Exploring NIS2 Compliance in the Energy Sector Using AI-Driven Cyber Threat Intelligence

Jani Siivola, Rami Paronen, Uzair Tariq, Quyet Pham, Warren Villegas, Ilkka Tikanmäki[1] and Jyri Rajamäki[2]
Laurea University of Applied Sciences, Espoo, Finland

Ilkka.tikanmaki@laurea.fi

Abstract: The NIS2 Directive introduces stricter requirements for how essential entities, including energy-sector operators, must manage cybersecurity risks and report incidents. In practice, many organisations face difficulties in transforming these legal obligations into concrete, daily security operations, especially in operational technology (OT) environments where visibility, logging, and coordinated responses are often limited. This paper examines how SecureAI, an AI-based anomaly detection and enrichment tool within the Cyber Threat Intelligence (CTI) ecosystem, can help energy operators meet key NIS2 obligations. The study is based on a qualitative desk-research approach, a comparative mapping of SecureAI capabilities against NIS2 Articles 20-26, and a realistic OT case scenario based on recent intrusion patterns. Prior research shows that AI can detect industrial anomalies faster and more accurately than rule-based systems, and that automated CTI processing can turn raw alerts into structured and shareable intelligence. At the same time, NIS2 requires accountable use of such tools, meaning that human oversight, transparency of analysis, and reliable evidence generation must be part of AI-supported workflows. These requirements guided the assessment. The analysis shows that SecureAI supports several key NIS2-related tasks. It identifies unusual behaviour in network and host telemetry, enriches findings with asset information and event relationships, and produces structured alert objects that support operator decision-making. The CTI Framework then converts these enriched alerts into STIX/TAXII objects suitable for reporting, documentation, and intelligence exchange. The case scenario–an unauthorised remote-access intrusion followed by suspicious HMI-PLC activity–demonstrates how SecureAI can highlight the anomaly, provide context for understanding its impact, and supply material for reporting and further investigation.

Keywords: NIS2 Compliance, Critical energy infrastructure, AI-driven anomaly Detection, Cyber threat intelligence automation, Operational cyber defence

1. Introduction

The NIS2 Directive places stricter cybersecurity obligations on essential-sector operators, including organisations in the European energy sector (European Parliament and Council, 2022). These entities must implement risk-management measures and meet rigorous incident-reporting requirements, yet many struggle to translate NIS2's high-level legal expectations into daily operational practices. The challenge is particularly pronounced in OT environments, where limited visibility, sparse logging and legacy systems hinder effective threat detection and response.

Recent advances in artificial intelligence (AI) and cyber threat intelligence (CTI) offer promising ways to address these operational gaps. AI-driven anomaly-detection systems have demonstrated stronger performance than traditional rule-based tools (Govea et al., 2024), while automated CTI platforms can transform raw alerts into enriched, contextualised intelligence suitable for reporting and information sharing. These capabilities align with NIS2 requirements for early detection, structured incident handling and coordinated information exchange.

This study examines how SecureAI—an anomaly detection and alert enrichment tool—can support selected NIS2 operational obligations for energy sector OT environments. We map relevant NIS2 requirements to SecureAI and assess their application through a representative OT intrusion scenario. Integrating SecureAI into an energy sector OT environment will improve the operator's capability to fulfil NIS2 requirements for threat detection, incident handling, reporting, and information sharing.

The Research Question of this study is: Can the combination of AI-based anomaly detection and CTI automation provide an operational capability that meets the NIS2 requirements in energy sector OT environments?

2. NIS2 and the Energy Sector

Energy infrastructure is increasingly exposed to unprecedented cybersecurity threats that jeopardise the stability and reliability of critical systems (Ajayi, Alozie & Abioba, 2025). The NIS2 Directive (Directive (EU)

[1] https://orcid.org/0000- 0001-8950-5221

[2] https://orcid.org/0000–0003–4798–2462

2022/2555) strengthens cybersecurity requirements for essential entities, including electricity, gas, oil and hydrogen operators (European Parliament and Council, 2022). Several provisions relate directly to technical operations. Article 20 assigns management responsibility for approving cybersecurity measures and ensuring staff training. Article 21 outlines operational security measures, including monitoring, incident handling, backup and recovery, and vulnerability management. Article 23 introduces strict reporting timelines (24-hour early warning, 72-hour notification and one-month final report). Article 24 allows Member States to require the use of certified ICT products for selected security functions. Article 29 mandates structured information sharing among trusted entities (Ruohonen, 2024).

