

iSOCaaS

INTELLIGENT SOC AS A SERVICE

Issue #2 · Q1 2026

Q1 2026 Progress Update — Core Platform Delivered & AI Enablers Online

Communication & Dissemination Update · Grant Agreement No. 101190388



Co-funded by the European Union — Digital Europe Programme · Grant Agreement No. 101190388 (DIGITAL-ECCC-2024-DEPLOY-CYBER-06)

Project timeline:



Month 16 / 36 · 44%

The first quarter of 2026 marks a significant milestone for iSOCaaS: the delivery of the Core SOC Enablers (D2.3) and the first version of the AI-based intelligent modules (D3.1), bringing the platform's two-tier architecture from specification to operational reality. This issue summarises what has been achieved, what is underway, and what lies ahead.

AT A GLANCE

Q1 2026 by the numbers

7

deliverables completed
since project start
↑ +2 in Q1 (D2.3, D3.1)

5

AI intelligent enablers
(T3.1–T3.5) — first
version

62

pilot users targeted: ≥52
new + ≥10 existing (KPI-
5.2)

5

KPI pillars: Core SOC ·
Intelligent SOC · Info
Exchange · Integration ·
Validation

WORK PACKAGE STATUS

Progress across all WPs — end of Q1 2026

WP	Title	Status
WP1	Project Management	● On track (M1–M36)
WP2	Requirements, Baseline & Architecture	● WP closed (M1–M12) — D2.1, D2.2, D2.3 submitted
WP3	AI-based Situational Awareness & Response	● D3.1 submitted · D3.2 due M22 (WP3: M4–M22)
WP4	Integration & Assessment	● Integration underway (M8–M36) · D4.1 due M26
WP5	Service Delivery	● Starts M18 (May 2026) — pilot recruitment prep.
WP6	Dissemination, Exploitation & Sustainability	● Active (M1–M36) — website, social, events, 3 project synergies

Q1 2026 MILESTONES

Key deliverables & achievements

✓ Delivered WP2 · D2.3

Core SOC Enablers

Full delivery of Swordfish (OSI) and SPA Suite (SPH) platforms, including SIEM, SOAR, Vulnerability Management, and Preparedness modules.

Submitted: 11 March 2026 (M16) · GA due: M12

✓ Delivered WP3 · D3.1

AI-based Enablers — First Version

First operational version of the 5 AI intelligent modules: CTI Discovery (T3.1), UEBA (T3.2), Adversarial ML Monitoring (T3.3), Attack Prediction & Threat Hunting (T3.4) and Response Recommendation (T3.5).

Submitted: 31 March 2026 (M16) · GA due: M12

 **In Progress** WP3 · D3.2

AI-based Enablers — Final Version

Final version in active development: broader CTI source coverage, production-grade UEBA, MITRE ATLAS adversarial mapping, and assessment of KPI-2.1 – KPI-2.5.

GA due: M22 (September 2026)

 **In Progress** WP2 → WP5

Pilot User Recruitment (preparation)

Recruitment strategy (D2.3) in execution, targeting ≥52 new organisations from NIS2 essential/important sectors and ≥10 existing SME users of the NCSA GR-SME-SOC cohort (KPI-5.2).

WP5 start: M18 (May 2026) · D5.1 due M23

DELIVERABLE SPOTLIGHT

D2.3 — Core SOC Enablers in Detail

Submitted on 11 March 2026 (M16), D2.3 brings together the operational tools that form the Baseline SOC Services Tier of the iSOCaaS platform, contributed by OSI and SPH.

Swordfish · OSI Commercial SOC Platform

Lead authors: Pergiouidakis, Stevinas, Voulalas, Logothetis, Kotoulas, Mathiopoulos (OSI)

- › **CyberOps Portal:** Real-time alert, incident and statistics delivery dashboards for pilot customers.
- › **SocStreams:** Alert & incident management with integrated SOAR playbook execution engine.
- › **EMC (Exposure Management Console):** Continuous vulnerability scanning and exposure dashboards.
- › **SRM (Service Request Management):** Ticket management and service request tracking portal.
- › **Microsoft Defender XDR integration:** Defender for Endpoint, Identity, IoT, Office 365, Cloud Apps, Cloud, and Sentinel SIEM — with AI-native ML capabilities and full test scenario documentation.

SPA Suite · SPH **Sphynx Security Platform**

Lead authors: Tsihlaki, Karageorgis (SPH)

- › **EVEREST SIEM:** Custom Security Information & Event Management system tailored for iSOCaaS pilot environments.
- › **Vulnerability Assessment:** Automated scanning and risk-scored reporting module.
- › **Questionnaire-Based Assessment:** Organisational cybersecurity maturity evaluation tool.
- › **CRISES (Custom Risk Detection):** User-defined risk detection model configuration.
- › **CTI Integration:** Threat intelligence feeds integrated into the SPA dashboard.
- › **SOAR module:** Automated response orchestration aligned with CACAO playbook standard.
- › **Preparedness & Training:** Fully functional training scenario builder with progression models and trainee-facing execution interface.

