6.3 (readiness) and confirmed at D6.5 (final acceptance).
- **Pilot targets.** All other figures in this deliverable are **example targets** (guidance). Each pilot **confirms or adjusts** its **pilot-agreed target** during **D6.4 readiness** (approval chain: *Component Lead* → *Pilot Owner* → *WP6 Lead*), and we record the decision in the requirements→test→evidence traceability.
- **Rationale.** Example targets are derived from (i) **D2.4 architecture & interfaces** (STIX/TAXII/CACAO interoperability and near-real-time operation), (ii) **WP7 impact objectives** (e.g., MTTR reduction), (iii) good practice for **Open edX/KYPO/ECSF** in training, and (iv) alert-quality control for analytics (precision/recall/FPR to limit alert fatigue).

	 Project Acceptance Gates	 Pilot Targets
Source	Quality Management Plan (D1.1/QMP) and WP7 KPI catalogue	Pilot agreement
Timing of Definition	Fixed at project level	Confirmed/adjusted during D6.4 readiness
Approval Chain	N/A	Component Lead → Pilot Owner → WP6 Lead
Rationale	N/A	D2.4, WP7 impact objectives, good practice, alert-quality control
Examples	KPI-6.1, KPI-6.2	MTTR reduction, STIX/TAXII/CACAO interoperability

Figure 3 Provenance of Metrics and Targets

REFERENCES

- [1] NG-SOC D2.1 – Detailed use-cases and scenarios for the pilots.
- [2] NG-SOC D2.2 – System modelling, sectorial risk analysis and cascading risks.
- [3] NG-SOC D2.3 – User and system requirements for secure digital infrastructures.
- [4] NG-SOC D2.4 – NG-SOC Architecture.
- [5] NG-SOC Grant Agreement Annex 1 – Description of the Action (Part A & B).
- [6] NG-SOC D7.2 – Business Plan (Evaluation Protocol and KPIs).
- [7] European Parliament & Council of the European Union. (2022, December 14). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152.
- [8] ENISA. (2022). European Cybersecurity Skills Framework (ECSF): Role profiles. European Union Agency for Cybersecurity.
- [9] ENISA. (2022). European Cybersecurity Skills Framework (ECSF): User manual. European Union Agency for Cybersecurity.
- [10] ECSO. (2022). European Cybersecurity Education & Professional Training: Minimum Reference Curriculum. European Cyber Security Organisation.
- [11] OASIS Open. (2024). CACAO Security Playbooks v2.0. OASIS Standard.
- [12] Regulation (EU) 2016/679 (GDPR) – Articles 5, 25, 32.
- [13] Directive (EU) 2022/2555 (NIS2) – Article 21 (Cybersecurity risk-management measures). EUR-Lex.

APPENDIX

Table 3 Map UR to Validation

Req ID	Requirement Name	Requirement Description	NG-SOC Components	Priority	Pilots	Use Case	Validation Scenario	Validation Method	Validation Proof Type (data sample/screenshot/video, etc.)	User Group
UReq-01	Automated Anomaly detection	The system must provide automated detection of anomalies in network traffic data with the ability to learn from past incidents (for example via the use of ML or AI methods)	BIPS, NG-SIEM	MUST	P1 CXB, P3 ELES/INFO	1b, 3b	Inject synthetic anomalies into NG-SIEM and verify automated detection and alerting. (in CaixaBank)	BIPS model report (model ID/version, confusion matrix, precision/recall/FPR, detection threshold); NG-SIEM alert/correlation artefacts (rule ID, alert IDs, MITRE ATT&CK mapping, timestamps).	Screenshot, sample data	Cybersecurity implementer, incident responder
UReq-02	Cross Organizational Incident Handling	Teams, internal or external to the organization, handling incidents must have a common interface to interact & coordinate - for example across different SOC's	CICMS, CTI	MUST	P1 CXB, P2 CYNET, P3 ELES/INFO	1b, 2c, 2d, 3b	Trigger incidents across multiple organizations and validate information exchange via CICMS/CTI-SS. (In CaixaBank)	CTI-SS/MISP event log (TLP, sharing group, STIX/TAXII collection, bundle UUIDs) evidencing cross-organisation exchange; CICMS case timeline (case ID, participants per organisation, task list, SLA timestamps); NG-SIEM alert entries linked to the case (severity ≥ policy threshold);	Screenshot, sample, JSON data	Cyber Incident Responder,

