Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.068509

ARTICLE

# A Security Operation and Event Management (SOEM) Platform for Critical Infrastructures Protection

**Roberto Caviglia[1], Daniyar Aliaskharov[2], Alessio Aceti[1], Mila Dalla Preda[3], Paola Girdinio[2] and Giovanni Battista Gaggero[2,*]**

[1]HWG Sababa Security S.r.l., Piazza Tre Torri 2, Milan, 20145, Italy
[2]Department of Electrical, Electronics and Telecommunications Engineering and Naval Architecture (DITEN), University of Genoa, Via Opera Pia 11A, Genoa, 16145, Italy
[3]Department of Computer Science, University of Verona, Strada le Grazie, 15, Verona, 37134, Italy
*Corresponding Author: Giovanni Battista Gaggero. Email: giovanni.gaggero@unige.it

Received: 30 May 2025; Accepted: 26 August 2025; Published: 23 October 2025

**ABSTRACT:** Industrial Control Systems (ICS) in Operational Technology (OT) environments face unique cybersecurity challenges due to legacy systems, critical operational needs, and incompatibility with standard IT security practices. To address these challenges, this paper presents the Security Operation and Event Management (SOEM) platform, a software designed to support Security Operations Centers (SOCs) in reaching full visibility of OT environments. SOEM integrates diverse log sources and intrusion detection systems, including logs generated by the control system itself and additional on-the-shelf products, to enhance situational awareness and enable rapid incident response. The pilot project was carried out within the funded project SOC-OT-IGE from the "Centro di Competenza Start 4.0" and is being developed in partnership with Ansaldo Energia and HWG Sababa. The validation has been conducted in a real-world pilot project. Thanks to the mapping to requirements for compliance with IEC 62443, the platform demonstrates its effectiveness through defined key performance indicators (KPIs). This work bridges the gap between IT-centric SOC methodologies and the specialized needs of industrial cybersecurity.

**KEYWORDS:** Cybersecurity; monitoring; intrusion detection; SIEM; SOC

## 1 Introduction

Security Operations Centers (SOCs) have become integral to IT security strategies for their capability to monitor, identify, and respond to threats in real time [1,2]. Although SOCs demonstrate strong effectiveness in IT environments, conventional SOC frameworks face significant difficulties when applied to Operational Technology (OT) systems [3]. The fundamental distinctions between IT and OT settings create distinct challenges. For instance, numerous Industrial Control Systems (ICS) operate on legacy hardware and software that often lack compatibility with contemporary cybersecurity tools commonly deployed in IT-oriented SOCs. Because of this dependence on outdated technology, coupled with the necessity for uninterrupted operations, conventional IT security measures—such as routine patching, antivirus checks, or system reboots—are often impractical and, in some cases, could jeopardize OT environments. Consequently, security approaches for ICS environments must be meticulously tailored to address these operational constraints while maintaining system security and reliability, which means taking into account the physical parameters of the systems and the evolution of the process [4].

To address these specific needs, we propose a specialized platform, called Security Operation and Event Management (SOEM), that has the aim to strengthen conventional SOC capabilities for OT environments. SOEM is engineered to bridge the gap between IT-centric SOC practices and OT requirements, offering a flexible and customized security approach. This paper aims to introduce a new approach for developing a platform designed to support Security Operations Center teams in monitoring Operational Technology within industrial networks. The platform leverages multiple log sources and commercial intrusion detection systems to enhance situational awareness for both industrial and IT engineers, enabling quick and effective responses to potential attacks. Validation is conducted within a pilot project on a real infrastructure, and results are presented through an anonymized network scheme to preserve reserved information; in particular, the validation is based on gaining compliance with the IEC 62443 standard.

The paper is structured as follows. Section 2.1 analyzes related works regarding cybersecurity monitoring tools for ICS. Section 3 describes the proposed platform, defining the reference architecture and the tools that act as a log source for the platform. Section 4 details the implementation of the platform on a real use-case scenario. Section 5 presents the KPI that we defined to assess the performances and validation of the proposed approach. Finally, in Section 6, conclusions are drawn.

## 2 Background

### *2.1 Related Works*

Regulatory pressures surrounding industrial cybersecurity have grown stronger in recent years, as emphasized in the ENISA report [5]. Meeting monitoring requirements can be supported by various technologies, and numerous studies have explored cybersecurity monitoring tools, often focusing on specific technologies or organizational assets. According to the classification proposed by [6], cybersecurity monitoring tools are critical for operational data collection. The Security Information and Event Management (SIEM) platform, in particular, is essential, bridging strategic data collection, analysis, and visualization categories. The organizational implementation of SIEMs is further examined in [7].

While some studies concentrate on SIEM platforms, others emphasize tools like Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR). For instance, reference [8] assesses EDR effectiveness in detecting and mitigating Advanced Persistent Threats (APTs) across various scenarios. Additionally, reference [9] reviews EDR tools, evaluating their performance in malware detection.

Network Intrusion Detection Systems (NIDS), which may be hardware- or software-based, monitor segments of network systems to detect malicious activity and policy violations [10]. This monitoring spans multiple layers of the TCP/IP stack. In industrial contexts, particularly at lower network levels, NIDS are often passive. However, there is a growing interest in solutions that can also block traffic, evolving NIDS into Network Intrusion Prevention Systems (NIPS).

