NIS 2 REPORTING OBLIGATIONS: Achieving compliance with a SIEM

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

Abstract: This paper examines how organizations can meet the reporting obligations imposed by the **NIS 2 Directive (EU 2022/2555)** through the deployment of Security Information and Event Management (SIEM) capabilities. Using a qualitative comparative analysis of the Directive's requirements and current operational guidance, complemented by sector-specific evidence from the energy and healthcare domains, the study identifies how real-time monitoring, structured logging, and staged notifications support compliance with **Articles 21 and 23** of the Directive. The analysis draws on the legal text of NIS 2 (European Commission, 2023) and recent guidance and threat-landscape reporting from **ENISA (2024; 2025)** and **CERT-EU (2024)** to demonstrate how SIEM-enabled detection, consolidation of evidence, and audit-ready reporting align with the Directive's early-warning (24 hours), incident-notification (72 hours), and final-report (one month) requirements. The paper contributes a practical mapping between regulatory obligations and technical processes that organizations can replicate across essential and important entities.
Keywords: SIEM, NIS 2 Directive, Cybersecurity, Cyber risk, Incident reporting, Security measure, ENISA, EU Regulation.

INTRODUCTION

Since the adoption of the **NIS 2 Directive (EU 2022/2555)**, cybersecurity has become an operational requirement for essential and important entities across the European Union. **Article 23** establishes a multi-stage reporting process—an *early warning within 24 hours*, an *incident notification within 72 hours,* and *a final report within one month*—designed to improve the speed and quality of the cross-border incident coordination (European Commission, 2023). Compliance therefore depends not only on the governance structures but also on the technical systems capable of rapid detection, evidence retention, and standardized reporting.

While the Directive and related commentaries explain the regulatory obligations, fewer studies address how technical tools such as SIEM platforms can operationalize compliance. This paper closes that gap by analysing how SIEM functions—centralized log collection, correlation, alerting, forensic retention, and standardized report export—map to the Directive's duties for risk management (**Article 21**) and incident reporting (**Article 23**) using **ENISA (2025)** and **CERT-EU (2024)** guidance as benchmarks.

https://doi.org/10.54851/v7i2y202501

The novelty of this research lies in integrating the legal interpretation with the operational implementation scenarios derived from the verified ENISA sectoral reports. The paper bridges the normative cybersecurity policy and applied cyber-operations, providing both a conceptual framework and practical guidance for achieving compliance across sectors (ENISA, 2024).

NIS 2 DIRECTIVE

The NIS 2 directive is a regulation of the European Union whose purpose is to strengthen the level of cybersecurity for critical infrastructures in the member states of the European Union.

To conduct that aim, NIS 2 directive is based on 3 fundamental pillars:

- **Strategic cooperation** from the exchange of cybersecurity information between entities.
- **Development of national strategies** aimed at improving the cybersecurity across the region; and
- **Key sectors of activity** - the scope is extended from the seven initial sectors provided by NIS 1 directive, adding eight more sectors, reaching a total of fifteen. The following sectors of activity are targeted: energy, health, transport, banking, water supply, digital infrastructure, public administration, digital service providers, postal and courier services, waste management, space, food production and distribution, manufacturing and distribution of chemicals, research and manufacturing.

Article 21 of the directive requires that essential organizations implement proper technical, operational, and organizational measures to manage risks to the security of the networks and information systems. The organizations must adopt an approach that considers all risks so that they are prepared to face a wide range of security incidents, as well as being capable of protecting the networks and information systems.

In addition, **Article 23** of the directive clearly defines what constitutes a significant incident and describes the reporting obligations that the organizations must follow. It also requires a single point of contact to give a quarterly summary report having anonymized, aggregated data on significant incidents, general incidents, cyber threats and near misses.

The implementation of this directive in Romania was conducted through the Government Emergency Ordinance 155/2024, respectively through Law no. 124 of July 7, 2025, for the approval of the Government Emergency Ordinance no. 155/2024 on the establishment of a framework for the cybersecurity of networks and information systems in the national civil cyberspace.

REPORTING OBLIGATIONS

Definition of incident

In NIS 1, an incident is defined as any event having an actual adverse effect on the security of the network and information systems, meaning harm must have already occurred. NIS 2 expands this to cover any event compromising the availability, authenticity, integrity, or confidentiality of the stored, transmitted, or processed data, or the related services. This new definition includes actual damage and events that could degrade or threaten these security dimensions.

