

Optimising Threat Intelligence Integration for Real-Time Security Operation Centre Incident Response

Sharvinthsai Rau Muniandy*, Rozilawati Razali

Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Malaysia

*Corresponding author: Sharvinthsai Rau Muniandy (e-mail: p141367@siswa.ukm.edu.my)

ABSTRACT

The increasing sophistication of cyber threats has placed significant pressure on modern Security Operations Centres (SOCs) to detect, analyse, and respond to incidents in a timely manner. Despite substantial investments in security technologies such as Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Threat Intelligence (TI) platforms, many organisations continue to experience operational challenges including alert fatigue, fragmented security tools, limited contextual awareness, and analyst burnout. These challenges often reduce the effectiveness of incident response and hinder the overall performance of SOC operations. This study investigates how Threat Intelligence can be more effectively integrated within SOC environments to improve real-time detection and response capabilities. Guided by the MITRE ATT&CK framework and the NIST Cybersecurity Framework, the study proposes a conceptual SOC back-end architecture that integrates SIEM, XDR, and Threat Intelligence platforms into a unified intelligence-driven workflow. A qualitative research approach was adopted, combining an extensive literature review with expert validation involving cybersecurity practitioners experienced in SOC operations. The findings indicate that effective Threat Intelligence integration enhances alert prioritisation, improves situational awareness, reduces operational complexity, and supports faster incident response. The study contributes a practical framework for intelligence-driven SOC operations and provides recommendations for organizations seeking to strengthen their cyber defence capabilities.

Keywords: Security Operations Centre (SOC), Threat Intelligence, Incident Response.

INTRODUCTION

The rapid expansion of digital technologies, cloud computing environments, and interconnected infrastructures has fundamentally transformed the cybersecurity landscape. While these technological advancements have enabled greater organisational efficiency and innovation, they have simultaneously expanded the attack surface available to cyber adversaries. Modern threat actors increasingly employ sophisticated techniques such as advanced persistent threats (APTs), ransomware campaigns, zero-day exploits, and supply chain attacks that often evade traditional perimeter-based security controls (CrowdStrike, 2024; ENISA, 2024). Consequently, organisations are under increasing pressure to strengthen their cybersecurity capabilities and improve their ability to detect and respond to emerging threats.

Security Operations Centres (SOCs) have become a critical component of organisational cybersecurity strategies by providing centralised capabilities for security monitoring, threat detection, incident investigation, and response coordination (SANS Institute, 2024). However, contemporary SOCs face significant operational challenges arising from the growing volume and complexity of security telemetry generated across enterprise environments. Analysts are frequently required to process thousands of security alerts daily, many of which are false positives or low-priority events. This situation contributes to alert fatigue, cognitive overload, and reduced detection effectiveness (SANS Institute, 2024; Ponemon Institute, 2023).

In addition to alert overload, many organisations continue to operate security technologies in isolation, resulting in fragmented visibility and inefficient workflows. Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Threat Intelligence (TI) platforms often lack seamless interoperability, requiring analysts to

manually correlate information from multiple sources (Palo Alto Networks, 2023; Gartner, 2023). Without adequate contextual intelligence, distinguishing genuine threats from benign activities becomes increasingly difficult, leading to delayed incident response and increased operational risk (Recorded Future, 2023).

Threat Intelligence has emerged as a critical capability for addressing these challenges by providing contextual information regarding indicators of compromise (IOCs), adversary infrastructure, and attack methodologies. When integrated effectively with SOC technologies, Threat Intelligence can enhance detection accuracy, improve alert prioritization, and support proactive threat hunting activities (Recorded Future, 2023; Ahmad, Shah & Khan, 2022). Nevertheless, organisations continue to face difficulties in operationalising Threat Intelligence across heterogeneous SOC environments. This study therefore investigates how Threat Intelligence can be optimised within modern SOC architectures to improve real-time threat detection and incident response, guided by the MITRE ATT&CK framework and the NIST Cybersecurity Framework (MITRE Corporation, n.d.; NIST, 2024).

