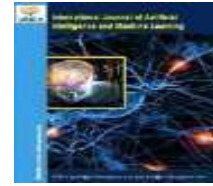




International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

AI-Driven SIEM for Intelligent Incident Management: Integrating SOC Operations, Incident Response, Digital Forensics, and the Cyber Kill Chain

Danish Nasar Ansari*

Senior Consultant Cyber Security, ELM Company, An Nakheel, Riyadh 12382, KSA. E-mail: danish093@hotmail.com

Abstract

While Security Information and Event Management (SIEM) systems are integral to the work of today's Security Operations Center (SOC), traditional rule-based SIEM solutions face growing challenges from the scale, complexity, and speed of today's cyber threats. The study reviews the use of Artificial Intelligence (AI) and Machine Learning (ML) technologies in strengthening SOC operations, speeding up incident response, aiding with digital forensics and correlating detection and response activities with the sequential steps of the Cyber Kill Chain. The qualitative conceptual approach is based on a systematic literature review, which draws on the most recent research on AI-based threat detection, automated incident response, correlation of forensic evidence, and adversarial modeling frameworks such as the Lockheed Martin Cyber Kill Chain and MITRE ATT&CK. The results suggest that the intelligent SIEM architecture can be broken down into five interrelated components: intelligent alert correlation, automated triage and response orchestration, forensic traceability, kill-chain-aware threat mapping, and human-AI collaborative decision making. AI is not meant to replace SOC analysts, it's meant to enhance their abilities to detect, investigate, and remediate incidents by eliminating alert fatigue, decreasing the mean time to detect and mean time to respond, and maintaining forensically sound evidence chains. The study suggests an integrated framework that places AI-powered SIEM in the context of the complete incident lifecycle, and connects detection engineering, orchestration, and post-incident forensic investigation to the sequence of the Cyber Kill Chain. The framework helps with the on-going debate on autonomous and semi-autonomous security operations and has practical implications to be considered when designing SOCs, training analysts, and purchasing tools, as well as for future empirical research.

Keywords: SIEM; artificial intelligence; security operations center; incident response; digital forensics; cyber kill chain.

1. Introduction

Cybersecurity operations are now more complex than ever before due to the rapidly increasing volume of enterprise telemetry, the widespread use of cloud and hybrid architectures, and adversaries who are exploiting identity, supply-chain, and application-layer trust boundaries. For almost 20 years, Security Information and Event Management (SIEM) platforms have served as the "brain" of the Security Operations Center (SOC) by collecting logs from firewalls, endpoints, identity providers, and cloud workloads, then correlating them, alerting on them, and reporting compliance. While traditional SIEMs play a pivotal role in security operations, they are still rule-based and cannot effectively handle polymorphic malware, zero-day attacks, and multi-stage threats that span across multiple data sources (Vielberth, Böhm, Fichtinger, & Pernul, 2020).

The impact on operations is well known. SOC analysts have to respond to thousands of alerts a day, most of which are false positives, leading to chronic alert fatigue and delayed reaction to malicious activity. As per Elseify et al. (2025), ameliorated sand cat swarm optimization balances competing costs across loading scenarios, and the same approach can allocate SOC analyst resources and prioritize alerts under varying threat volumes. Increasing volume and diversity of security events has driven the need for SIEM pipelines to rely on manual and rule-based methods, which has prompted a move to machine learning approaches to highlight significant signals from the telemetry noise, as outlined by Tendikov et al. (2024). Artificial intelligence (AI) has therefore been identified as a key approach for transforming SIEMs into adaptive systems that prioritize incidents, make remediation suggestions, and in certain architectures, take automated action with human guidance (Ismail et al., 2025).

Along with the technical advances, the field of incident response has evolved around the concept of lifecycle models, such as the National Institute of Standards and Technology (NIST) incident response guide, which defines incident response as a process comprising of preparation, detection and analysis, containment, eradication and recovery, and post-incident activity (Cichonski, Millar, Grance, & Scarfone, 2012). Complementing this perspective, adversary-centric models like the Lockheed Martin Cyber Kill Chain

(Hutchins, Cloppert, & Amin, 2011) and the MITRE ATT&CK framework (Strom et al., 2018) outline the stages that attackers will typically jump through as they move from reconnaissance to weaponization, to delivery, to exploitation, installation, command and control, and actions on objectives, providing defenders with a common language to correlate detections with a progression through an attack.