Reporting incidents

In NIS 1, reporting is mandatory only for significant incidents where harm has materialized and continuity of the service is affected. NIS 2 moves beyond this, requiring reports for incidents that have caused or have the potential to cause operational disruption or financial losses, as well as those that have affected or could affect other people by causing considerable losses. This means a potential harm and its impact on third parties now play a key role in figuring out reporting obligations.

Reporting obligations of cyber threats

The NIS 1 directive does not require reporting cyber threats, but NIS 2 introduces the obligations to share information on significant threats, including those that have not yet caused an incident. This must be accompanied by measures or remedies to mitigate the risk.

	NIS Directive	European Commission NIS 2 Proposal	Parliament Draft Resolution	Council General Approach	NIS 2 Directive
Definition of incident	'any event having an actual adverse effect on the security of' NIS	'any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via,' NIS		'an(y) event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via,' NIS	
Reporting of incidents	Significant (OES)/substantial (DSPs) impact: harm must have materialised since effect on the continuity of the service required	Significant impact on the provision of services: incidents that • have caused/the potential to cause operational disruption or financial losses • have affected/the potential to affect other persons by causing considerable losses	Parameters to consider when determining the significance enlisted in Art. 20(3) incl. inter alia number of recipeents of the services, incident duration	Similar to NIS 2 Proposal	
Reporting of cyber threats	No	Yes, if cyber threat is significant	No, but information of service recipients of 'incidents and known risks' and measures or remedies to take	No, but information of service recipients of significant cyber threat and measures or remedies to take	

Figure 1: *Evolution of the reporting obligations from NIS 1 to NIS 2*

Source: Schmits-Berndt, S., Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive.

Although the EU Commission, Parliament and Council each have their own distinct perspectives, the overall direction shows a rise in initiative-taking reporting alongside a broader interpretation of what constitutes incidents and cyber threats.

THE ROLE OF A SIEM IN AN ORGANIZATION

What is a SIEM?

SIEM stands for a technological approach that obtains, combines and assesses log data coming from a range of IT infrastructures, security tools and software used within an enterprise. Its main aim is to offer a single point of insight into security occurrences and possible risks, empowering enterprises to identify, examine and react to security breaches in an effective manner (Podzisn & Ramanovs, 2023).

Notable purposes of a SIEM:

- **Centralized log collecting and correlation -** SIEM gathers log data from many sources, including firewalls, antivirus software, servers, programs and network devices, then correlates these data to find anomalies or trends that could point to security issues (Gonzalez-Granadillo et al.).
- **Real-time threat detection -** By continuously monitoring the IT configuration, SIEM can find any suspicious behavior, including malware breakouts, forbidden access attempts, or unanticipated user activities.
- **Advanced incident response -** SIEM can automate specific threat responses, like warning system managers, setting off firewall rules, or quarantining affected devices, thereby speeding up the reduction and decreasing the damage caused by security events.
- **Regulatory compliance and reporting -** SIEM gives a hand to enterprises in sticking to security rules by keeping up thorough records, making reports and backing up audit needs, all of which are vital for control and handling risks.
- **Enhanced situational awareness -** By showing security details in a way that gives context and brings all together, SIEM lets security teams get a full picture of the IT world within the enterprise, which sharpens up how choices are made and how plans are formed.

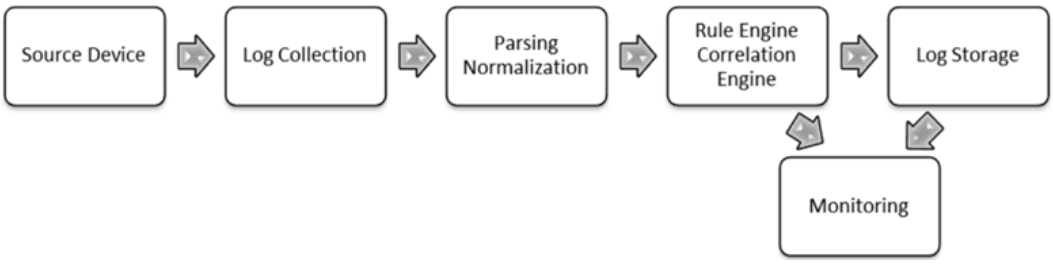

Figure 2: *SIEM basic components*

Source: Gonzalez-Granadillo, G., Gonzalez-Zarzosa, S. & Diaz, R., Security Information and Event Management (SIEM): Analysis, Trends and Usage in Critical Infrastructures.

