Operationalizing NIS2 Compliance through SIEM-Driven Alert and Incident Management

Cosmin-Matei MĂCĂNEAȚĂ
OMEGA-TRUST SRL
cosmin.macaneata@omega-trust.ro

Abstract: The NIS2 Directive (EU) 2022/2555 aims to improve cybersecurity rules for organisations with a focus on critical operators. To meet the new requirements, organisations must be able to monitor, detect and report cyber incidents effectively. Security Information and Event Management (SIEM) solutions from leading providers are designed to monitor and track certain activities on IT systems in order to quickly detect and process security threats. This article explains how SIEM systems handle alerts and incidents in Security Operation Centres (SOCs), in particular how they handle false positives, the mechanisms behind alert fatigue, how to correlate events, and how to conduct incident investigations. We also illustrate how these typical functions help organisations to meet the requirements of the NIS2 Directive and to enhance their security operations in general.
Keywords: SIEM, SOC, NIS2 Directive, Cybersecurity Monitoring, Incident Management, Alert Correlation

INTRODUCTION

In today's global context, cybersecurity has become a major priority for governments and organizations around the world. Given the current expansion of digital networks, critical services are becoming increasingly dependent on interconnected IT systems. As noted in relevant reports from recent years, essential services—such as the healthcare sector, financial institutions, energy networks, and government infrastructure—are increasingly affected by cyberattacks. This demonstrates the severity and significance of the impact of security incidents on economic stability and public safety.

In response to this growing trend of cyber threats, the European Union adopted the NIS2 Directive (EU) 2022/2555. This directive aims to establish a new, higher level of cybersecurity in member states (ENISA, 2024; European Commission, 2023). It expands the scope of the

https://doi.org/10.54851/v8i1y202605

existing framework on network and information security by introducing new, stricter requirements regarding risk management, incident detection, and reporting. For example: Article 21 requires organizations to implement appropriate technical and organizational measures to manage cybersecurity risks; and Article 23 establishes structured reporting rules, which include early notification within 24 hours, incident notification within 72 hours, and a final report to be submitted within one month. (European Commission, 2023).

Although the directive defines the obligations, it does not specify the technologies to be used. To ensure compliance, organizations must have the ability to monitor the large volumes of security data generated by modern IT systems. This is where SIEM platforms come into play, as they have the ability to collect data from multiple sources and apply correlation rules to identify suspicious activities. (Gonzalez-Granadillo, Gonzalez-Zarzosa & Diaz, 2021).

However, the effectiveness of SIEM platforms depends on how organizations manage the alerts generated by these systems within their own infrastructure. Security monitoring tools typically generate a large volume of alerts. Many of these alerts are harmless and do not represent actual cybersecurity incidents. In the absence of effective alert management processes, the sheer volume of alerts can overwhelm security analysts, thereby increasing the risk of human error and leaving critical incidents at risk of going unnoticed.

In this article, we will examine how SIEM platforms facilitate alert and incident management processes within Security Operations Centers (SOCs) and how these capabilities help meet the cybersecurity monitoring standards established by the NIS2 Directive. Although there are many studies covering SIEM architectures and incident response frameworks, we have observed that few analyze how operational SIEM monitoring processes meet regulatory requirements for cybersecurity. While studies and official guidance documents, including the ENISA report NIS2 Technical Implementation Guidance (2025), provide guidelines for implementing cybersecurity monitoring and incident reporting obligations from a governance and control perspective, studies on SIEM architectures from an academic perspective mainly focus on technical capabilities such as log collection, correlation of log events, identification of security incidents and other related processes.

This paper attempts to bridge this compliance gap and relate the ongoing operational processes in SIEM environments of Security Operation Centers (SOCs) to monitoring and incident reporting requirements introduced by the NIS2 Directive. Specifically, it elaborates on how tasks like alert triaging, false positive reduction, event correlation and incident management processes contribute to compliance with the NIS2's monitoring and incident reporting requirements.

METHODOLOGY

Below, we will present the methodology behind this study. It is based on a qualitative analysis of cybersecurity monitoring practices in SOC environments and their degree of compliance with the requirements of the NIS2 Directive (Cichonski et al., 2012).