URe q-03	Community Threat Intelligence	Teams, internal to the organization, handling incidents must be able to consume threat intelligence from the community	CICMS, CTI	MUST	P2 CYNET, P3 ELES/INF O	2c, 2d, 3b	Provide CTI data using STIX/TAXII feeds and confirm correct ingestion, normalization, and sharing through CTI-SS. (In CYNET)	CTI-SS ingestion report (source feed, MISP events count; rejected records with reasons); TAXII pull/push log (collection ID, synchronisation latency, auth/audit entries);	Screenshot, data sample	Cyber Incident Responder, Cyber Threat Intelligent Specialist,
URe q-04	Quick Countermeasure Deployment	Teams handling incidents must have the ability to design and deploy countermeasures (playbooks) easily and quickly (via a low code approach)	NG-SOAR	MUST	P1 CXB, P2 CYNET, P3 ELES/INF O	1a, 2d, 3a	An analyst uses the CACAO web app to build a countermeasure playbook using the low-code editor (drag-and-drop). The playbook is exported as CACAO JSON, loaded into the CACAO Executing engine, and can be executed in the NG-SOC environment. (In CaixaBank)	The CACAO editor is successfully used to create a playbook in a simple drag-and-drop manner. Further, the playbook can be exported/stored for further use.	Screenshot, data sample - CACAO JSON of created playbook	Cyber Threat Intelligence Specialist, Cyber Incident Responder
URe q-05	System Recommended Playbooks	Teams handling incidents could have a set of relevant playbooks filtered and made available as a recommendation	CICMS, NG-SIEM, NG-SOAR	COULD	P1 CXB, P2 CYNET, P3 ELES/INF O	1b, 2c, 2d, 3b	Present diverse incident scenarios triggering an alert in NG-SIEM and check if NG-SOAR recommends appropriate	NG-SIEM collects information about alerts and forwards it to the NG-SOAR recommendation engine, which provides relevant playbooks, if any exist.	Screenshots, Data samples (Enriched alert and list of relevant playbooks)	Cyber Incident Responder,

		on by the system					playbooks aligned with the presented threat. (In CaixaBank)			
URe q-06	Incident Intelligence Sharing	Identified incidents could be classified and annotated to contribute to shared intelligence feeds	CTI, CICMS, NG-SIEM	COULD	P1 CXB, P2 CYNET, P3 ELES/INFO	1a, 1b, 1c, 2c, 2d, 3a, 3b	Share incident intelligence from CICMS through CTI-SS using STIX 2.x over TAXII 2.x, and ingest community CTI to enrich NG-SIEM alerts (pilots P1/P2/P3 as applicable).	Outbound: from a CICMS case, export IoCs as STIX to CTI-SS; publish to a MISP; record ACK. Inbound: configure CTI-SS as MISP sync; pull STIX bundle; verify NG-SIEM enrichment (alertId, fields added, TLP/sighting) and CICMS reference to the CTI object.	Screenshot, Data sample, JSON	Cyber Threat Intelligence Specialist
URe q-07	Standardization of Intelligence Feed	Threat intelligence feeds created from the platform should use existing standards	CTI	SHOULD	P1 CXB, P2 CYNET, P3 ELES/INFO	1a, 1b, 2c, 3b	The NG-SOC platform generates a threat intelligence item (e.g., IOC enrichment result or incident summary) and exports it using a standardized MISP object through the MISP platform. (In ELES/INFO)	Validate the generated MISP object for compliance with the specification.	Screenshot, Data sample	Cyber Threat Intelligence Specialist, Cyber Incident Responder
URe q-08	Automate Parsing of known Threats	Threats and threat actors could be automatically parsed from	CTI	COULD	P1 CXB, P2 CYNET	1b, 2c	Convert an open-source threat report into a STIX 2.1 bundle,	Manual validation of the produced STIX bundle derived from the threat report.	Document: A sample threat report in PDF, Data sample: STIX bundle	Cyber Incident Responder,