NIS2 also places greater emphasis on the resilience of OT environments, which are especially challenging due to legacy equipment, limited telemetry, and the need to maintain operational continuity. Unlike traditional IT systems, OT assets cannot be easily patched or rebooted without affecting safety or uptime, which complicates the implementation of NIS2's risk-management measures. Energy networks are also highly interconnected, meaning disruptions in one part of the system can cascade across regions or even countries. These operational realities increase the difficulty of implementing consistent monitoring, rapid incident response, and evidence-based reporting.

Recitals 51–52 encourage the use of automated and AI-based security tools, provided they operate transparently and support interoperability. This establishes a foundation for evaluating how SecureAI might support NIS2-aligned operational tasks in energy-sector OT environments. The combination of strict regulatory obligations and structurally challenging operational contexts creates a clear motivation for exploring whether AI-driven detection and CTI workflows can provide practical, scalable support for compliance.

3. Literature Review

AI-based anomaly detection has demonstrated notable benefits in industrial systems, outperforming rule-based approaches in detecting irregular or malicious activity under noisy OT conditions (Aydın, 2025; Govea et al., 2024). Machine-learning and deep-learning models can capture subtle behavioural deviations that would be invisible to threshold-based or signature-based detection methods. Studies also highlight that OT traffic often exhibits stable behavioural patterns, which makes it well-suited for modelling normal baselines—an advantage leveraged by anomaly-detection systems.

Research on compliance automation shows how AI can support regulatory obligations by processing requirements, generating structured documentation and reducing manual reporting workloads (Alevizos, 2025; Seethala, 2025). Automation can also reduce human error and improve consistency in the documentation submitted to regulators. NIS2's tight reporting deadlines make this especially relevant, as organisations often struggle with assembling reliable evidence within 24–72 hours.

Cyber threat intelligence (CTI) frameworks contribute to coordinated incident handling by correlating multi-source telemetry, enriching alerts, and sharing structured intelligence (Gong & Lee, 2021). Established platforms such as MISP, OpenCTI and the TAXII protocol ecosystem demonstrate the maturity of automated intelligence exchange. Research also suggests that integrated CTI workflows enable faster triage and reduce analyst workload during multi-stage attacks. Together, these strands suggest that AI-driven detection and CTI automation can meaningfully support the operationalisation of NIS2 in energy-sector OT environments, especially where resource constraints or telemetry gaps hinder traditional approaches.

4. Methodology

A qualitative desk-research approach was used to analyse how SecureAI can support operational tasks related to the NIS2 Directive in energy sector OT environments. Operational cybersecurity obligations - governance oversight, cybersecurity risk management, incident reporting, certification-related documentation and information sharing - were extracted from Articles 20, 21, 23, 24 and 29 of NIS2. As NIS2 combines organisational and technical requirements, the analysis focuses on obligations that technical systems can realistically support. Governance, accountability and certification remain organisational responsibilities. Auditability and traceability were included as interpretive criteria when assessing technical outputs. Each selected operational requirement was compared against SecureAI and CTI capabilities to determine where they support NIS2-aligned workflows. The resulting alignment is summarised in Section 5.

5. Results

SecureAI contributes most directly to Articles 21, 23 and 29 while providing supporting evidence for Articles 20 and 24. To illustrate how SecureAI supports NIS2-aligned workflows, we apply it to a representative OT intrusion scenario inspired by recent attacks reported in the energy sector (Dragos Inc., 2025; ENISA, 2024). An attacker exploits an exposed remote-access interface to enter a substation network and issues unauthorised HMI commands to alter PLC setpoints. Such sequences reflect real-world intrusions targeting substation protection schemes, where even minor configuration changes can result in significant electrical or safety impacts.

In a typical substation architecture, remote-access servers sit between IT and OT zones and are intended only for maintenance use. If security controls are weak—such as default passwords, unpatched VPN appliances or inadequate segmentation—these access points become attractive attack vectors. Once inside, adversaries can move laterally across engineering workstations, historians, or HMIs to identify PLCs responsible for voltage regulation or protection logic.

SecureAI monitors remote-access activity, HMI command patterns and PLC responses. It would detect abnormal command timing or parameter changes that deviate from established baselines, such as bulk modifications of protection thresholds or rapid sequence execution outside maintenance windows. SecureAI then enriches alerts with affected assets, event relationships and estimated severity (Chalkias, 2024). This enables operators to take concrete mitigation actions—such as isolating the compromised access point, restoring PLC configurations or activating contingency procedures—while retaining human oversight for safety-critical decisions.

The CTI Framework structures the enriched alert, correlates it with further indicators (e.g., suspicious IPs, failed-authentication patterns, or known threat-actor TTPs) and converts it into STIX/TAXII packages supporting early detection (Art. 21), reporting workflows (Art. 23) and trusted information sharing (Art. 29) (European Parliament and Council, 2022). If deployed operationally, this structured evidence could also support internal post-incident reviews and regulator audits.

