

iSOCaaS

INTELLIGENT SOC AS A SERVICE

Issue #3 · Q2 2026

Q2 2026 Progress Update —
AI Modules Finalised & Pilot Deployment Begins

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 19 / 36 · 53%

Q2 2026 has been the most intensive quarter yet for iSOCaaS. The platform has crossed a major threshold: the AI-based intelligent enablers are in their final-version stage (D3.2, due M22), end-to-end system integration is actively underway in WP4, and WP5 Service Delivery started in M18 (May 2026), with the 10 GR-SME-SOC pilot users already on iSOCaaS and preparation for onboarding the new pilot users underway. With over half the project's timeline now elapsed, iSOCaaS is moving from design and development into operational validation.

AT A GLANCE

Q2 2026 by the numbers

7	5	62	4
deliverables completed since project start → next: D3.2 due M22	KPI pillars under active measurement	pilot users targeted (≥52 new + ≥10 existing, KPI-	validation levels: sectorial · national ·

5.2)
↑ 10 on iSOCaaS · 52
new in preparation

cross-border · EU (KPI-
5.3)

WORK PACKAGE STATUS

Progress across all WPs — end of Q2 2026

WP	Title	Status
WP1	Project Management	● On track · RP1 (M1–M18) reporting
WP2	Requirements, Baseline & Architecture	● WP closed (M1–M12) — D2.1, D2.2, D2.3 submitted
WP3	AI-based Situational Awareness & Response	● D3.2 in finalisation — due M22 (WP3: M4–M22)
WP4	Integration & Assessment	● End-to-end integration in progress (M8–M36)
WP5	Service Delivery	● Started M18 — 10 GR-SME-SOC users on iSOCaaS · new-user onboarding prep. · D5.1 due M23
WP6	Dissemination, Exploitation & Sustainability	● Active (M1–M36) — 4 of 10 D&C KPIs achieved

Q2 2026 MILESTONES

Key deliverables & achievements

🕒 Finalisation WP3 · D3.2

AI-based Enablers — Final Version

✓ Completed WP2 · T2.4 · MS6

GR-SME-SOC Users on iSOCaaS

The 10 existing SME users of the NCSA GR-SME-SOC were migrated to iSOCaaS under

Final versions of the AI modules: end-to-end CTI pipeline into OpenCTI, AI-system vulnerability assessment, final UEBA architecture and assessment of KPI-2.1 – KPI-2.5.

GA due: M22 (September 2026)

T2.4, completing the service consumers' recruitment part of MS6. They receive an extension of their SOC services within iSOCaaS (KPI-5.1).

10 pilot users onboarded by M18 (May 2026)

 In Progress WP4

End-to-End System Integration

Integration of Baseline and Intelligent SOC tiers, ATHENA cross-border SOC backbone, and national authority interfaces (NCSA, HMOD/CERT).

WP4 runs M8–M36 · D4.1 due M26 (Jan 2027)

 Preparation WP5

New Pilot Users — Recruitment

Preparation for onboarding ≥52 new users from NIS2 essential and important sectors: draft service agreements, SLAs and the onboarding procedure, together with the cyber insurance plans (KPI-5.5).

WP5: M18–M35 · first participation agreements July 2026 (M20)

DELIVERABLE SPOTLIGHT

D3.2 — AI-based Enablers: Final Version (preview)

D3.2 (due M22, September 2026) will close WP3, documenting the transition of all five AI-intelligent enablers (T3.1–T3.5) from first-version implementation to production-grade deployment. Highlights of the work completed so far:

T3.1 · KPI-2.1 CTI Discovery & Analytics

- › **End-to-end pipeline:** crawling, hybrid pattern / lookup / LLM extraction and STIX 2.1 bundle generation, validated on a live public source through to ingestion into OpenCTI.
- › Final CTI pipeline architecture with full integration readiness for Swordfish and SPA Suite platforms.
- › STIX 2.1 relationship inference refined and validated against production threat report corpora.

- › **KPI-2.1** — delivery of the final LLM-based CTI discovery solution, with STIX 2.1 output.