SOC analysts, the primary users of supervisory, event management, and response tools, operate mainly on SIEM and SOAR platforms—terms introduced by Gartner for commercial applications [11]. A thorough technical and market analysis of prominent SIEM solutions is available in [1]. SIEM platforms are designed to collect, parse, store, and analyze logs and can integrate logs from across an organization. Increasingly, these platforms are being adapted for OT environments [12]. However, integration remains limited; there is a pressing need for tools specifically designed to extend SIEM functionalities to OT contexts. To our knowledge, this study is the first to introduce a specialized platform tailored for SOCs in OT networks.

### *2.2 Commercial Tools*

- *Splunk Enterprise Security*: Splunk Enterprise Security enables robust integration with OT environments by leveraging its Industrial Asset Intelligence app and partner solutions such as Nozomi Networks and Dragos. Through these integrations, Splunk can ingest and analyze data from ICS/SCADA systems and support industrial protocols such as Modbus, DNP3, and OPC when processed via third-party connectors [13]. The platform offers real-time monitoring of industrial assets and creates dashboards that provide visibility into OT network behavior. Splunk's analytics engine supports anomaly detection in programmable logic controllers (PLCs), sensors, and other critical industrial components, making it suitable for converged IT/OT environments.
- *IBM QRadar*: IBM QRadar provides comprehensive OT visibility by integrating with external OT security solutions, including Nozomi Networks, Claroty, and Tenable OT. These integrations allow QRadar to ingest enriched telemetry from OT networks and perform correlation with IT events, enabling unified situational awareness. The platform supports a variety of ICS log formats through custom parsers and includes pre-configured threat detection rules for industrial environments. By supporting threat intelligence feeds (via STIX/TAXII) tailored to ICS threats, QRadar enables advanced behavioral baselining and detection of anomalies specific to industrial protocols and devices.
- *LogRhythm*: LogRhythm has developed features specifically designed to support operational technology security. It offers pre-built parsing rules and threat detection models tailored to ICS/SCADA environments and integrates with partners such as SCADAfence and Claroty. The platform allows secure log collection from OT systems, either agentlessly or via secure Syslog. It also provides customizable dashboards that help operators monitor critical infrastructure. Furthermore, LogRhythm's SmartResponse capabilities can be configured to automate containment or mitigation actions in response to anomalies detected within industrial networks.
- *Securonix*: Securonix incorporates OT monitoring by using its User and Entity Behavior Analytics (UEBA) engine to model baseline activity in industrial systems. It integrates with ICS security platforms like Nozomi Networks and Dragos to ingest passive network monitoring data and convert it into high-fidelity security insights. The platform applies AI/ML-driven analytics to detect deviations from normal OT behavior and correlates data across IT and OT systems to identify multi-stage attacks. It also maps threats using the MITRE ATT&CK for ICS framework, allowing industrial security teams to prioritize threats based on impact and tactics used.
- *FortiSIEM*: FortiSIEM, part of Fortinet's Security Fabric, offers OT log integration through native interoperability with other Fortinet products such as FortiGate, FortiNAC, and FortiSwitch. It enables centralized visibility of OT assets by passively discovering devices and identifying industrial protocols using network traffic analysis. With its integration into Fortinet's broader ecosystem, FortiSIEM can enforce segmentation policies and generate alerts when OT systems deviate from baseline behavior. It provides dashboards and rule templates specifically designed to monitor OT environments and can be extended with support for third-party industrial tools.

With respect to the tools described above, the proposed approach aims to support a Security Operations Center tailored specifically for Operational Technology environments. This framework emphasizes the unique requirements of industrial networks, focusing on real-time monitoring, incident response, and the integration of specialized OT security tools. In contrast, commercial SIEM platforms like Splunk Enterprise Security, IBM QRadar, LogRhythm, Securonix, and FortiSIEM are primarily designed for IT environments but have extended their capabilities to accommodate OT data. While they offer integrations for OT log ingestion and analysis, their core architectures are rooted in IT security paradigms. Key Differences include:

- Customization for OT Environments: SOEM is specifically designed to ensure compatibility with industrial protocols and devices. In particular, the Airfield Solution includes the parser of the Fieldbus protocol used between the local controllers and the I/O Modules.
- Real-Time Monitoring and Response: The proposed SOC framework emphasizes immediate detection and response to incidents within industrial networks, addressing the critical need for uptime and safety in OT environments. In particular, the physical-based monitoring logs allows to understand the impact of the ongoing cyberattack on the process, allowing to take countermeasure that preserve the safety of the plant. While commercial SIEMs offer real-time capabilities, they may not be optimized for the rapid response demands inherent in industrial settings.
- Integration with Specialized OT Tools: the design of the platform allows the integration of different log sources; this allows to choose only vendors that already guarantee compatibility with the OT protocols/devices used in the plant. Commercial SIEM platforms, although capable of integration, might not offer the same depth of compatibility with specialized OT tools without significant customization.

In summary, while both approaches aim to enhance security in OT environments, the SOEM offers a more tailored solution that addresses the unique challenges of industrial networks. Commercial SIEM platforms provide broad capabilities that can be extended to OT but may require additional customization to meet the specific needs of industrial settings.

### *2.3 The IEC 62443 Standard*

The primary standards governing cybersecurity in the OT sector include ISA/IEC 62443 and NIST SP 800-82. Additionally, the Cybersecurity Framework (CSF), introduced by NIST in 2014 and updated in 2022, remains a significant reference. According to the "SANS 2021 Survey: OT/ICS Cybersecurity," [14], the CSF and IEC 62443 are the two most widely adopted frameworks for mapping control systems.