6. Discussion and Conclusions

The findings align with research showing that AI-driven anomaly detection and CTI automation enhance situational awareness and response effectiveness in OT environments (Gong & Lee, 2021; Govea et al., 2024). SecureAI reflects these approaches through integrated detection, contextual enrichment and structured intelligence dissemination. Its ability to relate events across assets and generate machine-readable intelligence reduces cognitive load for analysts and supports the structured decision-making expected in NIS2-compliant operations.

The scenario demonstrates how SecureAI supports NIS2-aligned tasks by detecting abnormal behaviour, linking events to assets and providing evidence that triggers containment steps such as isolating compromised interfaces or reverting PLC settings. The CTI Framework adds auditability by generating structured, traceable incident data that regulators or internal teams can verify. This is important because NIS2 emphasises demonstrable accountability: operators must not only act but also show why they acted and what evidence informed their decisions.

However, several limitations persist. AI-based anomaly detection and CTI automation performance depend heavily on telemetry quality, and many OT environments still lack adequate logging or network visibility—issues identified repeatedly in industry assessments (ENISA, 2024). In addition, anomaly detection may generate ambiguous alerts that require contextual understanding from operators. Organisational readiness—including training, defined escalation paths and a culture of cyber-physical safety—is therefore as critical as the technology itself. Future integration with explainable AI techniques may also help operators better interpret model outputs during high-pressure events.

This study assessed how SecureAI can support selected operational obligations of the NIS2 Directive for energy-sector OT environments. The mapping and scenario analysis show that SecureAI enhances detection, contextualisation and structured reporting, contributing to NIS2 requirements for monitoring, incident handling and information sharing. When combined with human oversight, these tools offer a practical path to operationalising NIS2 duties.

Ethics Declaration: No human participants or personally identifiable information were involved. All data sources were publicly available.

AI Tools Declaration: Keenious was used for literature exploration, and ChatGPT 5.1 for drafting and refinement. Human authors verified all content.

References

Ajayi, O. O., Alozie, C. E., & Abieba, O. A. (2025). Enhancing cybersecurity in energy infrastructure: strategies for safeguarding critical systems in the digital age. *Trends in Renewable Energy*, *11*(2), 201-212.

Alevizos, L. (2025). Automated cybersecurity compliance and threat response using AI, blockchain and smart contracts. *International Journal of Information Technology*, *17*(2), 767–781. https://doi.org/10.1007/s41870-024-02324-9

Aydın, Z. (2025). Detecting Cybersecurity Threats in Digital Energy Systems Using Deep learning for Imbalanced Datasets: Deep Learning for Cyber Threat Detection in Critical Energy SCADA. *International Journal of Energy Economics and Policy*, *15*(3), 614–628. https://doi.org/10.32479/ijeep.19649

Chalkias, I. (2024). *D4.1 – Initial prototypes of the cyber-threat intelligence gathering, extraction, sharing components and AI-based solutions. [*. https://horizon-dynamo.eu/wp-content/uploads/2025/02/DYNAMO-RPT-D41-V2-0.pdf

Dragos Inc. (2025). *ICS/OT Cybersecurity Report* (Annual Year in Review No. 8; p. 56). Dragos Inc. https://pkcert.gov.pk/uploads/2025/02/Dragos-2025-OT-Cybersecurity-Report-A-Year-in-Review.pdf

ENISA. (2024, December 10). *Cyber Europe tests the EU Cyber Preparedness in the Energy Sector* [Press Release]. https://www.enisa.europa.eu/news/cyber-europe-tests-the-eu-cyber-preparedness-in-the-energy-sector

European Parliament and Council. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02022L2555-20221227

Gong, S., & Lee, C. (2021). Cyber Threat Intelligence Framework for Incident Response in an Energy Cloud Platform. *Electronics*, *10*(3), 239. https://doi.org/10.3390/electronics10030239

Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence. *Systems*, *12*(5), Article 5. https://doi.org/10.3390/systems12050165

Ruohonen, J. (2024). *A Systematic Literature Review on the NIS2 Directive* (No. arXiv:2412.08084). arXiv. https://doi.org/10.48550/arXiv.2412.08084

Seethala, S. (2025). An AI-Driven Compliance Intelligence Platform for Continuous Monitoring and Automated Risk Assessment in Regulated CRM and ERP Systems. *International Journal of Scientific Research and Engineering Trends*, *11*(6), 2395-566X. https://doi.org/10.5281/zenodo.17938605