RELATED WORK

The evolution of Security Operations Centres (SOCs) reflects a broader transition from reactive security monitoring toward intelligence-driven cyber defence. Early SOC implementations primarily focused on network monitoring and basic incident detection, whereas contemporary SOCs perform a broader range of functions, including threat hunting, digital forensics, compliance reporting, vulnerability management, and threat intelligence analysis (SANS Institute, 2024; Deloitte, 2023). This transformation has been driven by the increasing sophistication of cyber threats and the need for continuous monitoring across hybrid enterprise environments.

Despite these advancements, the literature consistently identifies alert fatigue as one of the most significant challenges affecting SOC performance. Analysts are often overwhelmed by the volume of security alerts generated by multiple monitoring systems, resulting in slower response times, reduced investigation quality, and an increased likelihood of overlooking critical threats (SANS Institute, 2024; Ponemon Institute, 2023). Studies conducted by the SANS Institute and Ponemon Institute highlight alert overload as a primary contributor to analyst burnout and operational inefficiencies within SOC environments (SANS Institute, 2024; Ponemon Institute, 2023).

Another major challenge is the existence of tool silos. Many security technologies operate independently, preventing effective information sharing and cross-platform correlation. This fragmentation limits situational awareness and requires analysts to manually investigate incidents across multiple interfaces, thereby increasing workload and delaying response activities (Palo Alto Networks, 2023; Ahmad, Shah & Khan, 2022). Recent developments in XDR platforms aim to address these issues by integrating telemetry from endpoints, networks, cloud environments, and identity systems into a unified detection and response framework (SentinelOne, 2024; Gartner, 2023).

Threat Intelligence has been widely recognised as an essential component of modern SOC operations because it provides contextual information that enhances detection and investigation activities. Threat Intelligence enables organisations to understand adversary motivations, infrastructure, and tactics, techniques, and procedures (TTPs), thereby supporting more informed security decisions (Recorded Future, 2023). Threat Intelligence is commonly categorised into strategic, operational, tactical, and technical intelligence, each serving different organisational objectives and stakeholders (Recorded Future, 2023; McMillan, 2022).

The MITRE ATT&CK framework has become one of the most widely adopted models for operationalising Threat Intelligence within SOC environments. By mapping adversary behaviours to standardised tactics and techniques, ATT&CK enables organisations to assess detection coverage, identify defensive gaps, and guide threat hunting activities (MITRE Corporation, n.d.). Similarly, the NIST Cybersecurity Framework provides structured guidance for integrating cybersecurity activities across the Identify, Protect, Detect, Respond, and Recover functions, thereby supporting continuous improvement of SOC capabilities (NIST, 2024).

Although existing studies acknowledge the benefits of Threat Intelligence integration, significant gaps remain in both academic and industry literature. Much of the current studies focus on the capabilities of individual technologies rather than on practical approaches for integrating SIEM, XDR, and Threat Intelligence platforms within a unified operational architecture (Palo Alto Networks, 2023; Ahmad, Shah & Khan, 2022). Furthermore, there remains limited empirical evidence demonstrating how Threat Intelligence integration affects operational metrics such as alert reduction, investigation efficiency, and analyst workload. These gaps highlight the need for a practical framework capable of supporting intelligence-driven SOC operations while addressing both technological and human factors.

METHODOLOGY

This study adopted a qualitative-dominant methodology aimed at developing and validating a conceptual framework for Threat Intelligence integration within modern SOC environments. Rather than implementing a live SOC infrastructure, the study focused on analysing existing knowledge, synthesizing best practices, and evaluating the proposed framework through expert assessment.

The research was conducted through four phases. The first phase involved an extensive review of academic and industry literature relating to SOC operations, Threat Intelligence, SIEM, XDR, and cybersecurity frameworks. Insights obtained during this phase were used to identify operational challenges and develop the conceptual framework. The second phase involved preliminary engagement with cybersecurity professionals to refine the identified requirements and ensure alignment with practical SOC challenges. The third phase focused on designing a SOC back-end architecture that integrated SIEM, XDR, and Threat Intelligence platforms. Finally, the proposed framework was validated through expert evaluation.