D1.2 Data Management Plan

		public reports (for example published by ENISA) and converted to an open standard (for example STIX)					ingest it into CTI-SS, and make the derived indicators/playbook available to NG-SIEM/NG-SOAR.			
UReq-09	Infrastructure Risk Estimation	The level of exposure in terms of a risk assessment must be able to be estimated from a description of the infrastructure deployed in an organization	DRME	MUST	P1 CXB, P3 ELES/INFO	1b, 1c, 3a, 3b	Validate user ability to use DRME to create assets and their relationships in the tool, in order to calculate risk	DRME (RMT/DRAS) risk snapshot per asset and in total	Screenshot/Video	Cybersecurity Auditor, Cybersecurity Risk Manager
UReq-10	Attack Surface Mapping	The level of exposure in terms of attack surface should be able to be estimated for an organization up to the level of known attack vectors	Pen Testing, NG-SIEM	SHOULD	P1 CXB	1a	Perform recon/scanning (e.g., Nmap/OpenVAS) to enumerate hosts/services/CVEs and register assets and critical findings; align scope with CXB pilot.	Agree Rules of Engagement and target range → run scans → export host/service inventory + vuln report (CVSS) → register any new assets in CMDB/NG-SIEM → open CICMS cases for critical findings and link remediation tickets.	JSON	Penetration Tester, Cybersecurity Auditor
UReq-11	Vulnerability-Driven Risk Updates	Risk levels estimated from known vulnerabilities in the infrastructure of an	DRME, Pen Testing	COULD	P1 CXB	1a, 1b, 1c	Use DRME to estimate the risk level of the infrastructure, then perform penetration	DRME (RMT/DRAS) risk snapshot per asset before and after the penetration testing	Screenshot/Video	Penetration Tester, Cybersecurity Auditor

		organization could be updated from the findings of estimating the attack surface					testing and feed the results to DRME for recalculating the risk level based on exploitable vulnerabilities found during pen testing.			
URe q-12	Modern Cybersecurity Training	The skills of the cybersecurity teams of an organization should be able to be brought up to the current standards via the provision of a training toolset comprising educational material and hands-on exercises	OpenEdX	SHOULD	P1 CXB, P2 CYNET	1a, 1c, 2a, 2b	Deliver Open edX courses and CyberRange exercises to upskill teams (CXB and CYNET), measuring completion, performance and response quality.	Publish/update course content → run a cohort → export edX analytics (completion %, scores, time-on-task) → run CyberRange scenario attempts with scoring/telemetry → conduct after-action review and capture UAT feedback.	Screenshot	Cybersecurity Educator
URe q-13	Prioritization of Incident Notification	The system should issue clear notifications once new incidents are detected, prioritizing potential threats based on their perceived severity (this	BIPS, NG-SIEM	SHOULD	P1 CXB, P2 CYNET, P3 ELES/INFO	1b, 2c, 2d, 3b	Deploy community-driven CTI scenarios within cyber range exercises and validate sharing effectiveness. (In CYNET)	NG-SIEM alert notification sample (JSON fields: event ID, timestamp, source host, severity, recommended actions); Prioritisation evidence (policy-based ordering; analyst dashboard view).	Screenshot	Cyber Incident Responder