For the research presented in this article, we combined the following aspects: a review of the existing academic literature on Security Information and Event Management (SIEM) platform architectures; various incident response processes; cybersecurity monitoring frameworks; and an analysis of SOC operational practices commonly used in enterprise environments. We used sources including scientific publications, cybersecurity standards such as NIST SP 800-61, and technical reports published by ENISA.

This study focuses on the operational lifecycle of security alerts generated by SIEM platforms. This includes: alert triage, event correlation, incident investigation, and incident reporting

processes. We will analyze these operational activities in relation to the cybersecurity monitoring and incident reporting requirements introduced by the NIS2 Directive. Through this approach, this article aims to identify how SIEM-based monitoring architectures can help organizations meet regulatory compliance requirements while improving the efficiency of security monitoring processes.

RESULTS AND CASE STUDY

This section illustrates the monitoring with SIEM through a practical example. It describes how the alerts from various parts of the infrastructure can be combined and analyzed in a SOC environment. The example is meant to demonstrate typical scenarios of alert correlation for an enterprise SOC monitoring.

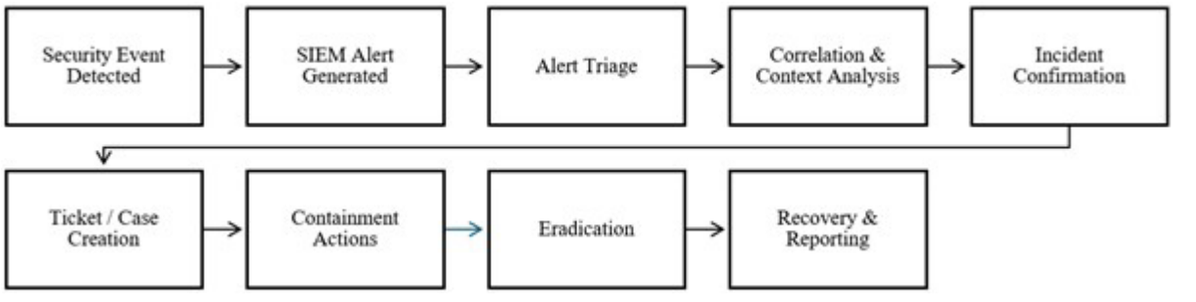

Figure 1. *SOC investigation workflow for security incident handling.*
Source: Author's conceptual model based on **Cichonski et al. (2012)** and typical SOC operational practices.

Enterprises today have a multitude of different network devices all sending logs to a SIEM platform. These devices and applications can include items like firewalls, authentication servers, endpoint protection software, and network monitoring devices, among others. In this scenario, the organisation has a variety of security systems in place working in concert to provide a layered defence.

During a simulated attack, the monitoring platform picked up a series of related events: first, multiple failed login attempts from various IP addresses within the organisation, followed by a single successful login from a geographic location from which the organisation had no prior authentication history.

All these events generated separate alerts in our monitoring solution, but thanks to correlation rules in our SIEM solution, they all ended up in the same investigation case, which hinted at a brute-force attack. After the SOC alerts were generated, the SOC analysts prioritized and investigated the related correlated events, incorporating information such as user behaviour patterns, historical login data and threat intelligence. After analysis, the SOC analysts identified the activity as a confirmed security incident, which was subsequently contained.

This example illustrates how SIEM correlation can significantly reduce the volume of incidents that require analyst attention, allowing them to focus on relevant patterns of behaviour indicative of attacks. Our research findings underline the need for structured alert management processes and also highlight the role of SIEM solutions in cybersecurity monitoring to meet the requirements of incident detection and reporting as laid out in the NIS2 Directive.

NIS2 DIRECTIVE AND OPERATIONAL CYBERSECURITY REQUIREMENTS

The NIS2 Directive represents a significant transformation in cybersecurity rules in Europe. It represents an expansion on the original NIS Directive and incorporates tougher cybersecurity

measures for organisations operating in sectors that are of key importance for society and the economy.

The NIS Directive specifies essential or important entities within various sectors, such as energy, transport, financial, including banking, health, including digital health technologies, other public and private entities providing essential services, including suppliers and manufacturers, and services to deal with emergencies such as fire-brigades and ambulance services. These entities will have to ensure adequate management of cybersecurity risks to protect their network and information systems against cyber threats.