The validation process involved thirty cybersecurity professionals representing a range of operational and technical roles, including SOC analysts, incident responders, security engineers, team leaders, and security architects. Participants reviewed the proposed architecture and completed a structured questionnaire designed to assess the clarity, realism, completeness, and practical relevance of the framework. Responses were analysed using descriptive statistics and qualitative interpretation to evaluate the level of expert consensus.

RESULTS AND DISCUSSION

The proposed architecture adopts an integrated approach to security monitoring and incident response by combining multiple security technologies within a unified operational framework. Security telemetry originating from endpoints, servers, network devices, cloud platforms, and other enterprise systems serves as the primary source of data. These data streams are collected and normalised by the SIEM platform, which performs event correlation and generates alerts based on predefined detection rules.

The XDR layer provides deeper visibility into endpoint behaviour and enables the detection of advanced attack techniques that may not be observable through traditional log analysis alone. By monitoring process execution, file activity, user behaviour, and network interactions, the XDR platform contributes additional context to security investigations.

Threat Intelligence functions as an enrichment layer that provides information regarding malicious indicators, adversary infrastructure, attack campaigns, and known tactics and techniques. When security events generated by the SIEM or XDR platforms are enriched with intelligence data, analysts gain additional context that supports more accurate prioritization and faster decision-making. This integration enables security teams to correlate internal observations with external threat information, thereby improving both detection quality and incident response effectiveness.

The architecture is aligned with the MITRE ATT&CK framework to support behavioural detection and threat hunting activities, while the NIST Cybersecurity Framework provides guidance for broader security governance and operational processes. Together, these frameworks ensure that Threat Intelligence integration is both technically effective and strategically aligned with organizational cybersecurity objectives. Figure 1 below demonstrates the proposed architecture.

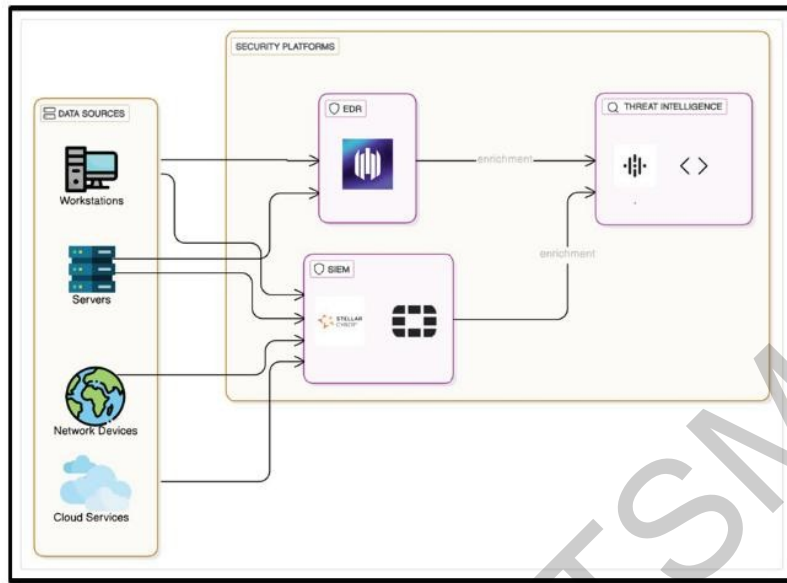


FIGURE 1. Proposed SOC Back End Architecture.

The findings from the expert validation demonstrate strong support for the proposed framework. The experts generally agreed that the conceptual model clearly represented the relationships between SIEM, XDR, and Threat Intelligence components and accurately reflected the operational workflows commonly found in modern SOC environments. The majority of experts indicated that the framework effectively addressed persistent challenges such as alert fatigue, tool silos, and limited contextual awareness during investigations.

The experts also considered the proposed architecture to be realistic and technically feasible for implementation within contemporary SOC environments. The integration of Threat Intelligence was viewed as particularly valuable for improving alert prioritisation and enhancing analyst situational awareness. The experts emphasised that intelligence enrichment enables analysts to focus on high-priority threats while reducing the effort spent investigating false positives and low-risk events.