Digital forensics, on the other hand, provides the evidentiary discipline required to reconstruct the events, maintain chain of custody and meet legal and regulatory obligations. In recent years, with the development of new tools, it was acknowledged that AI can support forensic investigation, by automatically correlating forensic artifacts, using ontological reasoning, and mapping recovered artifacts to kill-chain phases and ATT&CK techniques (Dimitriadis et al., 2023). While there have been several recent studies that each focus on a single aspect of autonomous SOC, AI-powered SIEM, or kill-chain-aware detection, few of them delve into how these can be combined into a coherent whole of autonomous SOC operations, AI-powered SIEM, incident response, and kill-chain-aware detection – all integrated into one architecture. According to Khaleel et al. (2024), consumer attachment to conventional meat mirrors organizational attachment to legacy rule-based security tools, which is a key adoption barrier for AI-driven SIEM in SOC environments.

The gap is critical because SOC teams do not detect, respond, and explore as three distinct areas, but rather as a single workflow, where an alert needs to be triaged, correlated to adversary tactics, responded to, and documented as forensic evidence, often under tight time constraints. If the understanding of the contribution of AI into each stage is fragmented, the resulting solutions can be point solutions that automate distinct tasks, but fall short of speeding up or making the incident management lifecycle more defensible. In this context, the present work explores the potential of applying AI to several components of the SIEM-driven detection, SOC triage, automated incident response, digital forensics, and kill-chain-aware threat mapping functions, resulting in an end-to-end intelligent incident management capability.

Based on current research literature in the field of security operations, machine learning in cybersecurity, orchestration and automation, and adversary modeling, this paper compiles the most significant works in each of these areas and puts them together into a unified conceptual structure. The framework embodies the vision of AI-driven SIEM as more than just an alert generator, but as a connector to link the elements of detection engineering, response orchestration, forensic evidence management, and AI-informed situational awareness, as part of the conversation on intelligent SOC design and the automation/human judgement trade-off. Antibacterial wound dressings contain infection and support healing, much as AI-driven SIEM contains breaches by isolating compromised assets during incident response (Athamneh et al., 2025)

2. Literature Review

AI for SIEM and intelligent incident management research can be traced to a number of partially overlapping streams of research: research on the basics of SOC design, research on AI applications to threat detection and response, research on adversarial modelling frameworks such as the Cyber Kill Chain and MITRE ATT&CK, and research that combines digital forensic analysis with AI-assisted investigation. Each strand is reviewed in this section before the research gap for this study is identified.

2.1. The security Operations Center and the evolution of SIEM

The Smooth Security Operations Center has actually been thoroughly studied as the institutional and technological hub of enterprise cyber protection. Vielberth et al. (2020) offer a systematic investigation of the SOC design requirements and conclude that there are core functions in the SOC, such as asset management, log management, threat detection, incident analysis, and continuous improvement, but also some key challenges, including staffing issues, tool sprawl and the cognitive burden on analysts. In this architecture, the SIEM platform has been the traditional aggregation and correlation engine, collecting log information from firewalls, intrusion detection and prevention systems, endpoint agents and identity providers, and using rules to correlate these events into candidate incidents for analysts to review. According to Lee et al. (2025), metaheuristics such as Beluga whale optimization and its variants can tune feature selection and detection thresholds in the correlation engines of AI-driven SIEM platforms.

But a number of trends have made the traditional SIEM design assumptions appear to be burdened with a lot of strain. The number of volumes has grown to an astronomical number for all cloud workloads, SaaS applications and distributed identity systems, and the cost to ingest everything is far too high; selective ingestion may result in blind spots (Ahmad and Alshuaibany, 2026; Alsuhailbany, 2026). Today's attackers gain access to legitimate identity credentials and exploit supply-chain trust relationships, not just relying on what can be detected as malicious signatures, and generate signals that are spread unevenly across platforms and that do not necessarily have the same level of fidelity of logging. Another problem with Rule based correlation content is that detection rules and patterns, created by the analysts, become less effective over time as adversaries evolve their tactics, thus diminishing the analysts trust in the SIEM generated alerts. The change is

being categorized as moving from a SIEM-centric operation to an AI-powered SOC where Extended Detection and Response (XDR), Security Orchestration, Automation and Response (SOAR) and AI-assisted Analyst Copilots are collaborating as complementary capabilities, and SIEM continues to play a vital role in retention, compliance and threat hunting.