Organizations subject to the new general data breach notification directive also need to be able to detect, analyze and report data breaches. Real-time operational monitoring is key to identifying attacks as they occur. Following the guidance on NIS2 implementation provided by ENISA (2025), organizations subject to NIS2 requirements will need to have a cybersecurity monitoring solution that provides real-time visibility into network traffic, system logs and security events across the organization's infrastructure. Such a solution will be needed to detect incidents, investigate and report as required, all within the specified timelines.

Operational cybersecurity monitoring is a key requirement for NIS2 compliance. Organisations will need to establish monitoring setups to collect and analyse log data from various sources of data, detect security events and potential security incidents, and maintain records to support compliance reporting requirements. Existing SIEM solutions address these monitoring requirements by providing centralized log analysis and event correlation features.

SECURITY MONITORING IN SOC ENVIRONMENTS

The Security Operations Center (SOC) is typically where the monitoring of security threats for an organization takes place. SOC teams monitor security events as they occur, identify potential threats, investigate alerts and anomalies and work with other teams to contain, remediate, and learn from security incidents.

Today's IT environments generate an enormous amount of security related data from a variety of sources, including Firewalls, Intrusion Detection Systems, Servers, Operating Systems /Traditional Network Devices, Applications and Endpoint Protection (EPP) or Endpoint Information Protection (EIP) environments. Monitoring and analysis of this information would be almost impossible to do manually.

Traditional SIEM systems solve this problem by collecting logs from different locations, normalizing them into a monitoring system and analyzing these events based on correlation rules and behavioral analysis in order to identify any potential security threats. The life cycle of a security alert in a SIEM monitoring environment begins when a monitored system generates an event. The SIEM system then captures the event and processes it against correlation rules defined by the security team. If a rule is tripped and the security team has defined an action for that rule, the SIEM generates an alert for an analyst to review for potential threats to the organization.

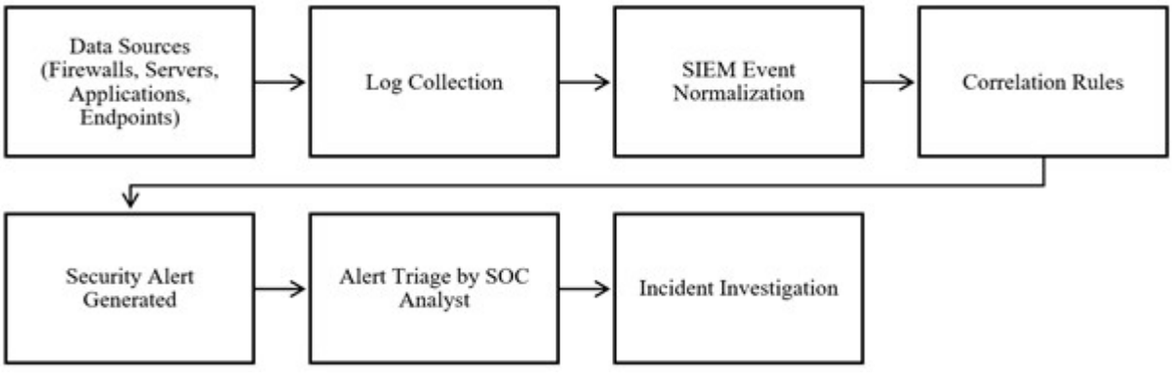

Figure 2. *Security alert lifecycle in a SIEM-based monitoring environment.*
Source: Adapted from Cichonski et al. (2012).

Within SOC environments, analysts also conduct alert triage. This process involves evaluating and prioritizing alerts based on their potential impact and the likelihood of indicating malicious activity. Analysts close alerts that are benign or irrelevant. However, they escalate alerts that are deemed suspicious for further investigation.

ARCHITECTURE OF SIEM MONITORING SYSTEMS

SIEM products are designed to employ a layered architecture to support the processing, analysis and monitoring of security events generated across an organisation's information infrastructure (Gonzalez-Granadillo, Gonzalez-Zarzosa & Diaz, 2021; Podzins & Ramanovs, 2023).