Limitations of SIEMs

Due to financial limitations, as well as compliance and privacy constraints, SIEMs always function with a fundamentally incomplete picture. This operates with fragmented user identities, shared accounts and missing logs, resulting in low correlation capabilities and high false positive and false negative rates.

In the SIEM context, there are also storage challenges. Archived data are mostly underused, retention periods are short and not long enough to check advanced threats over time. Even though cloud storage theoretically could overcome these challenges, the confidentiality issues of cloud storage mean it is rarely used.

While automation is often said to be a benefit, it's not as great as some think. Most platforms still need heavy involvement from humans to find what a threat is, what countermeasures should be used and what actions should be taken to rollback or contain the event.

The future of SIEMs

The SIEM platform is in a substantial change, which is being driven by a wide range of external forces that go well beyond technology itself. Political, economic, social, technological and environmental pressures are each exerting a profound influence on the way the SIEM systems are evolving.

Politically, the administrations are stepping up investments in the cybersecurity infrastructure and promoting collaborations between the government and private sectors, which is contributing to propelling the adoption of sophisticated SIEM solutions.

Technologically, the emergence of the cloud computing and mobile technology has significantly boosted the pace and complexity of the data that the SIEM systems must process.

Socially, the increased volume of personal and organizational data online has raised the risk of cyber threats. The potential for attacks has grown as several data become available and accessible.

From an economic standpoint, the rise in flexible work arrangements and economic growth has introduced new challenges. Now the SIEM systems must support a wider variety of users and devices, many of which are not covered by traditional IT setups.

Additionally, environmental factors such as the growth of the Internet of Things have led to more vulnerable endpoints. The challenge of efficiently gathering, organizing and analyzing this rapidly growing number of data sources is both essential and complicated.

Potential of the future SIEMs

SIEMs have emerged as prime operators within the modern IT infrastructures because they perform automated threat detection and response. Still, the role of these SIEMs turns appropriately limited in the cases where we are speaking about critical infrastructure, because of the human analyst it is necessary to draw

fine distinctions around security incidents and determine the proper countermeasures.

Another major line of approach opportunities exists for the integration of the multiple complementary security mechanisms. Instead of relying on a single line of defense, the next-generation SIEMs should therefore include layered security approaches.

The conception subsequently leads to the establishment of new security metrics, based on a quantitative and probabilistic analysis for the rigorous evaluation of the interactions and aggregate effects of various defense strategies on the overall system resilience.

The SIEM systems with artificial intelligence are a pivotal development in cybersecurity, offering enhanced visibility and faster response for organizations. Whereas the legacy systems are rule-driven systems with a lot of predefined rules which will trigger hundreds of alarms, an AI based platform can set up a baseline on behavior and tag an anomaly if it may be suspicious. Combined with the predictive and adaptive analytics, the AI-powered SIEM enables a quicker, more intelligent decision-making and leads to a proactive threat management approach, turning the SIEM into a proactive cyber security resilience.

Figure 3: *Components of AI-Driven SIEM*

Source: Jangampet, V.D., n.d. The rise of the machines: AI-driven SIEM user experience for enhanced decision-making.

Another important area of improvement in different implementations would be the use of OSINT. An advanced SIEM should look for greater flexibility than mere keyword searches with the extraction of some contextual information like geography or an implicated entity to enrich the investigative options of the analysts.

SIEM SYSTEMS IN CRITICAL INFRASTRUCTURES

The critical infrastructure lays the very basis for the public safety and national security. Those sectors depend on the industrial control systems and supervisory control and the data acquisition (SCADA) systems that were initially designed for operational continuity rather than cybersecurity.

Most of these systems serve as legacy environments today: they are outdated, disruptive to patch and intrinsically vulnerable. Common protection methods such as firewalls and network segmentation can cause complacency in system administrators and security officers, giving to the threat actors, in most cases, the ability to exploit the connectivity between the enterprise and the industrial networks to move laterally.

Protecting these major environments is quite a complex task. Commonplace, if similar, the IT mechanisms employed disrespectfully can disturb or even close industrial operations, while the administrators are bound by analyzing huge data incidentally and event collating data on point to find the potentially emerging threats.

SIEM provide centralized monitoring and correlation, though no present system can claim to catch each attack ever faced. The fast growth of the SIEM has seen modern architectures with advanced analytics, alerting with applied context and real-time visibility cross multiple layers of the infrastructure, hence making it an increasingly critical issue for the critical infrastructure security.