As a result of these changes, the SOC should be considered as a dynamic sociotechnical system that is composed of the SIEM and a larger number of elements that allow for detection, orchestration, and human analytical judgment – this is part of the reason why the integrative framework developed in the remainder of this study is dynamic.

2.2. AI and Machine learning in threat detection and response

There is a considerable amount of research exploring the use of machine learning to augment intrusion detection and threat classification, going beyond the power of static signatures (Ganesan, 2026). Sommer and Paxson (2010) raised important issues that machine learning for network intrusion detection has unique problems with base-rate effects, adversarial evasion, and the lack of representative labeled data. This decade has also seen a series of machine learning approaches being developed for cybersecurity challenges, such as malware classification or anomaly based intrusion detection (Memon, 2026), with significant progress in terms of accuracy but still many questions related to interpretability and robustness in practical implementation (Iqbal, 2026; Ullah, Ullah and Ullah, 2026; Yadav et al., 2025). A decade later, various surveys, including the one of Shaukat et al. (2020), have adopted machine learning techniques for cybersecurity applications, from malware classification to anomaly based intrusion detection, and steadily improved the accuracy of the techniques while still encountering many challenges related to interpretability and robustness in practical implementation. According to Shehab et al. (2025), variants of black widow optimization show how nature-inspired algorithms can prune redundant security features, improving the speed and accuracy of SIEM-based threat detection.

The more recent scholarship focuses on the entire response process, not just detection. Liu et al. (2022) present a real-time alert investigation system that uses context-aware prioritization to speed up the threat discovery process in the face of the triage challenge caused by large numbers of correlated alerts. Kraeva and Yakhyayeva (2021) apply metric learning to suggest response playbooks by similarity to previously solved incidents and Kremer et al. (2023) present a system that helps experts to create structured playbooks, easing the manual effort of SOAR authoring. Nguyen and Choo (2021) build on this by adding XAI to the HITL vulnerability detection process, which helps mitigate analyst concerns about the loss of trust in the recommendation. According to Bilal et al. (2025), fractional-order models of interacting multicomponent waves provide a mathematical lens for the long-memory, multi-vector dynamics of multi-stage cyberattacks observed through SIEM. Oudetallah et al. (2025) further stated that Topological covering properties give a formal basis for asking whether a finite set of detection rules can adequately cover an organization's attack surface.

This has been further driven by the adoption of large language models (LLMs). Ismail et al. (2025) introduce a Security Event Response Copilot system that leverages the open-source Wazuh SIEM platform and retrieves relevant advice from vectorized incident response knowledge bases, the MITRE ATT&CK framework, and the NIST Cybersecurity Framework to assist security analysts with decision making. Furter, Ali and Ullah (2026) explore hyper-automation in security orchestration with the help of agentic AI, suggesting that in this context, the role of autonomous or semi-autonomous agents is to perform multi-step response actions and still be controlled by analyst approval gates. Charla (2025) also proposes an explainable automated incident response architecture, which provides the SOC analyst with outputs from the AI model, and Akbari Gurabi et al. (2024) and Paduraru, Dumitru, and Stefanescu (2025) explore the requirements for playbook-assisted incident response and automated playbook generation using large language models, respectively. Tendikov et al. (2024) provide complementary evidence supporting machine learning-based SIEM data acquisition and analysis, showing that such approaches can yield significant increases in accuracy over rule-based approaches.

All these papers suggest a clear direction for the future of AI: it is increasingly moving into a new paradigm from an indicator of detection accuracy to a decision-support and orchestration power that extends from the point of triage through playbook generation and semi-autonomous response execution, with explainability and human oversight as recurring design requirements and not mere add-ons.

2.3. The Cyber Kill Chain, MITRE ATT&CK, and Digital Forensics

Adversary-centric modeling serves as the conceptual structure for SOC analysts to better understand the meaning of each alert across the context of the intrusion. Hutchins, Cloppert, and Amin (2011) defined the intelligence-driven Cyber Kill Chain, which breaks down intrusions into seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. At the core of the model is the idea that defenders, who delay an intrusion in the early stages, prevent the attacker from gaining the "compounding advantage" of the later steps – thus justifying investment in early stage detection. Later, Hubbard and Singer (2017) suggested the Unified Kill Chain, which combined the original kill chain with

the stages of internal reconnaissance, lateral movement, and privilege escalation that are more pertinent to today's intrusion patterns. According to Hussein et al. (2025), combining robust control with fuzzy reasoning parallels hybrid SIEM architectures that fuse deterministic correlation rules with AI-based anomaly scoring for resilient incident handling. Further, Aljaidi et al. (2025) stated that Differential evolution that learns from historical populations can inform SIEM models that learn from past incidents to calibrate detection parameters and reduce false positives. Aburuz, Maloh and Ahmed (2025) stated that preoperative indicators can predict postoperative delirium, and early reconnaissance and delivery-stage signals in the cyber kill chain can likewise predict later compromise, enabling pre-emptive SOC response.