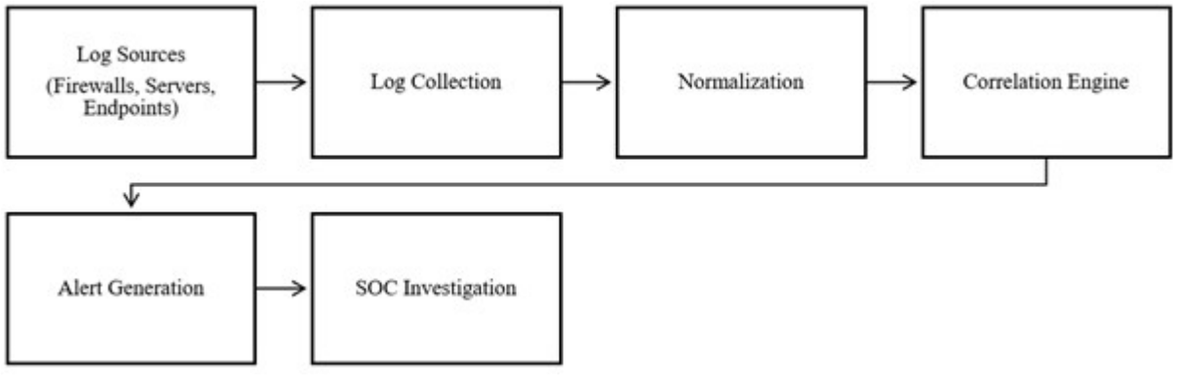

Figure 3. *Typical SIEM monitoring architecture*
Source: Author's conceptual model based on Gonzalez-Granadillo, Gonzalez-Zarzosa & Diaz (2021) and Podzins & Ramanovs (2023).

SIEM systems first capture data at the data collection layer, gathering logs from items such as network devices, servers, security firewalls, and applications. Typical log data includes information regarding login attempts, network activity, configuration changes, system errors and other security related activity.

A second layer of defence is event normalization and processing. Log data is often delivered in a variety of formats, from multiple systems, and must be normalized to facilitate analysis. Most SIEM systems perform this normalization automatically, allowing the defensive systems administrator to compare events from multiple

sources to recognize attack patterns. The correlation engine is a key component of any SIEM architecture. The correlation engine utilises the normalised events from the SIEM Architecture to analyse for potential security threats based on pre-defined correlation rules and behavioural analytics. Some security monitoring tools use correlation rules to detect more complex patterns of behaviour, such as repeated failure to authenticate, privilege escalation, unexpected communication between machines on a network, or processes running that look suspicious. Each pattern is set up as a correlation rule, and each match that the correlation rule detects generates an alert that needs to be investigated by staff in the SOC.

SIEM monitoring systems can transform log data into meaningful security information to aid in the detection and investigation of security incidents.

DISTINCTION BETWEEN ALERTS AND SECURITY INCIDENTS

In monitoring cybersecurity threats, there is often confusion between two critical, yet distinct, terms: “alerts” and “security incidents.” While both are essential aspects of threat detection and response, they represent different levels of analysis. Our monitoring tools and services issue alerts whenever certain rules are triggered or anomaly detection identifies unusual activity.

These alerts highlight suspicious activity such as repeated login failures, unusual network connections, changes to server configuration and other abnormal behaviour. However, just because you receive an alert does not necessarily mean there is an ongoing cybersecurity incident. Many of the alerts are a result of normal system behaviour, standard administrative actions, or other non-malicious events that only temporarily affect the organization’s network.

What constitutes a Security Incident? A security incident is a violation or threat of violation of computer security policies, acceptable use policies, or standard security practices - as documented in the NIST Computer Security Incident Handling Guide (Cichonski et al., 2012). In short form, a security incident is any malicious event – confirmed or suspected – that requires some sort of response.

In order to meet regulatory obligations, incident management procedures must understand the difference between incidents and alerts. As cyber monitoring capabilities continue to improve, the number of daily alerts can surge, but under the new NIS2 Directive, organisations are only required to report significant, more dangerous incidents. Therefore, organisations need to be able to establish procedures that allow them to triage and escalate the correct incidents to the right teams and authorities. This requires sufficient context with which to judge the severity of a given alert.

Correlation of events, historical system behaviour, threat intelligence, and other analytical techniques all play a role in helping SOC analysts decide whether any given SIEM alert actually represents a real problem, or just another edge case or otherwise benign event.