This paper focuses on ISA/IEC 62443 Part 3-2 and -3, which outlines system security requirements and security levels. This part of the standard introduces seven Fundamental Requirements (FRs), further broken down into Security Requirements (SRs) and Requirement Enhancements (REs). It emphasizes a risk-based approach, including defining zones and conduits to manage security risks. For example, tools and network configurations are highlighted as essential cybersecurity measures. Security Levels (SLs), ranging from SL-1 to SL-4, are assigned to each SR based on the sophistication and resources of potential attackers and the complexity of the corresponding cyber threat. In detail:

- 62443-3-2: Focused on security risk assessment for system design, this section involves identifying the System Under Consideration (SUC), dividing it into zones and conduits, evaluating risks for each, and determining a target security level (SL-T) for each zone and conduit.
- 62443-3-3: This section specifies detailed technical Security Requirements (SRs) linked to the seven foundational requirements outlined in IEC 62443-1-1.

Reversing the approach, to validate our solution, we analyze which Security Target Level the System Under Consideration can achieve by introducing the SOEM platform, as detailed in Section 5.

## 3 Proposed Platform

SOEM is designed to deliver a real-time monitoring interface that equips operators with actionable insights into process efficiency, security incidents, and Key Performance Indicators (KPIs). Through the integration of operational and security data into a single dashboard, the system facilitates rapid identification of anomalies and emerging threats, thereby reducing the likelihood of disruptions to critical infrastructure SOEM also aids SOC teams in overseeing and safeguarding OT networks by aggregating data from diverse

log sources and integrating with commercial Network Intrusion Detection Systems. The aim is to foster collaboration between IT and OT personnel, ensuring that security measures are both technically robust and operationally feasible

### *3.1 Reference Architecture*

Fig. 1 illustrates a typical deployment architecture where SOEM is integrated within the OT environment. The scheme follows a classical architecture of the Purdue model, in which there is a multiple segmentation of networks. In this setup, the primary security monitoring tools include a NIDS, a NIPS, endpoint protection, and physical monitoring systems [15]. Additionally, SOEM gathers data from SCADA systems to analyze the industrial process dynamics, enabling the detection of physical anomalies that may indicate a cyberattack. This capability marks a key distinction from traditional SIEMs, as the SOEM dashboard provides alerts not only on cybersecurity threats but also on anomalies within the industrial process itself.

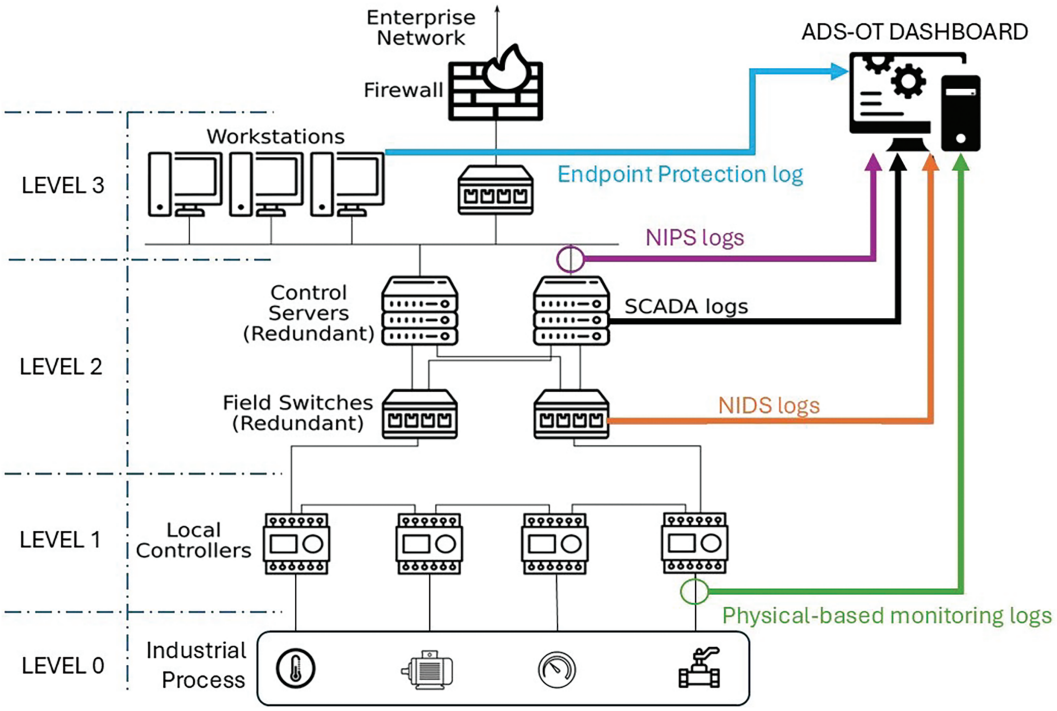


**Figure 1:** Reference Network Architecture of an ICS

The NIPS is installed "above" the SCADA server, not to compromise critical commands in case of false positives; at the same time, lever 3 may be more exposed to attacks coming from the outside of the plant. NIDS is installed on the span port of the switch to capture all the traffic of the control network; additionally, also traffic coming from the enterprise switch may collect the traffic. Endpoint protection is installed on all machines of level 3, both workstations and servers. Finally, Physics-based monitoring is installed between the local controllers and sensors/actuators.