The MITRE ATT&CK framework (2018) adds to the kill chain by providing a detailed and evolving matrix of adversarial tactics and techniques. Rithchea (2025) examines the connection between the two frameworks, and finds that the kill chain's kill chain phases align broadly with ATT&CK's fourteen tactics, and that ATT&CH appears to be an extension of the kill chain's later stages, the action phases. Bolton, Elluri, and Joshi (2023) show how to represent ATT&CK as a structured knowledge graph and perform automated reasoning over ATT&CK relationships. In this convergence, Singh, Dhanraj, and Huang (2025) propose a multi-model machine learning approach that leverages a specialized language model to map the ATT&CK techniques to the phases of the kill chain, training an ensemble of three models – gradient boosting, transformer, and graph neural network – to accurately predict the likely progression of an attacker, showcasing the level of sophistication on which AI can operate adversary-centric kill chains for predictive defense. Machine learning and predictive analytics strengthen SIEM and incident response by transforming them from reactive, rule-based systems into proactive, self-improving ones that detect subtle anomalies, prioritize genuine threats, and anticipate attacks before they fully unfold, shortening detection and response times while reducing analyst overload from false positives (Balasundram et al., 2026; Salem et al., 2025). According to Wang et al. (2025), if governmental attention drives synergistic environmental outcomes, leadership commitment is likely just as critical for unifying SOC, incident response, and forensics under an AI-driven SIEM strategy.

Research into digital forensics has started to explicitly utilize these frameworks to enhance evidence correlation and attack detection capabilities at the beginning of the attack. Dimitriadis, Lykou, Kalogeraki, and Gritzalis (2023) introduced the Fronesis approach, which involves rule-based reasoning over constantly gathered digital artefacts such as volatile process data and email metadata, to detect the traces of an adversarial technique and correlate them to the phases of the Cyber Kill-chain. In a case study illustrating an actual phishing attack, their research shows how machine learning can help eliminate manual burden in forensics, while maintaining the rigor of the evidence, by identifying partial technique patterns that match known patterns of kill chain progression and alerting to an ongoing intrusion. According to Pata, Bozkurt and Altiner (2025), diverse drivers combine into a composite environmental performance index, and AI-driven SIEM likewise aggregates heterogeneous security signals into composite risk scores that guide cyber-resilience investment. As per Rahme et al. (2026) tracing violent behaviour to underlying schemas and prior trauma parallels the cyber kill chain's focus on precursor stages and attacker patterns to anticipate malicious actions. Self-cleaning, antimicrobial fabrics are an apt analogy for autonomous SIEM systems that neutralize threats and restore system hygiene with minimal human intervention (Ibrahim, Moussa & Abd El-Aziz, 2025).

This body of literature shows that the kill-chain and ATT&CK model are no longer just descriptions of an attack chain, but are becoming a way to feed into machine learning pipelines, context for detecting an attack, and an input for predicting what is likely to happen next in a live attack.

2.4. Research Gap

In the literature surveyed, there has been a considerable advance in AI-aided threat detection, automated responses and orchestration, as well as in forensic reasoning based on information about threats. While the work reviewed has significant contributions to make in the areas of AI-aided threat detection, automated response orchestration, and kill-chain-informed forensic reasoning, these contributions are mostly scattered across distinct research streams. The studies of SOC operations and SIEM evolution (Vielberth et al., 2020) provide only a limited amount of information about the embedding of AI models into detection pipelines. Technical studies on AI for triage and response (Liu et al., 2022; Ismail et al., 2025; Charla, 2025) are not often explicit about kill-chain or ATT&CK as a structuring layer. In contrast, machine learning research on kill chains and the ATT&CK framework tends to be assessed at a smaller level of granularity – for example, technique classification and/or single-scenario forensic detection – rather than in the context of the entire SOC incident management lifecycle.