FALSE POSITIVES AND ALERT FATIGUE

Security Operations Centers (SOCs) face a significant problem from monitoring systems they are responsible for protecting - namely, the large volume of false positive alerts (Singer & Friedman, 2014). A false positive is a detection that incorrectly flags normal, legitimate activity as suspicious.

False positives can occur for a variety of reasons, including overly broad or poorly tuned detection rules, incomplete context, and misconfigured monitoring tools allowing normal system activity to generate alarms that are misinterpreted as anomalous behaviour.

A frequent problem in the industry is the high rates of false positives that lead to “alert fatigue”. In this scenario, the security analysts spend a significant amount of time reviewing unimportant logs, which in the end turn out to be benign. Over time, this can exhaust the security personnel, leading to less efficient monitoring processes and an increased likelihood of a severe incident going unnoticed (Singer & Friedman, 2014).

SIEM systems tackle the issue of noise in logs by implementing methods to reduce the number

of irrelevant alerts produced by monitoring systems. These approaches include techniques to tune rules, contextually enrich data, and perform behavioural analytics. Organizations can reduce alert noise by tuning correlation rules and detection thresholds. Contextual enrichment can also support better analyst decision-making. This might include information about the asset being attacked, information about normal behaviour for that user, or threat intelligence generated by third party providers.

Behavioural analytics tools also help decrease false positives by allowing security teams to set a baseline of normal behaviour for the organization. As a result, SIEM systems are better able to identify true anomalies of behaviour that may indicate potential security threats while minimizing the number of unnecessary alerts generated by typical organizational activity. Reducing false positives is key to keeping SOC analysts and their managers productive; let them focus on the anomalies that actually matter.

ALERT CORRELATION AND AGGREGATION

Event correlation, or the ability to identify connections between multiple events occurring across systems and times, is a core feature of SIEM systems. While traditional monitoring tools display individual events on screens for administrators to review, SIEM platforms analyze these occurrences for potential relationships.

Correlation techniques on the log data include analysis of source and destination IP addresses, user IDs, timestamps, event types etc. However, the correlation methods go a step further by grouping correlated events generated over a period of time together as a single alert generated by the SIEM platform, that could indicate a security incident.

For example, the combination of repeated authentication failures followed by an authenticated login from an atypical location could indicate a brute-force attack. Individually, these activity patterns may appear to be normal, yet collectively, they can indicate potentially malicious behaviour.

Event correlation in SIEM allows SOC analysts to identify complex attack patterns (different stages of malicious activity) and represent a flow of events as one investigation case (investigation), reducing the number of alerts for analysts to monitor and providing a clearer context of the situation.

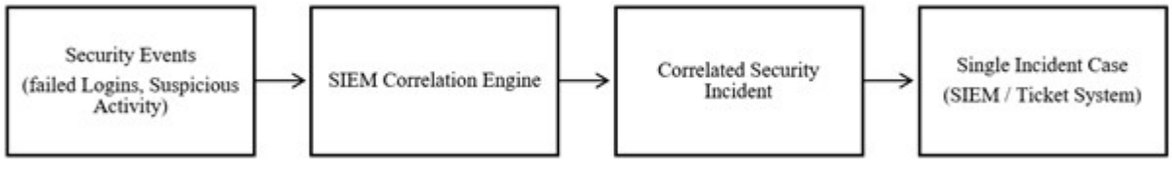

Figure 4. *Example of event correlation identifying a coordinated attack pattern.*
Source: Conceptual model based on SIEM correlation principles (Gonzalez-Granadillo, Gonzalez-Zarzosa & Diaz, 2021).

Through event correlation, SIEM systems help analysts spot coordinated attack campaigns. This allows them to focus their investigation efforts based on the seriousness and possible effects of the detected activities.

INCIDENT LIFECYCLE AND TICKET MANAGEMENT

As suspicious alerts are further investigated, they go through the incident lifecycle management process. Incident response

methods generally follow a process that includes detection, analysis, containment, eradication, and recovery (Cichonski et al., 2012).

The detection phase is the point at which monitoring tools find potential threats. Analysis occurs when a security analyst inspects each detected threat to assess whether or not actual damage occurred. Once an incident has been confirmed, efforts are made to contain the activity in order to prevent further harm. This involves actions to limit the spread of the activity and isolate systems that may be affected. Analysts may also block connections to known malicious sources and freeze or reset compromised accounts.