### *3.2 The Platform*

The SOEM solution is designed to collect logs, alerts, data, and parameters from various devices and sources spanning Levels 1 to 3 of the Purdue model. The architecture of SOEM, illustrated in Fig. 2, includes the following components:

- Data Parser: This module aggregates logs, alerts, parameters, and other data from diverse sources such as NIDS, NIPS, endpoint protection tools, physical monitoring devices, and SCADA or DCS systems, ensuring thorough OT data acquisition.
- Database: Serving as the central storage layer, it retains all parsed information for further processing and evaluation.
- Correlation Engine and Machine Learning Module: This component leverages predefined correlation rules alongside advanced ML techniques to analyze stored data, uncover patterns, and detect abnormal activities.
- Dashboard: The visualization interface presents the outputs of correlation and machine learning processes, enabling operators to monitor performance metrics and security alerts in real time.

An overall scheme is shown in Fig. 2.

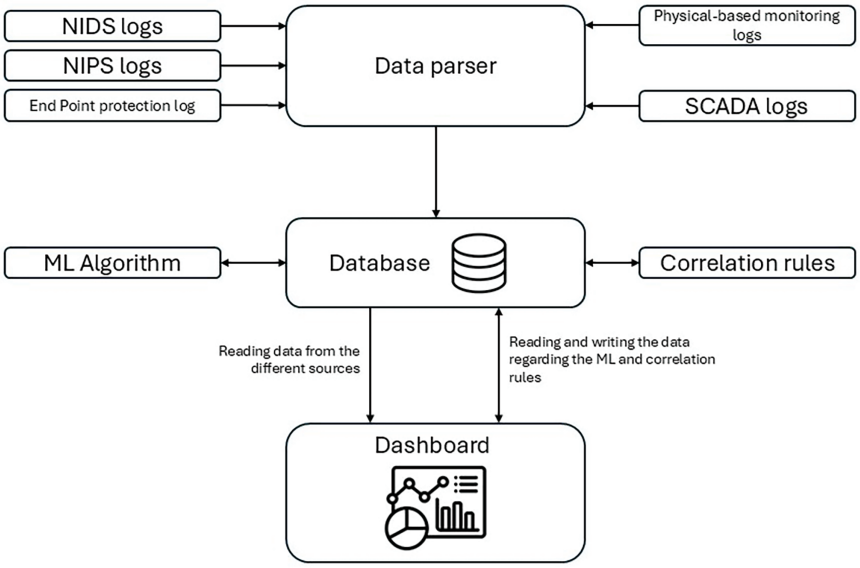


**Figure 2:** ELK block scheme

The Elastic Stack (ELK) consists of three core components, each playing a distinct role in managing logs and monitoring an OT environment. Logstash acts as the data ingestion and preprocessing engine, collecting logs from diverse OT sources such as sensors, industrial control systems, and network devices. It normalizes and filters the data, ensuring consistency and relevance before passing it to Elasticsearch. Elasticsearch serves as the central repository, efficiently storing and indexing the log data for quick retrieval and analysis. It allows users to query and analyze large volumes of data in near real-time, making it ideal for detecting anomalies or patterns. Finally, Kibana provides a user-friendly visualization and interface layer, enabling operators to create interactive dashboards, analyze trends, and respond to alarms. Together, these tools streamline data collection, storage, analysis, and visualization for effective OT system monitoring.

### *3.3 Data Analysis*

The ELK platform includes a built-in Anomaly Detection (AD) plugin that provides out-of-the-box algorithms to automatically detect anomalies in time series data. The core algorithm installed by default is a Random Cut Forest (RCF) model—a robust, unsupervised technique that identifies anomalous patterns by measuring how "isolated" a data point is relative to the rest of the data. ELK's AD feature is designed for streaming, near-real-time analysis, and supports both univariate and multivariate anomaly detection. It integrates natively with ELK's indices and dashboards, allowing users to configure detectors, visualize anomaly scores, and set up alerting with minimal setup.

By default, ELK anomaly detection is optimized for operational monitoring use cases such as detecting sudden spikes or drops in metrics, identifying system faults, or flagging unusual behavior in logs. For more control, a more robust solution is to customize detection by applying pre-defined thresholds to critical measures—useful when you want strict and pre-defined limits in addition to statistical models. Users can choose the default AD capabilities for quick, automated anomaly detection, or integrate their own machine learning algorithms into ELK using tools like ingest pipelines, connectors, or external processing frameworks for even more advanced, tailored detection workflows.

## 4 Implementation

The first prototype of the SOEM platform was carried out within the funded project SOC-OT-IGE from the "Centro di Competenza Start 4.0" and is being developed in partnership with Ansaldo Energia and HWG Sababa [16]. A key component of this evaluation involves testing the solution in a realistic environment. To facilitate this, the evaluation architecture uses an ICS network, illustrated in Fig. 3, which replicates a network responsible for managing key parameters of a steam turbine generator. It incorporates a simulator that replicates system dynamics, enabling safe and flexible testing within a controlled environment. Ansaldo Energia employs this architecture to validate new ICS configurations prior to deployment, ensuring both operational safety and effectiveness.