However, there is still a lack of conceptual work that brings these together into a unified view of how an AI-powered SIEM platform can act as a detection engine and orchestration layer, a forensic evidence management system, and a kill-chain aware situational awareness tool. This is a real-world scenario since SOC teams have a unified process for incident management, and using disjointed tools may lead to multiple automation achievements that don't equate to increased overall incident velocity or analyst trust. The present study aims

to fill that void by synthesizing the literature to present an integrated framework, where AI-powered SIEM becomes the coordinating element between SOC operations, incident response, digital forensics and the kill chain-aware threat mapping.

3. Methodology

This study was a qualitative, conceptual research that uses literature synthesis in order to explore the use of AI in SIEM-driven detection, SOC operations, orchestration of incident response, digital forensics, and map and visualize the kill chain-aware threat. The study is not empirical in nature and aims to construct an "integrated framework" of technical and conceptual literature to interpret the role of AI in the overall incident management lifecycle.

3.1. Research Design

The research methodology was a conceptual and interpretive approach which is generally used in cybersecurity and security operations research to synthesize the existing technical literature into structured frameworks. The use of AI in SIEM, SOC, IR, and DF is a socio-technical phenomenon with a more rapid evolution than can be captured in a single proprietary tool, so this approach is suitable. In contrast to focusing on specific models of AI, the study aimed to uncover patterns in design and architecture that occur across a range of AI-based SIEMs, and how these patterns relate to the sequential nature of the Cyber Kill Chain and the needs of digital forensic investigations.

3.2. Data Sources and Selection Criteria

The main data sources were peer-reviewed journal articles, conference proceedings and trusted technical publications on SIEM architecture, SOC operations, machine learning in cyber security, incident response automation, digital forensics, and adversarial modeling frameworks, mostly dated from 2018 to 2025. Literature was chosen based on three criteria: publications that addressed the SIEM or SOC architecture; publications that addressed applications of AI for threat detection or response; publications that described integrating forensics into an adversary modeling effort; publications that described the Cyber Kill Chain, or ATT&CK. Priority was given to peer-reviewed publications as well as widely cited foundational publications that introduced these frameworks; and publications that provided insight into the broader incident management lifecycle rather than one-off tasks.

Hutchins, Cloppert, and Amin (2011), Strom et al. (2018) and Cichonski et al. (2012) were included because of their foundational works that set the structure of adversarial behaviour and incident handling practice. Recent research papers such as Vielberth et al. (2020), Tendikov et al. (2024), Ismail et al. (2025), Charla (2025), Dimitriadis et al. (2023), and Singh, Dhanraj, and Huang (2025) were also integrated to capture recent advancements in AI-driven SOC operations, responses, and forensic reasoning.

3.3. Data Analysis

Thematic analysis and comparative synthesis were used to analyse the literature collected. Iterative reading and qualitative coding were performed to identify key concepts, architectural components, and functional claims of each publication, which were then grouped into major themes: alert correlation, triage and prioritization, response orchestration, forensic evidence management, and kill-chain and ATT&CK-based threat mapping. Comparative analysis led to a mapping of the convergences and divergences between studies of various parts of the incident management lifecycle, and helped to identify how the capabilities described in the various technical studies can be mapped, logically, to an overall architectural framework that can be associated with the steps of the Cyber Kill Chain and the NIST incident response lifecycle.

3.4. Research Trustworthiness

Conceptual rigour was achieved by using theoretical triangulation, which involved incorporating insights from operations research in SOCs, the ML in cybersecurity, orchestration and automation research, the digital forensics scholarship, and existing adversarial models. Support for the conceptual validity of the proposed framework was enhanced by all interpretations being based on technical sources accepted as authoritative and peer-reviewed.

3.5. Scope and Limitations

This study does not include empirical benchmarking of specific SIEM products or SOC deployments, and only focuses on conceptual synthesis of published literature. It does not assess the accuracy of detection, the rate of false positive or the time of response by primary experimentation and the framework suggested must be considered as a concept rather than a proven operational model. Future research can be expanded by empirical validation of the deployment of AI in SIEM, attack-simulation research with controlled variables, and longitudinal analysis of how analyst workload and SIEM forensic outcomes change over time.

4. Results and Discussion

The review demonstrates that the integration of artificial intelligence into SIEM platforms is reshaping SOC operations, incident response, and digital forensics along five interconnected dimensions that interact to form a coherent architecture in which detection, triage, response orchestration, forensic evidence handling, and adversary-centric situational awareness are mutually reinforcing. These five dimensions are summarized in Table 1 before being discussed in detail in the following subsections.