T3.2 · KPI-2.2 User & Entity Behaviour Analytics

- › Final UEBA architecture with middleware integration for production scalability across pilot environments.
- › Model, dataset and metadata management handled natively within the SPHYNX platform, with automated retraining and model-health monitoring.
- › Entity resolution module added: deduplication and linking of users/entities across multi-source log ingestion.
- › Full testing and validation completed across representative behavioural datasets.
- › **KPI-2.2** — delivery of the final AutoML-based UEBA solution, validated on a public dataset and on production telemetry.

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

- › **MITRE ATLAS mapping:** All WP3 AI components mapped against the ATLAS adversarial ML threat framework — coverage of model evasion, poisoning, and extraction attacks.
- › **OWASP ML Security Top 10 alignment** documented for all modules.
- › Adversarial monitoring delivered within the UEBA subsystem, complemented by AI supply-chain vulnerability assessment through ML-BOMs.
- › Data-poisoning and model-drift detection: automated alerts to SOC analysts when baseline integrity is threatened.
- › **KPI-2.3** — identification of ≥5 vulnerabilities of AI systems, mapped to MITRE ATLAS and OWASP.

T3.5 · KPI-2.5 Proactive & Reactive Response Recommendation

- › CACAO playbook library extended to 83 playbook templates in the final version, above the ≥50-playbook target (KPI-1.2).
- › AI Playbook Recommender validated in a laboratory environment, drawing on five threat-intelligence sources (KPI-2.5).
- › Interfaces with the other enablers and the Core SOC tier handed over to WP4 integration (T4.1).

Towards WP3 completion (M22): With the submission of D3.2, WP3 will deliver a production-ready, AI-augmented Intelligent SOC Services Tier that extends the Baseline SOC with beyond-state-of-the-art capabilities, with all 5 enablers integration-ready for WP4.

PILOT DEPLOYMENT — WP5

Pilot programme: 10 users on iSOCaaS, 52 new users in preparation

WP5 Service Delivery started in M18 (May 2026) and runs until M35. The ≥62-user pilot programme (KPI-5.2) is built on two groups. The 10 existing users of the NCSA GR-SME-SOC form the pilot user base already migrated to iSOCaaS under T2.4. For the ≥52 new users, Q2 focused on preparation — draft service agreements, SLAs and the onboarding procedure — with the first participation agreements signed in July 2026 (M20). National-level validation is provided by the national authorities of the consortium:

Cohort	Entities	Status	Coverage
Existing users — SME Cohort (NCSA GR-SME-SOC)	10	● Migrated to iSOCaaS (T2.4 · MS6)	
New users — Essential & Important Sectors	≥52	● Preparation & recruitment (agreements, SLAs, onboarding)	
National-level validation (NCSA / HMOD) — not counted in the 62	2	● Engaged (KPI-5.4)	

Cyber Insurance Integration: The cybersecurity insurance scheme — a unique differentiator of iSOCaaS — is being prepared in parallel with pilot onboarding. Consortium partners KUA and Insuretics are coordinating 12-month insurance coverage tied to the iSOCaaS service level, targeting ≥62 insurance plans for pilot participants (KPI-5.5).

PERFORMANCE INDICATORS

KPI status — mid-project overview

iSOCaaS tracks its KPIs across 5 pillars (Core SOC Services Tier · Intelligent SOC Services Tier · Information Exchange & Collaboration · System Integration & Deployment · Validation & Global View). Status of key indicators at the close of Q2 2026 (M19):

Pillar	Key KPI	Target	Status
Core SOC Services	KPI-1.1 Situational awareness capacity	≥50 CTI sources integrated	 In progress
Core SOC Services	KPI-1.2 Incident response capacity	≥50 CACAO playbooks	 83 templates in D3.2 (due M22)
Intelligent SOC	KPI-2.1 LLM-based CTI discovery	Delivery of the LLM-based CTI discovery solution (STIX 2.1)	 Final version in D3.2 (due M22)
Intelligent SOC	KPI-2.2 AutoML-based UEBA	Delivery of the AutoML-based UEBA solution	 Final version in D3.2 (due M22)
Intelligent SOC	KPI-2.3 Adversarial ML monitoring	≥5 vulnerabilities of AI systems identified (ATLAS + OWASP)	 Reported in D3.2 (due M22)
Integration & Deployment	KPI-4.2 Pilot deployment scale	≥62 service instances deployed	 10 of 62 (GR-SME-SOC users)
Validation	KPI-5.1 Service delivery duration	≥12 months continuous service	→ Running for the 10 migrated users