The evaluation architecture is organized according to the Purdue Model levels, as follows:

- Level 3—Operation Systems: This level includes SCADA and EWS systems, which oversee the control and configuration of the ICS. The process switch at this level links SCADA and EWS with ICS devices, while various components are deployed here:
  - Switch: This switch provides additional ports and limits the need for direct connections to the core switch, facilitating efficient monitoring by mirroring traffic from the process switch for NIDS and active NIDS tools. Two subnets are established: one for monitoring tools management and one for data transfer to the SOEM server.
  - Firewall: This firewall ensures secure, trusted communication between downstream and upstream systems, preventing the SOEM from becoming a potential entry point for threats.
  - OT Endpoint Protection: Endpoint protection software installed on the SCADA machine extracts security data, which is transmitted to the SOEM server through designated firewall rules.
  - NIPS: Positioned between SCADA and the ICS process, this tool focuses on securing communications and enforces rules to prevent cyber intrusions.
- Level 3.5—De-Militarized Zone (DMZ): Serving as a buffer between the IT and ICS networks, the DMZ houses the SOEM server, which aggregates data from various monitoring tools, as well as downstream OT monitoring systems. The server monitors tasks, request counts, and data flow to prevent data exfiltration.
  - NIDS: The NIDS passively analyzes mirrored traffic.

- Active NIDS: Beyond passive scanning, active NIDS queries network devices to retrieve specific information like component models, firmware versions, and recent requests.
- SOEM Dashboard: This user interface provides a comprehensive view of alerts and alarms generated by correlation rules and machine learning algorithms. Firewall roles are configured to maintain secure communication with the SOEM server.

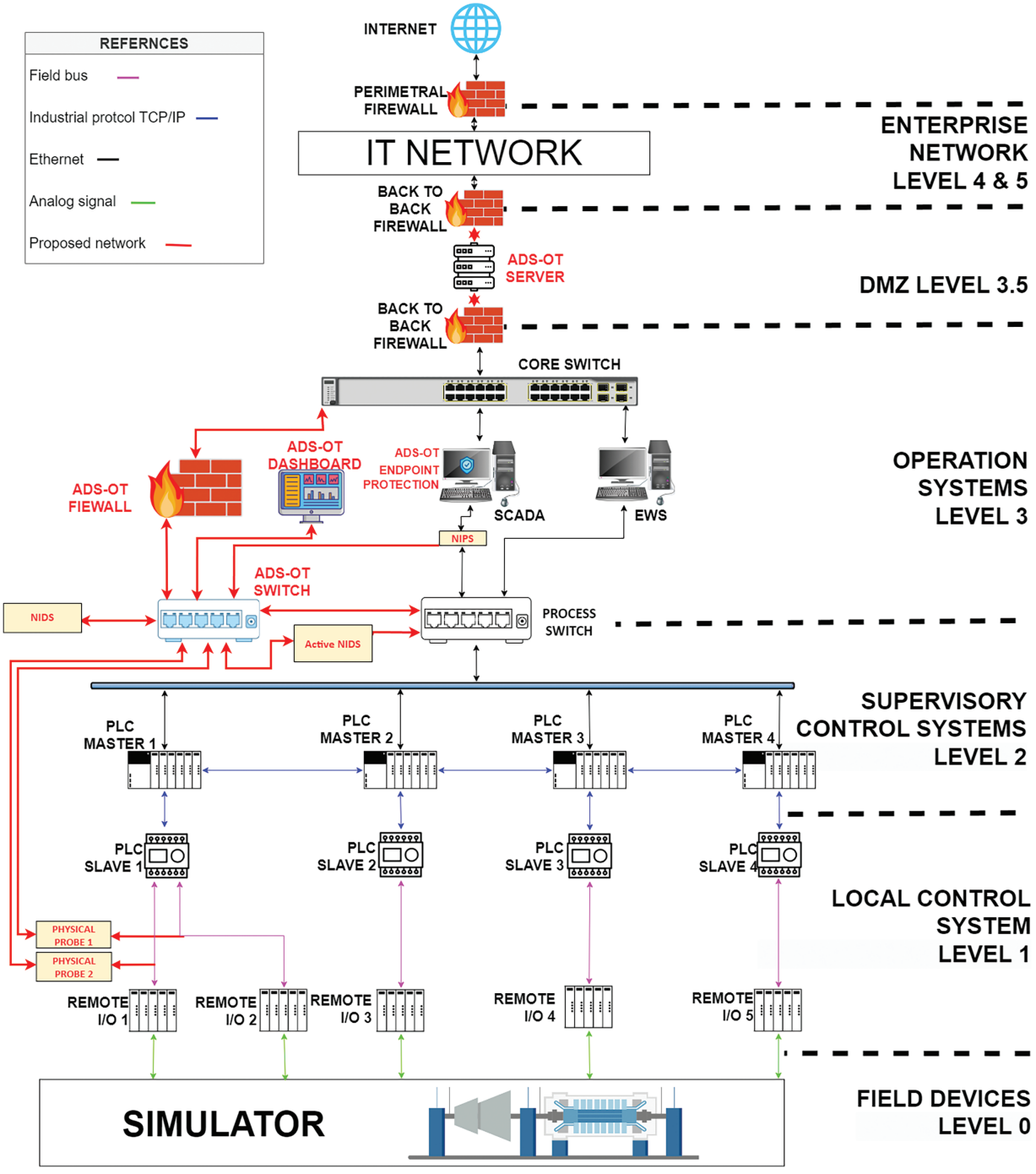


**Figure 3:** Anonymized Network Scheme of the system under consideration

- Level 2—Supervisory Control Systems: This level consists of a ring of master PLCs with high processing capabilities, enabling the calculation of new setpoints based on data exchange within the PLC network. These loops operate on a longer time cycle than lower-level control loops.
- Level 1—Local Control Systems: Comprising slave PLCs and Remote I/Os, this level directly interacts with the process through analog signals. Timeliness is critical at this level; delays in communication or processing could compromise operations. Two physical monitoring tools are installed to monitor data between PLC Slave 1 and Remote I/O 1 and 2 via the Fieldbus protocol, which is correlated with SCADA data through defined rules.
- Level 0—Field Devices: At this layer, a simulator is used as a combined hardware-software platform to replicate the physical behavior of a steam turbine generator. The simulator, built with a Matlab Simulink model, interfaces with the ICS through analog signal exchanges.

