WHEN NATIONAL CERT EXPERTISE MEETS SECTOR INNOVATION

In critical infrastructure, trust moves faster than data. At ALiEnS-SOC this principle is not a slogan - it is an operational reality. The involvement of Slovenia's national Computer Emergency Response Team, SI-CERT, represents far more than institutional support. It is the foundation that allows the ALiEnS-SOC project to transform threat intelligence into actionable protection for the energy sector.

A Trusted Gateway to International Cyber Cooperation

As Slovenia's national CERT, SI-CERT operates within established international cooperation frameworks that connect national and sectoral response teams across Europe and beyond. Within ALiEnS-SOC, this structured cooperation ensures that relevant insights from Slovenia's electro-energy environment can be exchanged through trusted channels, while respecting confidentiality and operational sensitivity.

For this project, this translates into practical value: information does not remain confined to a single organisation or sector. Instead, validated intelligence can circulate among trusted peers, and in return we gain timely alerts, additional context, and coordinated mitigation measures. In this way, national visibility is systematically reinforced by international perspective, strengthening resilience across the energy sector. To operationalise this exchange in a structured and scalable way, ALiEnS-SOC relies on a technical backbone that ensures intelligence is not only shared, but standardised, protected, and immediately usable.

MISP as the Operational Backbone

To make international cooperation practical, ALiEnS-SOC uses MISP (Malware Information Sharing Platform), an open-source platform designed for structured sharing of cyber threat intelligence, with SI-CERT's instance acting as the central distribution point.

In simple terms, this means that relevant cybersecurity insights can be shared with trusted partners in a clear and organised way. Information is reviewed, structured, and labelled before it is exchanged, ensuring that recipients understand how it can be used and how sensitive it is.

At the same time, confidentiality remains a priority. Sensitive details are carefully handled so that operational value is preserved without exposing internal systems or identities.

For ALiEnS-SOC, this approach ensures that shared intelligence is not just informative, but usable. It can support detection systems, guide defensive measures, and strengthen coordinated response efforts across the energy sector - without adding unnecessary complexity.

From Early Warning to Coordinated Defence

International engagement through SI-CERT significantly expands the project's operational horizon. By receiving first sightings of campaigns targeting both OT (Operational Technology – the

systems that control physical processes such as power grids, substations, and industrial equipment) and IT (Information Technology - traditional digital systems such as servers, networks, and business applications) environments, consortium gain valuable lead time to harden controls and brief operators.

High-confidence indicators can be pushed directly into blocklists and detection systems, reducing response times and limiting the radius of attacks. Cross-border correlations reveal infrastructure reuse, evolution of attacker techniques, and lateral movement patterns that are directly relevant to grid operations.

Supply chain visibility is enhanced through alerts related to vendor components and industrial protocols, accelerating patching and mitigation processes. In the case of DDoS threats, shared telemetry and signatures allow coordinated filtering across providers and peering points, safeguarding both customer-facing services and operator coordination channels.

Through this structured international cooperation model, ALiEnS-SOC ensures that shared intelligence is practical, operational, and immediately deployable across the sector.

Elevating Skills Across the Energy Cyber Ecosystem

The partnership is not limited to technical exchange. International cooperation acts as a force multiplier for skills, methodologies, and tooling. Joint exercises, after-action exchanges, and shared playbooks elevate analyst tradecraft across the consortium.

To illustrate this in practice, imagine a scenario in which an energy operator within the ALiEnS-SOC ecosystem detects unusual activity targeting a substation management system. During a joint exercise, analysts simulate the incident together with international partners, compare investigative approaches, and review how detection rules performed. In the after-action discussion, they identify small tuning improvements and update shared playbooks to clarify response steps. The result is not just a resolved exercise scenario, but improved readiness across all participating organisations.

Continuous quality feedback reduces false positives and improves detection tuning. Standardised exports and automation shorten the path from intelligence to controls, improving mean time to detect and respond. Over time, these practices embed durable maturity within the ALiEnS-SOC ecosystem - maturity that outlives any single campaign or threat actor.

Turning Collective Defence into Local Advantage

At its core, ALiEnS-SOC is about building an AI-powered, intelligence-driven Security Operations model for Slovenia's electro-energy sector. With SI-CERT's global ties and MISP-based distribution model, local telemetry becomes collective defence - and collective defence returns as local advantage. This continuous loop of trusted exchange is how a sector as vital as energy stays one step ahead: fast, careful, and connected. When national CERT expertise meets sector innovation, resilience is no longer reactive. It becomes strategic.

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The project funded under Grant Agreement No. 101190349 is supported by the European Cybersecurity Competence Centre.