Information Exchange & Pilot Strategy: D2.3 also establishes the information sharing and incident reporting mechanisms aligned with NIS2 obligations, and defines the structured recruitment strategy for onboarding 62 pilot users ahead of the WP5 service delivery phase.

DELIVERABLE SPOTLIGHT

D3.1 — AI-based Enablers: First Version

Submitted on 31 March 2026 (M16), D3.1 presents five intelligent SOC enablers that form the Intelligent SOC Services Tier of the iSOCaaS platform.

Enabler 1 · T3.1 · KPI-2.1 **CTI Discovery & Analytics**

- › Hybrid extraction pipeline combining LLM-based AI extraction, regex pattern matching, and lookup tables against curated threat datasets.

- › Ingestion of further unstructured sources (dark web, Telegram channels, social media, PDF threat reports) in design for the final version.
- › Output: validated STIX 2.1 bundles (SDOs, SCOs, SROs) in JSON — 18+ extractor categories including MITRE ATT&CK, CVEs, malware families, and IoC types.
- › LLM-driven relationship inference maps extracted objects into coherent STIX Relationship Objects (SROs).
- › Supports local LLMs via Ollama and commercial APIs — configurable, offline-capable.

Enabler 2 · T3.2 · KPI-2.2 User & Entity Behaviour Analytics (UEBA)

- › Daily behavioural aggregation from audit logs: processes, file access, system events, login patterns.
- › AutoML Engine with Bayesian hyperparameter optimisation across multiple model families (Random Forest, XGBoost, LightGBM, Isolation Forest, KNN).
- › Sliding 30-day adaptation window — continuous baseline updates aligned with evolving user patterns.
- › Health monitoring with drift detection across numerical, categorical, and target distributions.

Enabler 3 · T3.3 · KPI-2.3 Adversarial ML Monitoring & Mitigation

- › Human-in-the-loop feedback cycle: SOC analysts validate anomaly alerts before data is incorporated into model retraining.
- › Selective update strategy prevents model poisoning by excluding unvalidated or confirmed-malicious behavioural instances from training windows.
- › Full traceability logging of anomaly scores, analyst decisions, and model update actions.

Enabler 4 · T3.4 · KPI-2.4 Attack Prediction & Threat Hunting

- › Threat Hunting Orchestration solution integrated with SocStreams Hunting Workbench.
- › AI Fuzzy Correlation Agent for automated hunt lead generation.
- › Workbench features: hunt definitions, scheduled hunts, hunt lead management — all operational and documented.
- › Semi-supervised ML for attack hypothesis generation and proactive threat identification — in design for the final version.

Enabler 5 · T3.5 · KPI-2.5**Proactive & Reactive Response Recommendation (SPHYNX SOAR)**

- › Full CACAO-compliant playbook lifecycle: design, import/export, execution, and real-time monitoring dashboard.
- › No-code graphical playbook editor for SOC analysts.
- › AI-based CACAO Playbook Recommender (semantic similarity matching of playbooks to incident types) — in design for the final version.
- › Multi-instance CACAO Engine for load balancing and operational isolation.

WHAT'S NEXT**Looking ahead to Q2 2026**

- › **D3.2 — AI Enablers: Final Version (GA due M22, Sep 2026)** — Production-ready AI modules with broader CTI source coverage, MITRE ATLAS adversarial coverage, full KPI assessments, and integration readiness.
- › **WP4 Integration (M8–M36)** — End-to-end integration of Baseline and Intelligent SOC tiers with cross-border information exchange backbone; D4.1 due M26 (Jan 2027).
- › **WP5 kick-off (M18, May 2026)** — Finalisation of recruitment for the ≥62-entity pilot cohort (≥52 NIS2 essential/important sector organisations + ≥10 NCSA GR-SME-SOC users); D5.1 due M23 (October 2026).

- › **Dissemination & Events** — iSOCaaS will be presented at Infocom Security 2026 (April), ENCORES 2026 and AI WEEK 2026 (May), with a dedicated iSOCaaS workshop at the end of May. Follow our channels for announcements.

STAY CONNECTED

Follow iSOCaaS

Keep up with project news, events, and publications across all platforms:

isocaas.eu[in LinkedIn](#)[X @iSOCaaS_eu](#)[f Facebook](#)[▶ YouTube](#)

SPH · OSI · KUA · INS · CS · HMOD · NCSA · NSQ

Co-funded by the European Union under the Digital Europe Programme,
Grant Agreement No. 101190388.

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 Competence Centre (ECCC).

Neither the European Union nor the granting authority can be held responsible for them.

isocaas.eu · contact@isocaas.eu