Table 1 summarizes the technology choices made for implementing SOEM.

**Table 1:** Commercial technologies choice for the implementation

| SOEM technologies | Commercial solutions |
|---|---|
| Server database | Elasticsearch [17] |
| Dashboard | Kibana [18] |
| Switch | Switch Aruba 4100i |
| Firewall | Firewall Fortinet 60D |
| NIDS | Radiflow ISID [19] |
| Active NIDS | Tenable OT [20] |
| NIPS | EdgeIPS [21] |
| Endpoint protection | Stellar [22] |
| Physical Probe | Airfield WatchField [23] |

Fig. 4 shows one window of the dashboard of the implemented platform. It can be noticed how the dashboard allows collection and summarization of log sources, and at the same time allows users to have visibility on the critical parameters of the industrial process.

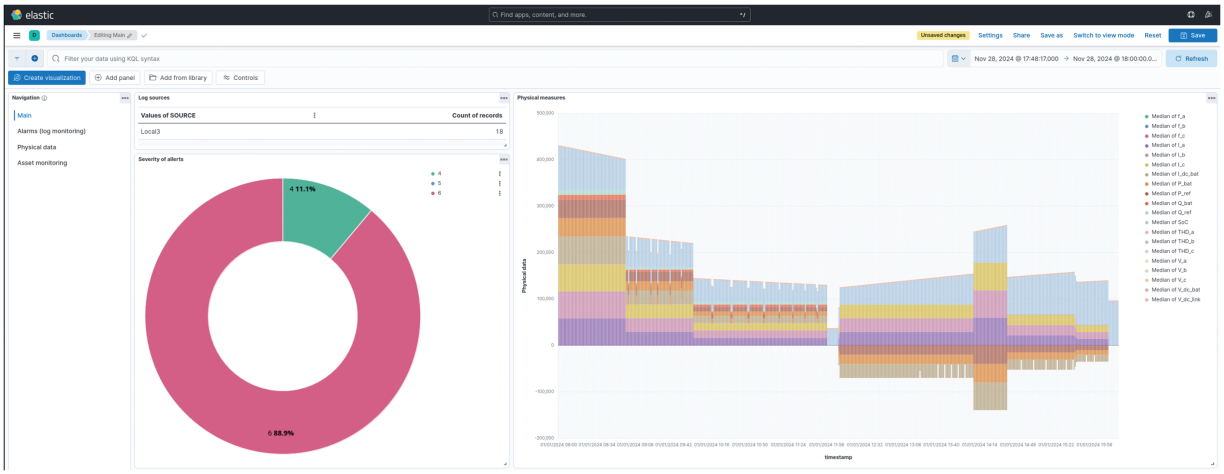


**Figure 4:** The dashboard of the SOEM Proof of Concept

## 5 Validation

### *5.1 Validation Process*

To conduct a thorough performance evaluation, it is essential to assess how the SOEM platform improves the cybersecurity monitoring capabilities of the ICS system managing the steam turbine generator. Three evaluation scenarios have been defined:

1. As-Is Scenario: This baseline scenario represents the current configuration of the steam turbine generator ICS system, with no additional monitoring tools or sensors installed. Only the pre-existing software monitors network traffic and physical parameters.
2. Improvement 1: In this scenario, commercial monitoring solutions are deployed independently within the system. These tools operate separately, each providing its own interface to the central SOC. They do not integrate with each other through the SOEM solution, resulting in isolated monitoring functions.
3. Improvement 2: This scenario involves implementing the SOEM platform developed for the project. The platform unifies data from the various monitoring tools listed in Table 1, correlates information, and provides a single, centralized Human Machine Interface (HMI). This integrated approach allows for a comprehensive and streamlined monitoring experience.

To evaluate the effectiveness of these scenarios, specific KPIs are used, divided into two categories:

- Technical KPIs: These indicators evaluate how effectively the system identifies active attacks. A key metric is the detection rate, defined as the proportion of successfully detected attacks compared to the total number of attacks executed during penetration testing. For instance, one such measure could be the system's ability to detect a Man-in-the-Middle (MITM) attack occurring between Levels 2 and 3.
- Compliance KPIs: These measures assess the system's adherence to the ISA99/IEC 62443 framework, emphasizing how effectively the proposed monitoring solutions satisfy the standard's requirements.

Detailed results on the penetration testing cannot be disclosed due to a confidentiality agreement. The proposed platform is validated primarily through compliance KPIs, showing how the proposed solutions helps achieving the requirements requested by the standard.

### *5.2 Compliance-Based Performance Evaluation*

We consider the portion of the network under the firewall as a single zone, i.e., a group of assets that share the same cybersecurity requirements. We analyze the SL that can be achieved in the three evaluation scenarios previously presented. Table 2 reports the security Level that can be achieved by respecting the Security Requirements of the various Fundamental Requirements by implementing the proposed solutions. In particular, the table aims to show the improvement that can be reached both with the deployment of on-the-shelf alone tools and with the implementation of the proposed platform. The symbol > indicates that this condition allows reaching that SL or higher. For example, >SL3 means that the solution allows reaching both SL3 and SL4, since there are no further requirements to be respected to reach SL4. The indication N/A (Not Applicable) is put when the SR is not related to monitoring/logging actions.