		estimate may be formed from shared intelligence)								
URe q-14	Automatic Creation of Cases in Case Management System	Incident case must be able to be created both automatically once a new incident is identified by the system as well as by human users	CICMS, NG-SIEM	MUST	P1 CXB	2d	When NG-SIEM identifies an alert that exceeds the threshold, it will automatically create a new case in the incident case management system with relevant information.	NG-SIEM severity policy/trigger proof (rule ID, threshold); CICMS automatic case creation (case ID, time-to-case from alert, auto-filled fields).	Screenshot	Cyber Incident Responder
URe q-15	Targeted Audience Information Sharing	Relevant information (CTI) could be shared with the appropriate audience (other entities and authorities)	CTI	COULD	P1 CXB, P2 CYNET, P3 ELES/INFO	1b, 1c, 2c, 3a	Evaluate incident response workflows in energy grid simulations, ensuring timely coordination through. (In ELES/INFO)	CTI-SS targeted distribution log (audience/constituency, scope, packaging STIX/TAXII, TLP); Receiver acknowledgement/import log with sample delivered artefacts.	Screenshot	Participant
URe q-16	Playbook Management - Storage & Search	A Playbook Knowledge Management System (KMS) for secure storage, searching, and filtering CACAO playbooks, and easily exchangeable to ensure	NG-SOAR	MUST	P1 CXB, P2 CYNET, P3 ELES/INFO	1b, 2d, 3b, 3c	Use cyber range scenarios to validate Playbook KMS functionality by searching, filtering, and retrieving relevant playbooks. (In CYNET)	NG-SOAR KMS record for the playbook (version, owner, last update, signatures); CACAO v2 validator output attached to the current version.	Screenshot	Participant

		effective and consistent incident handling.								
URe q-17	Playbook execution	NG-SOAR must act as an individual and independent tool for automating routine actions across the SOC while it manages and orchestrates the creation and execution of the best available playbooks to, e.g., isolate hosts, block malicious IPs, and suspend compromised accounts, halting the attack's spread	NG-SOAR	MUST	P1 CXB, P2 CYNET, P3 ELES/INF O	1b, 2d, 3b	Measure efficiency at CaixaBank using NG-SOAR Playbooks to automate workflows. (In CaixaBank)	NG-SOAR execution metrics (automation ratio, manual steps count, mean run time); Run log with task outcomes and API calls to external systems.	Screenshot, Metrics	Participant
URe q-18	Provision of the context (data) used for the marking of suspicious events	When events are marked as suspicious, the system should provide contextual information (raw data that triggered the alarm) to enable the screening of	BIPS	SHOULD	P1 CXB, P3 ELES/INF O	1b, 3b	Provide human-readable context for suspicious alerts so analysts can validate/triage them. (In CXB/ELES)	Show BIPS alert details (contributing features/explanation) → retrieve the NG-SIEM raw & correlated events referenced by the alertId → attach both as artefacts to the analyst workflow/case and record the triage	Screenshot	Incident responder

D1.2 Data Management Plan

		incidents by humans						decision with rationale.		
URe q-19	Suspicious activity tracking based on most recent intelligence information	The system must be fed with the most recent intelligence, so that IoCs and other data can be actively used in detection and response (so that the system can recognize the most modern known threats)	CTI, NG-SIEM	MUST	P1 CXB, P3 ELES/INF O	1a, 1b, 1c, 3a, 3b, 3c	Ingestion of CTI and operationalizing the IoC in BIPS/NG-SIEM. (In CaxiaBank)	CTI-SS freshness metrics (age of IoCs, last sync time, number of new indicators); CTI-SS import log (collection ID, objects added) enriches NG-SIEM matches triggered; BIPS detections are correlated with the new indicators (where applicable).	Screenshot	Incident responder
URe q-20	Automatic Risk Calculation Update	The risk assessment must be able to be calculated again once the infrastructure is modified	DRME	MUST	P1 CXB, P3 ELES/INF O	1a, 3a	Update infrastructure information in DRME and recalculate risk to show delta, or run a risk assesment at a later time to showcase new vulnerabilities and exploitation metrics	DRME trigger showing infrastructure change (asset added/modified); New risk snapshot and diff report versus previous baseline.	Screenshot	Risk manager
URe q-21	Automate Infrastructure Identification	The risk assessment could use automated means of parsing the description of	DRME	COULD	P1 CXB, P3 ELES/INF O	1a, 1c, 3a	Identification of infrastructure using OpenVas and nmap	Update DRME Model based on Infrastructure componenets found during network discovery and identification	Screenshot/Video	Cybersecurity Auditor, Cybersecurity Risk Manager