Containment, eradication, and recovery: after containing an incident, system administrators remove any remaining portions of malware or other incident components (eradication) before allowing the systems to return to service (recovery). In this phase, system administrators address any weaknesses in the environment that the incident exploited.

Evidence must be maintained through the whole lifecycle. Companies have to keep evidence of investigation steps, system logs, and remediation efforts to track incidents internally and for compliance reports.

Many SIEM offerings integrate with ticket management/case management offerings, which allow analysts to track the progression of an incident and assign out work to be investigated. This type of feature ensures that incidents are being investigated in an organized manner and also allows for appropriate documentation of work being performed to address an incident.

SIEM platforms may also integrate with ticket management tools to support collaboration between security teams and IT operations teams during incident response.

AUTOMATION AND ROOT CAUSE CORRELATION

Automation plays a critical role in cybersecurity monitoring. Due to the elevated number of security events generated by today's infrastructures, it has become beyond the capacity of analysts to manually analyse each event in a timely manner (Akbari et al., 2025).

SIEM systems typically include built-in automation capabilities that allow analysts to increase the scope of alert processing through automation. Many systems include functions that support automation of alert enrichment with data sources and threat intelligence services, as well as automated ticket creation for alerts. Through automation, analysts are able to complement manually collected data with additional information to improve alert understanding.

Another benefit of automation is identifying incidents that are caused by the same threat actor or vulnerability. In today's complex IT environment, one attack can trigger several alerts on different systems and without automation and correlation tools, these would be treated as separate incidents by the analyst, increasing their workload.

By identifying common indicators between alerts, such as IP addresses, usernames, malware, or attack patterns, SIEM systems can aggregate related alerts into one investigation case. This allows for the identification of related attack patterns and for the analyst to gain a full view of the scope of the attacks occurring.

Automation in threat analysis tools helps to improve efficiency by taking some manual processes out of the equation and enables the analyst to work on more in-depth analysis.

CONTRIBUTION TO NIS2 COMPLIANCE

SIEM systems are capable of meeting several of the operational requirements set out in the NIS2 Directive, in particular those related to the continuous monitoring of information systems and the detection and reporting of security incidents. Their value is, however, only fully understood when considered in the context of the specific requirements of the legislation and not in isolation from the pertinent organisational functions.

Cybersecurity obligations are laid out in Article 21 of the NIS2 Directive, requiring organizations to implement appropriate technical and

organizational measures for ensuring the processing of information, in particular with a view to safeguarding and restoring the reliability of information-processing services in case of physical or logical dangers to the information-security infrastructure after events endangering information security have occurred ("resilience") and to "effectively monitor information-security incidents and, where relevant, notify and work with other organisations and authorities, including other actors at national, European and international level, on handling such incidents. The monitoring of computer security incidents is often supported by a Security Information and Event Management system (SIEM), which provides comprehensive visibility on computer and network activity. By aggregating and normalising log messages from all relevant data sources, a SIEM system enables organisations to continuously monitor their infrastructure, identify anomalies in activity, and respond appropriately.

SIEM platforms in use by enterprise organisations support their obligation to report incidents as laid out in Article 23. These notifications need to be made within strict timeframes, including an early warning alert within 24 hours, an incident update within 72 hours, and a full report no later than one month from the discovery of a possible security breach. To meet these obligations, the organisation must be able to quickly determine whether a security incident is in fact occurring, assess the risk, and then log and report accordingly.

In order to generate appropriate regulatory reports and prove compliance to regulatory bodies, during audits, security and investigative activities must be tracked and logged. Many SIEM products can provide valuable support to the security analyst in this respect, by capturing and preserving data from various sources in structured forms of records such as log, correlated event, actions taken by analyst, and timestamps of each step involved in the whole process of investigation.

In addition to these new obligations, the management of incidents in large, complex organisations will require them to maintain a record of traceability and accountability throughout the entire lifecycle of the incident. SIEM-integrated case management and ticketing systems can assist in maintaining a record of key decisions, escalations and actions throughout the entire process. Such records will be essential in reconstructing the evolution of an incident and in providing evidence of adequate procedures for its management.