**Table 2:** IEC 62443-based compliance comparison

| FR | SR | As is | Improvement 1 | Improvement 2 |
|---|---|---|---|---|
| | 1 | N/A | | |
| | 2 | N/A | | |
| | 3 | N/A | | |

(Continued)

**Table 2 (continued)**

| FR | SR | As is | Improvement 1 | Improvement 2 |
|---|---|---|---|---|
| FR2 | 4 | N/A | | |
| | 5 | N/A | | |
| | 6 | N/A | | |
| | 7 | N/A | | |
| | 8 | SL1 | SL1 | >SL3 |
| | 9 | SL1 | >SL3 | >SL3 |
| | 10 | N/A | | |
| | 11 | N/A | | |
| | 12 | N/A | | |
| FR3 | 1 | N/A | | |
| | 2 | SL0 | SL2 | >SL3 |
| | 3 | N/A | | |
| | 4 | SL0 | SL2 | >SL3 |
| | 5 | N/A | | |
| | 6 | N/A | | |
| | 7 | N/A | | |
| | 8 | N/A | | |
| | 9 | SL0 | SL2 | SL4 |
| FR 5 | 1 | SL2 | SL4 | SL4 |
| | 2 | SL2 | >SL3 | >SL3 |
| | 3 | N/A | | |
| | 4 | N/A | | |
| FR 6 | 1 | SL0 | SL1 | >SL3 |
| | 2 | SL0 | SL2 | SL2 |
| FR 7 | 1 | SL0 | SL3 | SL3 |
| | 2 | N/A | | |
| | 3 | N/A | | |
| | 4 | N/A | | |
| | 5 | N/A | | |
| | 6 | SL1 | >SL3 | >SL3 |
| | 7 | N/A | | |
| | 8 | SL0 | >SL2 | >SL2 |

While most of the SRs are not addressed by monitoring tools, the ones related to log collection and analysis are all addressed by the proposed approach. In particular, it can be noticed how the SOEM platform allows reaching a Security Level 3 in the considered goal, while without the zone can reach only SL 2.

### *5.3 Discussion and Limitations*

Similarly to a SIEM platform, it is difficult to numerically quantify the benefits of the introduction of a centralized platform for log collection. While the previous section shows how the introduction of the

SOEM can allow reaching higher SL in specific requirements, an overall evaluation should include the user experience of the SOC team. In fact, while the introduction of commercial monitoring tools allows by themselves to reach certain security requirements, it is worth remarking that it could be particularly difficult to handle dashboards from different vendors. At the same time, commercial SIEM platforms do not include a visualization of data related to the industrial process, and therefore do not promote the collaboration between industrial and cybersecurity engineers. In this sense, a complete evaluation of the proposed solution should include the benefits in terms of user experience of different figures involved in the SOC team for critical infrastructures. Future works will include the test of the platform in a real SOC during a penetration testing; metrics that will be used will include the percentage of detected attacks, time-to-detect, and time-to-response after the implementation of the proposed platform.

## 6 Conclusions

This paper introduces the Security Operation and Event Management (SOEM) platform, a specialized solution for addressing the unique cybersecurity needs of Operational Technology (OT) environments. By bridging the gap between IT-centric Security Operations Center (SOC) practices and the specific requirements of Industrial Control Systems (ICS), SOEM offers a tailored approach to enhance situational awareness and enable effective incident response.

Through the integration of diverse log sources, commercial intrusion detection systems, and adherence to the IEC 62443 standard, SOEM has been validated in a real-world industrial scenario, demonstrating its practicality and performance. The results highlight the platform's potential to improve security monitoring while respecting the operational constraints of critical infrastructure systems. Future work will focus on refining the platform's capabilities, including scalability, automation, and real-time response mechanisms, to further strengthen its applicability across diverse OT environments.

**Acknowledgement:** We would like to thank the company Ansaldo Energia for the support during the tests.

**Funding Statement:** This work was performed together with the industrial partners HWG Sababa S.p.A. within the Italian National Project "SOC-OT" funded by "Centro di Competenza Start 4.0". This work was partially supported by the project "Airfield" under the PoC Launchpad initiative funded by the Fondazione Compagnia di San Paolo.

**Author Contributions:** The authors confirm contribution to the paper as follows: Conceptualization, Giovanni Battista Gaggero, Roberto Caviglia and Alessio Aceti; methodology, Giovanni Battista Gaggero and Roberto Caviglia; software, Giovanni Battista Gaggero, Roberto Caviglia and Daniyar Aliaskharov; validation, Giovanni Battista Gaggero and Roberto Caviglia, resources, Giovanni Battista Gaggero, Paola Girdinio, Mila Dalla Preda and Alessio Aceti; writing—original draft preparation, Giovanni Battista Gaggero and Roberto Caviglia; supervision, Giovanni Battista Gaggero, Paola Girdinio, Mila Dalla Preda and Alessio Aceti; project administration, Giovanni Battista Gaggero; funding acquisition, Giovanni Battista Gaggero, Paola Girdinio, Mila Dalla Preda and Alessio Aceti. All authors reviewed the results and approved the final version of the manuscript.