D1.2 Data Management Plan

		the underlying infrastructure								
URe q-22	Intelligence Based Threat Rules	Threat detection rules must be in place based on known intelligence	NG-SIEM	MUST	P3 ELES/INFO	3a, 3b, 3c	Assess the scalability of handling large volumes of CaixaBank alerts. (In CaixaBank)	Rule creation/update in NG-SIEM driven by CTI-SS (rule ID, linked indicator IDs); Effectiveness evidence (false-positive reduction or new detections across a defined period).	Logs/Metrics	Incident responder
URe q-23	Easy Detection Rule Adding	The addition of new detection rules should be possible for humans and technologies (for example via an API)	NG-SIEM	SHOULD	P1 CXB, P2 CYNET, P3 ELES/INFO	1b, 2c, 2d, 3b	Validate CYNET's ability to run large-scale simulations with multiple concurrent CTI (In CYNET)	NG-SIEM UI-based rule addition (screenshots/logs) and NG-SIEM API-based rule injection (request/response); Test event proving the new rule fires (alert ID, timestamp).	Screenshot logs	Cyber Incident Responder
URe q-24	Automated Log Parsing	The system must be able to parse various log formats and map the attributes to categories. It should allow for easy-to-use tuning of the parsing and mapping rules	NG-SIEM	MUST	P1 CXB, P3 ELES/INFO	1b, 3a, 3b, 3c	Check capacity to update risk metrics dynamically during pilot incidents. (In ELES/INFO)	NG-SIEM parsing/mapping unit-tests per log source (field map, target schema); Parsing accuracy/error-rate report and example of tuned rule.	Screenshot	Incident responder
URe q-25	Efficient & Fast Searching	The system must have a user friendly and fast searching and filtering engine	NG-SIEM	MUST	P3 ELES/INFO	3a, 3b, 3c	Demonstrate fast, relevant search over NG-SIEM indices for common SOC	Define a set of representative analyst queries → measure p95 query latency and result counts on	Screenshot	Incident responder

D1.2 Data Management Plan

		to support further investigation of specific events					investigations (In ELES).	production-like data → verify relevance (filters/full-text/dynamic queries) with an analyst review → capture screenshots/exports and KPI summary.		
URe q-26	Reusable Playbooks	Playbooks developed within the system must be able to be shared and reused	NG-SOAR	MUST	P1 CXB, P3 ELES/INF O	1a, 1c, 3b, 3c	NG-SOAR notification playbook to be reused with different alerts and/or use cases. (In CaixaBank)	NG-SOAR evidence of re-use: prior playbook (ID/version) applied to a new incident (ID); Outcome comparison (time saved) and CACAO integrity check.	Screenshot	Cybersecurity auditor, CTI specialist
URe q-27	Playbook management - & Access, history and import/export	The playbooks stored in the system must be editable, manageable, and reusable by users.	NG-SOAR	MUST	P1 CXB, P3 ELES/INF O	1b, 1c, 3b, 3c	Validate NG-SOAR playbook management (RBAC, approvals, version history, export/import) (In CaixaBank)	NG-SOAR edit history (diffs), role-based access; Inspect NG-SOAR KMS playbooks, and execution logs.	Screenshot	Cybersecurity auditor, CISO, incident responder, CTI specialist
URe q-28	Standardized Playbooks Development	Playbooks must adhere to technical open standard (CACAO/JSON)	NG-SOAR	MUST	P1 CXB, P3 ELES/INF O	1b, 1c, 3b, 3c	Author and maintain CACAO v2-compliant playbooks in NG-SOAR (CXB & ELES), validate against the schema.	Create/update a playbook using the consortium template → run CACAO v2 validator (zero schema errors) → record versioning/approvals in SOAR/KMS	Screenshot	Cybersecurity auditor, CISO, incident responder, CTI specialist
URe q-29	Share playbooks within CTI with other constituency	NG-SOAR must be able to share playbooks with other	NG-SOAR, CTI	MUST	P1 CXB, P3 ELES/INF O	1b, 1c, 3b, 3c	Sharing of the developed playbook with the constituency in order to	CTI-SS (MISP) export of the playbook as STIX 2.1 object (object IDs) or TAXII collection push from NG-SOAR;	Screenshot	Cybersecurity auditor, CISO, incident responder,