The health sector has increased the amount of its exposure to electronic records, cloud services and networked medical devices

(ENISA, 2023). Real-time analytics, scalable log management, compliance reporting and unified dashboards provided by the SIEM systems help this kind of setting to meet the standards of different regulatory frameworks such as HIPAA.

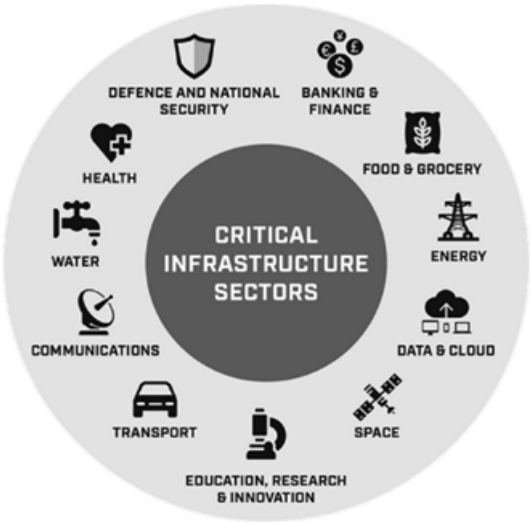

Figure 4: *Critical infrastructures sectors*

Source: Berdibayev, R., Gnatyuk, S., Yevchenko, Y. & Kishchenko, V., 2021. A concept of the architecture and creation for SIEM system in critical infrastructure.

Since the energy sector presents an exceptionally large attack surface and threats that keep getting more sophisticated by the day, the SIEM systems find a significant use there, too. They can detect anything ranging from denial-of-service attacks to GPS signal anomalies, theretofore affording operators time to act before the incidents could occur. The situational awareness remains much less than complete and an all-inclusive defense in depth is still a work in progress (ENISA, 2024).

Transportation, with digitalization moving full speed ahead, presents new vulnerabilities threatening both the data integrity and physical operations, from ransomware to disruptions of the service. The SIEMs can help prevent, detect and respond to such issues, while providing an avenue for organizations to strategize long-term cybersecurity implementation, thereby raising staff awareness and ensuring that policies are enforced.

The financial sector has a couple of challenges such as the risk of scaling of the cloud adoption, the need for regulatory compliance and the threat of insiders. The incident analysis is further complicated by inconsistent reporting formats.

However, solutions like the SIEM alleviate the problem by automating the reporting process, lowering the number of false positives and increasing the visibility of security events, which in turn enhances the organization's resilience.

METHODOLOGY

This study employs a **qualitative comparative analysis** using three evidence streams:

1. **Document analysis.**
   Examination of the **Directive (EU) 2022/2555,** with focus on **Articles 21 and 23**, and the European Commission's explanatory material on the staged reporting model (European Commission, 2023).
2. **Operational guidance mapping.**
   Review of **ENISA's NIS2 Technical Implementation Guidance (ENISA, 2025),** which provides actionable examples for demonstrating the cybersecurity risk-management measures, together with the **ENISA (2024)** *Threat Landscape Report* and the **CERT-EU (2024)** *Threat Landscape Year* in Review.
3. **Sectoral evidence.**
   Analysis of **ENISA's (2023)** *Health Threat Landscape* and the public summary of **ENISA's (2024)** *Cyber Europe* exercise for the energy sector. These sources identify sector-specific detection and reporting challenges relevant to NIS 2 compliance.

Each NIS 2 reporting requirement was then mapped to SIEM-supported processes (event normalization, correlation, alerting thresholds, evidence retention, and reporting workflows). Only the information traceable to the cited institutional or legal sources was included (Akbari Gurabi et al., 2025).

RESULTS AND CASE STUDIES

Case 1: Energy Sector (ENISA, 2024)

The ENISA (2024) Cyber Europe Energy Exercise Summary highlights the importance of the consolidated logging and cross-border information exchange for an early warning and a coordinated incident response. While it does not assess specific products, the report shows that centralized event correlation and standardized templates—capabilities typical of the SIEM solutions—are essential for meeting the Directive's 24-hour and 72-hour reporting stages (European Commission, 2023).

Implication: The energy operators can align the SIEM alert taxonomies with the Article 23 criteria and pre-populate notification templates to improve both the timeliness and completeness of their reports.

Case 2: Healthcare Sector (ENISA, 2023)

The ENISA (2023) Health Threat Landscape found that the healthcare organizations remain disproportionately targeted by the ransomware and data-breach incidents, often involving the connected medical devices. The centralized monitoring and log correlation across the IT and IoT environments enhance anomaly detection and enable the production of the audit-ready evidence (ENISA, 2023).