SIEM technology can therefore be only part of the puzzle to ensure compliance with NIS2. Moreover, having the technology in place is just the first step. Adequate operation procedures and trained staff also need to be in place. In order to meet these requirements adequate governance, to manage the reporting obligations of the organization and procedures to ensure adequate and timely action, need to be defined and put in practice by the management and technical teams of the organization.

We repeat, SIEM systems are there to enable larger security and privacy ecosystems. They can help with collecting and analysing data, ensuring that proper evidence and an audit trail is being created, and in general enable proper monitoring and reporting in line with the NIS2 Directive obligations of the various stakeholders.

CONCLUSION

Cyber criminals are becoming increasingly sophisticated and to combat this organisations require a monitoring solution that can process large amounts of security information and flag potential security incidents in real time.

Security Information and Event Management (SIEM) platforms provide organizations with vital tools to gather, correlate, monitor, manage alarms and conduct forensic investigations. Security intelligence produced by these systems enables organizations to turn raw security events into meaningful organization-wide intelligence that facilitates effective activity.

SIEM systems make analysts' jobs easier by enabling them to tell true security incidents from normal events. This makes monitoring more effective and helps mitigate problems associated with false alarms and alert fatigue.

Many of these features also support the

structured documentation and monitoring that the NIS2 Directive requires, as well as continuous reporting to relevant bodies.

This paper presents a conceptual analysis of the processes of SIEM monitoring and explores the possibilities and challenges associated with each process. The study is purely theoretical in nature and no real SOC environment was monitored for data. Future research could, however, simulate a monitoring process and gather data in real SOC environments, in order to also study how correlation and automation are actually handled in practice by complex monitoring systems.

As cyber threats continue to evolve, organisations will increasingly rely on monitoring technologies, automation and an integrated approach to incident response.

REFERENCE LIST

Akbari, M., Nitz, L., Bregar, A., Popanda, J., Siemers, C., Matzutt, R. & Mandal, A. (2025) Requirements for a playbook-assisted cyber incident response, reporting and automation. *Journal of Cybersecurity*. [Online first]. doi: 10.1093/cybsec/tyaf001

Singer, P.W. & Friedman, A. (2014) *Cybersecurity and cyberwar: what everyone needs to know.* New York: Oxford University Press.

CERT-EU. (2024) *Threat landscape – year in review.* Brussels: Computer Emergency Response Team for the EU institutions.

Cichonski, P., Millar, T., Grance, T. & Scarfone, K. (2012) *Computer security incident handling guide (NIST SP 800-61 Revision 2).* Gaithersburg: National Institute of Standards and Technology.

ENISA. (2023) *ENISA threat landscape – health sector.* Athens: European Union Agency for Cybersecurity.

ENISA. (2024) *ENISA threat landscape 2024*. Athens: European Union Agency for Cybersecurity.

ENISA (2025) *NIS2 technical implementation guidance.* Athens: European Union Agency for Cybersecurity.

European Commission. (2023) *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).* Official Journal of the European Union.

Gonzalez-Granadillo, G., Gonzalez-Zarzosa, S. & Diaz, R. (2021) Security Information and Event Management (SIEM): Analysis, trends and usage in critical infrastructures. *Sensors*, 21(14).

Jangampet, V.D. (2022) AI-driven SIEM user experience for enhanced cybersecurity decision-making. *International Journal of Information Security Science*, 11(3).

Lunter, L. (2025) *Simplify your path to NIS2 compliance with log management and SIEM.* [Blog post] Available at: https://logmanager.com/blog/it-compliance/nis2-compliance-log-management-siem/ [Accessed: 24th April 2026].

Menaa, A., Parry, J. & Roest, J. (2023) *NIS2 compliance readiness for organizations across the European Union.* Brussels: Cybersecurity Policy Institute.

MITRE. (2024) *MITRE ATT&CK Framework*. Available at: https://attack.mitre.org [Accessed: 10th March 2026].

Podzins, O. & Ramanovs, A., 2023. Why SIEM is essential in modern cybersecurity monitoring environments. *Information Technology and Management Science*, 26(1).

Scarfone, K. & Mell, P. (2007) *Guide to intrusion detection and prevention systems.* Gaithersburg: National Institute of Standards and Technology.