		constituency through CTI exchange standards (MISP, STIX/TAXII)					automate the workflow and reduce response time. (In ELES/INFO)	Peer ingestion/ACK in CTI platform and integrity hash verification.		CTI specialist
URe q-30	System Optimized Playbook Execution	The playbooks available in the system should be able to be executed by means available by the system and the target infrastructure	NG-SOAR	SHOULD	P1 CXB, P3 ELES/INFO	1b, 3c, 3b, 3c	A CACAO playbook stored in the NG-SOC environment is executed through NG-SOAR using only actions supported by the deployed infrastructure. The entire playbook runs without unsupported steps.	NG-SOAR execution pre-checks (reachability, variable substitution, dry-run); Successful execution in target environment (evidence of applied changes).	Screenshot / data sample	Cybersecurity implementer, incident responder, CTI specialist
URe q-31	Inherited Vulnerability Assessment	The risk analysis should consider not only individual vulnerabilities, but rather investigate cascading effects and vulnerability inheritance phenomena	DRME	SHOULD	P1 CXB, P3 ELES/INFO	1a, 1b, 1c, 3a, 3b	Showcase cascading risks in DRME user interface on CXB and ELES/INFO infrastructure	DRME 'cascading effects' view (asset dependency graph excerpt); Risk impact propagation example across dependent assets.	Screenshot/Video	Cybersecurity Auditor
URe q-32	Accessible Security Documentation	The cybersecurity teams operating the system should	CyberRange CZ, OpenEdX, DRME, NG-SOAR	SHOULD	P1 CXB, P3 ELES/INFO	1a, 1c, 3c	Operators access the NG-SOC documentation portal and view	Verify that manuals or training guides exist, are accessible through the platform, and	Documentation documents	Incident responder, cybersecurity implementer

		have access to documentation or training material on the main functions of the tools available to them					user guides or training material covering key system components (e.g., CTI-SS, NG-SIEM, NG-SOAR). The material clearly explains core functions, workflows, and usage patterns.	cover the required operational features.		r, cybersecurity educator
UReq-33	Friendly and Intuitive User Interface (UI)	The system should feature a user-friendly and intuitive User Interface (UI) that allows users to interact with the system effortlessly.	BIPS, NG-SIEM, CICMS, CTI, NG-SOAR, Pen Testing, OpenEdX, DRME, CyberRange CZ	SHOULD	P1 CXB	1a, 1b, 1c, 3a, 3b, 3c	Validate CaixaBank SOC user experience in handling automated playbooks. (In CaixaBank)	Usability walkthrough (task completion times, error rate) on NG-SIEM UI used by the SOC; Feedback summary (issues found and UX fixes applied).	Questionnaire	Cybersecurity implementer, incident responder, participant
UReq-34	Enhanced Cyber Threat Intelligence Integration for financial attacks	Integrate specialized threat intelligence feeds must provide detailed insights into cyber threats targeting the financial sector, including known actors, tactics, techniques, and procedures	CTI	MUST	P1 CXB	1b	Ingest multiple external and community CTI feeds (MISP/STIX) into CTI-SS and validate enrichment, normalization, and sharing across relevant parties. (In CaixaBank)	Ingestion of sector-specific financial CTI (MISP feeds, feed name, STIX patterns, bundle UUIDs) in CTI-SS;	Screenshot	Cybersecurity implementer, incident responder

		(TTPs) used in attacks like data breaches, ransomware, and ATM skimming.								
UReq-35	Integrate with other SIEMs	The solution must provide connectivity and integration capabilities with other Security Information and Event Management (SIEM) systems to facilitate data exchange and interoperability.	NG-SIEM	SHOULD	P2 CYNET	1b	Integrate NG-SIEM with external SIEM solutions (e.g., existing SOC tools) and validate interoperability, alert forwarding, and correlation in pilot environments. (In ELES/INFO)	SIEM↔SIEM forwarding logs (Syslog/CEF/JSON over TLS) visible in both systems; Correlation IDs alignment and an API exchange test report (auth, endpoints, payload examples).	Screenshot	Cybersecurity implementer, incident responder



NGSOC

Next Generation Security Operations Centres



Co-funded by
the European Union



ECCE
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

This project has received funding from the European Union's Digital Europe Programme (DIGITAL) under grant agreement No 101145874