Implication: By mapping the recurring threat patterns to the SIEM correlation rules and automated reporting fields, the healthcare entities can prepare structured early-warning and incident-notification reports consistent with NIS 2 Article 23.

Both sectors demonstrate that the technology supports compliance when the SIEM processes are explicitly aligned with the Directive's legal definitions of significant incident, early warning, and notification.

ACHIEVING NIS 2 COMPLIANCE BY IMPLEMENTING A SIEM

The NIS 2 instruction specifies that, particularly those in important industries running within the borders of the European Union must improve their cybersecurity measures. Following the requirements of the NIS 2 directive depends on the deployment of the SIEM systems among other important actions. Meeting several significant needs specified in the directive depends critically on these systems.

As outlined in **Article 21,** NIS 2 emphasizes the need for logging operational and security-related activities (European Commission, 2023). The SIEM systems merge data from various parts of a company into one centralized location for analysis and collection. The organizations guarantee the access to all the needed data for monitoring, auditing, and reporting purposes by combining this information, therefore helping to spot and fix the cybersecurity issues (Lunter, 2025).

Article 21 of NIS 2 stresses the need for businesses to swiftly identify and manage the cyber events. With real-time surveillance and alert capabilities, the SIEM solutions enhance an organization's ability to spot the possible threats. The SIEM systems enable the correct detection of the unusual activities and potential security breaches by combining data from multiple sources, thereby enabling the fast incident resolution and reaction.

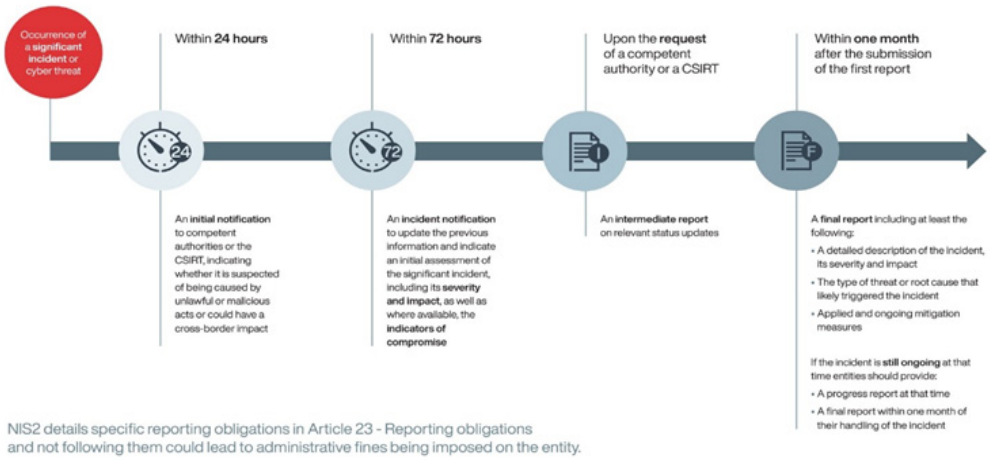

Figure 5: *Timeline in case of a significant incident or cyber threat*

Source: (Menaa, A., Parry, J. & Roest, J., NIS2 Compliance Readiness for Organizations across the European Union)

Article 23 of NIS 2 specifies that businesses should report major cybersecurity incidents within one day of discovery to their national authorities (European Commission, 2023). The first report should clearly describe the event and its consequences. By offering thorough logs and reports that record the event's characteristics, effects and the steps used to resolve it, the SIEM systems help to meet this requirement. Keeping these records is essential to meet the reporting time limits and help the regulatory organizations with their evaluations.

Including real-time reporting capabilities, a SIEM system offers companies the tools needed to comply with NIS 2, hence lowering the chances of penalties and reputational harm amongst consumers and the public (Perkola, 2025).

NIS 2 challenges companies to use a cybersecurity plan founded on risk analysis, which entails ongoing monitoring and refinement of their security mechanisms. The SIEM systems help in this effort by giving an understanding of security patterns, finding continuous weaknesses and assessing how effective the current protective measures are. These facts encourage educated decisions meant to strengthen the security system of the company.

CONCLUSION

The evidence from verified EU sources confirms that the **SIEM capabilities**—centralized logging, correlation, alerting, retention, and exportable reporting—directly support the compliance with the **NIS 2 Directive's Articles 21 and 23.** ENISA's operational guidance and sector exercises show that such capabilities strengthen incident visibility and facilitate timely notifications, reducing administrative overhead and improving data quality.