Pillar	Key KPI	Target	Status
Validation	KPI-5.2 Pilot user coverage	≥62 users (≥52 new + ≥10 existing)	 10 of 62 · new users in preparation
Validation	KPI-5.3 Multi-level validation	Sectorial + national + cross-border (ATHENA) + EU level	 Cross-border integration in WP4
Validation	KPI-5.4 National authority validation	NCSA + HMOD engagement	✓ Active
Validation	KPI-5.5 Cyber insurance integration	≥62 insurance plans activated	 Scheme design (KUA/INS)

Impact KPIs (iKPIs) — e.g. increases in processed CTI volume, early-warning and incident-response capacity — are measured at the end of the project.

DISSEMINATION — WP6

Events, publications & outreach

Q2 2026 was the busiest dissemination quarter so far, with consortium partners presenting iSOCaaS at national and European cybersecurity events and publishing new research results. Earlier, the paper “Intelligent Security Operation Centre Services for Critical National Infrastructure” was presented at IEEE CNS 2025 (Avignon, September 2025).

- Apr 2026

Infocom Security 2026 — iSOCaaS presented by NSQ at Infocom Security 2026.
- May 2026

ENCORES 2026 (Delft) — OSI presented its AI capabilities and AI Code of Ethics, showing how trustworthy AI is applied in iSOCaaS.
- 19–21 May 2026

AI WEEK 2026 (Milan) — iSOCaaS participation by NSQ.
- 28 May 2026

iSOCaaS Cyber Security Event (Athens) — Info Day organised by NSQ.

- Apr 2026

Journal paper — “Next-Gen Security Operation Center Services for Critical National Infrastructures” (Lekidis, Yigit, Maglaras, Karantzalos, Spanoudakis) submitted to [MDPI Electronics](#).
- 16 Jun 2026

iSOCaaS presentation — iSOCaaS presented by Insuretics (INS).
- Q2 2026

Social media & web — Introductory video published on YouTube (May 2026); continued activity on LinkedIn, X and Facebook. [isocaas.eu](#) reached over 15,400 visits by 31 May 2026.

Dissemination & Communication KPIs — status to date

KPI	Description	Target	Done	Status
D&C-KPI-1	Info Days for pilot user selection	≥2	2	✓ Achieved
D&C-KPI-2	Workshops & seminars	≥4 (≥100 attendees)	2	🕒 In progress
D&C-KPI-3	Participation in trainings, workshops & open events	≥6	9	✓ Exceeded
D&C-KPI-4	National Authorities' & CSIRT/CERT meetings	≥10	—	→ Planned (HMOD / NCSA)
D&C-KPI-5	Cybersecurity stakeholder events & initiatives	≥4	4	✓ Achieved
D&C-KPI-6	Website statistics	≥2,000 sessions / year	15,427 visits*	✓ On track (~635 / month)
D&C-KPI-7	Blog posts on isocaas.eu	≥6 / year	3	🕒 In progress
D&C-KPI-8	eNewsletters	≥6 by project end	3	🕒 Issue #3 of 6
D&C-KPI-9	Promotional videos	≥2 by project end	1	🕒 In progress

KPI	Description	Target	Done	Status
D&C-KPI-10	Cooperations with other initiatives & projects	≥3	3	✓ Achieved

* Cumulative website visits from launch (Q1 2025) to 31 May 2026.

Synergies (D&C-KPI-10): GR-SME-SOC (SOC4SME) — SMEs already receiving SOC services under GR-SME-SOC are migrated to iSOCaaS (T2.4) and receive an extension of those services, while the GR-SME-SOC recruitment strategy is reused for iSOCaaS end-users. **ERMIS** — cooperation on cyber insurance through the common partners SPH, INS, NCSA and KUA. **SecAwarenessTruss (SAT)** — SPH, HMOD and NCSA cooperate on common training programmes.

Next newsletter: Issue #4 will cover Q3 2026 (M20–M22) — including the submission of D3.2 and closure of WP3, WP4 integration progress, and the first participation agreements with new pilot users (July 2026) under WP5.

STAY CONNECTED

Follow iSOCaaS

Keep up with project news, events, deliverables, and pilot results:

 isocaas.eu

 in LinkedIn

 [@iSOCaaS_eu](#)

 Facebook

 YouTube

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