The results further suggest that an intelligence-driven SOC architecture can improve operational efficiency by supporting more effective event correlation and faster incident triage. By combining data from SIEM, XDR, and Threat Intelligence sources within a unified workflow, organisations can achieve greater visibility across their security environments and respond more effectively to evolving cyber threats.

CONCLUSION

The growing complexity of cyber threats continues to challenge the effectiveness of modern Security Operations Centres. Although organisations increasingly deploy advanced security technologies, the lack of effective integration often limits their ability to achieve meaningful improvements in threat detection and incident response. This study addressed this challenge by proposing a Threat Intelligence-driven SOC architecture that integrates SIEM, XDR, and Threat Intelligence platforms within a unified operational framework.

Expert validation confirmed that the proposed architecture is both practical and relevant to contemporary SOC operations. The findings demonstrate that effective Threat Intelligence integration can improve contextual awareness, reduce operational complexity, enhance alert prioritisation, and support faster incident response. By aligning technological integration with established frameworks such as MITRE ATT&CK and the NIST Cybersecurity Framework, organisations can establish a more proactive and intelligence-driven approach to cybersecurity operations.

Future research should focus on implementing the proposed architecture within operational environments and conducting quantitative evaluations to measure its impact on detection accuracy, response time, analyst workload, and overall SOC performance.

REFERENCES

- Accenture Security. 2023. *State of Cyber Resilience 2023*. Dublin, Ireland: Accenture.
- Ahmad, M., Shah, S., & Khan, K. 2022. Threat intelligence integration for security operation centers: A systematic review, *Computers & Security* 121 (2022): 102–118.
- Alsmadi, M. N., & Alsmadi, A. 2023. The role of cyber threat intelligence in cybersecurity operations, *Journal of Information Security and Applications* 70 (2023): 1–12.
- Bada, M. A., & Nurse, J. R. C. 2020. The social and psychological impact of cyberattacks, *Computers & Security* 96 (2020): 1–15.
- CrowdStrike. 2024. *Global Threat Report 2024*. Austin, TX: CrowdStrike Inc.
- Deloitte. 2023. *Future of Cyber Security Operations Centers*. New York, NY: Deloitte Insights.
- ENISA. 2024. *ENISA Threat Landscape 2024*. Heraklion, Greece: European Union Agency for Cybersecurity.
- Gartner. 2023. Innovation insight for extended detection and response (XDR), *Gartner Research Report*, Stamford, CT.
- Hutchins, A., Cloppert, M., & Amin, R. 2011. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, *Proceedings of the 6th International Conference on Information Warfare and Security* (2011): 113–125.
- IBM Security. 2024. *Cost of a Data Breach Report 2024*. Armonk, NY: IBM Corporation.
- Langner, R. 2019. To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve, *The Langner Group* (2019).
- McMillan, R. 2022. *Cyber Threat Intelligence*. Sebastopol, CA: O'Reilly Media.
- MITRE Corporation. n.d. *MITRE ATT&CK® Framework*. Bedford, MA. Retrieved from <https://attack.mitre.org>
- National Institute of Standards and Technology (NIST). 2024. *Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0*. Gaithersburg, MD: NIST.
- Palo Alto Networks. 2023. *The Modern SOC and Threat Intelligence Integration*. Santa Clara, CA: Palo Alto Networks.
- Ponemon Institute. 2023. *The State of Security Operations Centers*. Traverse City, MI: Ponemon Institute.
- Recorded Future. 2023. *Threat Intelligence Handbook* (2nd ed.). Somerville, MA: Recorded Future.
- SANS Institute. 2024. *SOC Survey 2024: Security Operations Center Evolution and Maturity*. Bethesda, MD: SANS Institute.
- SentinelOne. 2024. *Singularity XDR: Technical Overview*. Mountain View, CA: SentinelOne.
- Verizon. 2024. *2024 Data Breach Investigations Report (DBIR)*. New York, NY: Verizon Enterprise Solutions.