**Availability of Data and Materials:** Not applicable.

**Ethics Approval:** Not applicable.

**Conflicts of Interest:** The authors declare no conflicts of interest to report regarding the present study.

## Abbreviations

The following abbreviations are used in this manuscript

| | |
|---|---|
| SOEM | Security Operation and Event Management |

| | |
|---|---|
| SIEM | Security Information and Event Management |
| ICS | Industrial Control Systems |
| OT | Operational Technology |
| SOC | Security Operations Center |
| KPI | Key Performance Indicators |
| EDR | Endpoint Detection and Response |
| XDR | Extended Detection and Response |
| NIDS | Network Intrusion Detection Systems |
| NIPS | Network Intrusion Prevention Systems |
| FR | Fundamental Requirements |
| SR | Security Requirements |
| RE | Requirement Enhancements |
| SL | Security Level |
| SUC | System Under Consideration |
| DMZ | De-Militarized Zone |

## References


1. González-Granadillo G, González-Zarzosa S, Diaz R. Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors. 2021;21(14):4759. doi:10.3390/s21144759.
2. Sashwin K, Nithika K, Priyadharshini S, Maduvant S, Saranya. Analysis, trends, and utilization of security information and event management (SIEM) in critical Infrastructures. In: 10th International Conference on Advanced Computing and Communication Systems (ICACCS); 2024 Mar 14–15. Coimbatore, India; 2024. p. 1980–4.
3. Vielberth M, Böhm F, Fichtinger I, Pernul G. Security operations center: a systematic study and open challenges. IEEE Access. 2020;8:227756–79. doi:10.1109/access.2020.3045514.
4. Minetti M, Bonfiglio A, Benfatto I, Yulong Y. Strategies for real-time simulation of central solenoid ITER power supply digital twin. Energies. 2023;16(13):5107. doi:10.3390/en16135107.
5. Annex III. ICS security related standards, guidelines and policy documents [Internet]. [cited 2023 Nov 2]. Available from: https://www.enisa.europa.eu/publications/annex-iii.
6. Evesti A, Kanstrén T, Frantti T. Cybersecurity situational awareness taxonomy. In: 2017 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA); 2017 Jun 19–20; London, UK. p. 1–8.
7. Bhatt S, Manadhata PK, Zomlot L. The operational role of security information and event management systems. IEEE Secur Priv. 2014;12(5):35–41.
8. Karantzas G, Patsakis C. An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. J Cybersecur Priv. 2021;1(3):387–421. doi:10.3390/jcp1030021.
9. Arfeen A, Ahmed S, Khan MA, Jafri SFA. Endpoint detection & response: a malware identification solution. In: 2021 International Conference on Cyber Warfare and Security (ICCWS); 2021 Feb 25–26; Online. p. 1–8.
10. He K, Kim DD, Asghar MR. Adversarial machine learning for network intrusion detection systems: a comprehensive survey. IEEE Commun Surv Tutor. 2023;25(1):538–66 doi: 10.1109/comst.2022.3233793.
11. Gartner glossary terms [Internet]. [cited 2023 Oct 31]. Available from: https://www.gartner.com/en/glossary/all-terms.
12. Armellin A, Gaggero GB, Cattelino A, Piana L, Raggi S, Marchese M. Integrating OT data in SIEM platforms: an energy utility perspective. In: 2023 International Conference on Electrical, Communication and Computer Engineering (ICECCE); 2023 Dec 30–31; Dubai, United Arab Emirates. p. 1–7.
13. Subramanian K. Introducing the Splunk platform. In: Practical splunk search processing language: a guide for mastering SPL commands for maximum efficiency and outcome. Cham, Switzerland: Springer; 2020. p. 1–38.
14. Bristow M. A sans 2021 survey: OT/ICS cybersecurity. North Bethesda, MD, USA: SANS; 2021.
15. Armellin A, Caviglia R, Gaggero G, Marchese M. A framework for the deployment of cybersecurity monitoring tools in the industrial environment. IT Prof. 2024;26(4):62–70. doi:10.1109/mitp.2024.3396356.

16. Gaggero GB, Caviglia R, Girdinio P, Marchese M. Toward a security operation center for operational technology in industrial networks. In: Proceedings of the 2024 IEEE International Workshop on Technologies for Defense and Security; 2024 Nov 12–13; Naples, Italy. p. 160–4.
17. Elastic. The heart of the Elastic Stack [Internet]. [cited 2024 Oct 31]. Available from: https://www.elastic.co/elasticsearch.
18. Elastic. Discover, iterate, and resolve with ES—QL on Kibana [Internet]. [cited 2024 Oct 31]. Available from: https://www.elastic.co/kibana.
19. Radiflow. iSID Visibility, Anomaly Detection [Internet]. [cited 2024 Oct 31]. Available from: https://www.radiflow.com/products/ot-visibility-and-anomaly-detection/.
20. Tenable. Tenable one [Internet]. [cited 2024 Oct 31]. Available from: https://www.tenable.com/products/tenable-one.
21. Txone. EdgeIPS [Internet]. [cited 2024 Oct 31]. Available from: https://www.txone.com/products/network-defense/edgeips.
22. Txone. Stellar [Internet]. [cited 2024 Oct 31]. Available from: https://www.txone.com/products/endpoint-protection/stellar/.
23. AIrFIELD Security. WatchField [Internet]. [cited 2024 Oct 31]. Available from: https://www.airfieldsecurity.it/en/solutions/.