The paper contributes a **compliance-mapping framework** linking the regulatory requirements to the implementable technical measures. Future research should evaluate the efficiency gains quantitatively and explore the **standardized SIEM reporting templates** to enhance the interoperability among the national authorities in the EU (Rotin & Landeka, 2025).

For the entities striving to achieve the compliance with the NIS 2 Directive, putting in place a SIEM system is essential, offering a structure for overseeing cybersecurity dangers that align with the needed rules. SIEM, by making unified logging easier, sees to it that all noteworthy security events across networks, systems, and applications are steadily gathered

and kept, building a one-stop place for keeping watch and checking things. This unified way not just makes it simpler to stick to NIS 2 paperwork and proof rules but also makes possible dangers more visible.

SIEM systems give entities the power to spot unusual goings-on and possible security fails right as they occur, thanks to better ways of finding and dealing with incidents. The security groups can discover difficult dangers by connecting data from many places, act fast, and make the effects of an event less severe, which meets NIS 2 directive calls for fast danger lessening and solid risk handling.

Furthermore, the SIEM systems make it easier to get reports done, smoothing the way for getting ready and turning in necessary updates to country-level groups. They offer full, structured, and checkable logs of events, like what kind of danger it was, what things were hit, and what was done to fix it, making sure groups hit NIS 2 deadlines and back up being open about their security steps.

SIEM pushes for always getting better and making choices based on risk by looking at the old and live data to find repeating weak spots, judge how well the security measures work, and guide wise security spending. Because of this, the organizations can not only keep up with NIS 2 but also change their security approach in a forward-thinking way, cutting down on how likely and how bad future events might be.

REFERENCE LIST

Akbari Gurabi, M., Nitz, L., Bregar, A., Popanda, J., Siemers, C., Matzutt, R. & Mandal, A. (n.d.) *Requirements for a Playbook-Assisted Cyber Incident Response, Reporting and Automation.* [Accessed 13th August 2025]

Berdibayev, R., Gnatyuk, S., Yevchenko, Y. & Kishchenko, V. (n.d.) *A concept of the architecture and creation for SIEM system in critical infrastructure* [Accessed 19th August 2025].

CERT-EU. (2024) Threat Landscape 2024 – Year in Review. [online] *European Union Computer Emergency Response Team.* Available at: https://cert.europa.eu [Accessed 10th October 2025].

ENISA. (2023) Health Threat Landscape 2023. [online] *European Union Agency for Cybersecurity.* Available at: https://www.enisa.europa.eu/publications/health-threat-landscape-2023 [Accessed 10 Oct 2025].

ENISA. (2024) Cyber Europe 2024 – Energy Sector Exercise Summary. [online] *European Union Agency for Cybersecurity.* Available at: https://www.enisa.europa.eu [Accessed 10th October 2025].

ENISA. (2024) ENISA Threat Landscape 2024. [online] *European Union Agency for Cybersecurity.* Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 [Accessed 10 Oct 2025].

ENISA. (2025) NIS2 Technical Implementation Guidance. [online] *European Union Agency for Cybersecurity.* Available at: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance [Accessed 10th October 2025].

European Commission. (2023) Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). *Official Journal of the European Union*, L 333/80. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555 [Accessed 10th October 2025].

Gonzalez-Granadillo, G., Gonzalez-Zarzosa, S. & Diaz, R. (n.d.) *Security Information and Event Management (SIEM): Analysis, Trends and Usage in Critical Infrastructures* [Accessed 13th August 2025].

Jangampet, V.D. (n.d.) *The rise of the machines: AI-driven SIEM user experience for enhanced decision-making* [Accessed 20th August 2025].

Menaa, A., Parry, J. & Roest, J.(n.d.) *NIS2 Compliance Readiness for Organizations across the European Union* [Accessed 19th August 2025].

Lunter, L. (n.d.) *Simplify Your Path to NIS2 Compliance with Log Management and SIEM* [Accessed 13th August 2025].

Perkola, P. (n.d.) *Preparing for NIS2 directive reporting obligations with ISO 27001* [Accessed 13th August 2025].

Podzisn, O. & Ramanovs, A.(n.d.) *Why SIEM is Irreplaceable in a Secure IT Environment?* [Accessed 13th August 2025].

Rotin, T. & Landeka, K.(n.d.) *Application of the NI 2 Directive and the Cybersecurity Act in Essential and Important Entities* [Accessed 13th August 2025].

Schmits-Berndt, S.(n.d.) *Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive* [Accessed 13th August 2025].