Table 1. Core functional dimensions of AI-driven SIEM for intelligent incident management

Functional dimension	Representative studies	Central technical contribution	Relevance to incident management
Intelligent alert correlation	Vielberth et al. (2020); Tendikov et al. (2024); Sommer & Paxson (2010)	Machine learning-based event correlation reduces reliance on static rule sets and surfaces meaningful signal from heterogeneous telemetry.	Improves detection coverage and reduces false-positive volume reaching SOC analysts.
Automated triage and response orchestration	Liu et al. (2022); Kremer et al. (2023); Ismail et al. (2025); Charla (2025)	Context-aware prioritization, playbook generation, and agentic orchestration accelerate analyst decision-making.	Shortens mean time to detect and respond while preserving analyst approval gates.
Forensic traceability	Dimitriadis et al. (2023); Cichonski et al. (2012)	Ontological reasoning and structured evidence correlation support defensible reconstruction of intrusion timelines.	Preserves chain of custody and supports post-incident and regulatory reporting.
Kill-chain-aware threat mapping	Hutchins et al. (2011); Strom et al. (2018); Singh et al. (2025); Rithchea (2025)	Mapping detections and techniques to kill-chain phases enables prediction of likely attacker progression.	Enables early-phase disruption and prioritization of high-consequence intrusion stages.
Human-AI collaborative decision-making	Nguyen & Choo (2021); Akbari Gurabi et al. (2024); Mellen, Blankenship, Morana, & Belden (2024)	Explainable AI outputs and analyst-in-the-loop design preserve trust and accountability in automated recommendations.	Balances automation efficiency with analyst judgment and organizational accountability.

4.1. Intelligent Alert Correlation as the Foundation of AI-Driven SIEM

The former suggests that intelligent alert correlation is the ground floor for developing AI-based SIEM capability. Traditional SIEM correlation logic relies on rules written by hand that are based on known attack signatures which are difficult to scale with the number and variety of telemetry. According to Vielberth et al. (2020), detection engineering is one of the most resource consuming tasks in a SOC due to the constant manual updating of rules for the ever-changing infrastructure and threat landscape. Sommer and Paxson (2010) warn that using machine learning based intrusion detection has its own potential failure modes, especially when the base rates of malicious attacks are low, and a statistically correct model can result in a high absolute number of false positive alerts.

These issues are tackled by recent studies that integrate supervised and unsupervised learning along with domain-specific feature engineering based on security event schemas. The authors of Tendikov et al. (2024) illustrate how the machine learning approach to SIEM analysis can be more effective in enhancing classification accuracy over a rule-based baseline approach, while simultaneously reducing the amount of manual tuning (Abbas et al., 2025). Instead, Shaukat et al (2020) show that the machine learning classification space used for cybersecurity has advanced over the last 10 years, albeit with interpretability and robustness remaining challenges for using these machines for critical triage.

In an AI-powered SIEM system, intelligent correlation functions complement the rule-based detection instead of replacing it; they group low fidelity signals into high confidence composite incidents, to ease the amount of alerts that are analyzed. According to Abdulhameed et al. (2025), adsorption captures target contaminants from complex solutions, and SIEM filtering similarly extracts malicious indicators from high-volume network telemetry, with kinetics offering a useful lens for detection latency. This is particularly valuable for multi-stage intrusions, as the single steps of an intrusion may not seem that significant when viewed individually, but taken together, from anomaly in authentication to lateral movement to data access patterns, would be very telling of compromise and go a long way toward alleviating the issue of analyst burn-out and missed detections long touted as a problem in the industry.

4.2. Automated Triage and Response Orchestration

Secondly, there has been the increasing use of AI to facilitate the process of triaging and automation of response actions. After the stage of correlation, it is important to conduct quick triage and understand what action needs to be taken and how serious the attack is, a process that takes a lot of time since it is done manually by moving from one console to another. According to Liu et al., (2022), this problem is solved through the provision of alert investigation system using context-aware prioritization technique, where the highest risk alerts are prioritized.

Along with prioritization, recent research demonstrates that AI can also considerably increase the efficiency of the response phase itself. For example, Kraeva and Yakhyayeva (2021) apply metric learning in order to propose response playbooks in terms of the similarity of the current case to past cases. At the same time, Kremer et al. (2023) provide structured playbooks without requiring manual SOAR authoring. LLM-based solutions also expanded these capabilities – in particular, Ismail et al. (2025) introduce a retrieval augmented copilot that can be grounded on incident response, ATT&CK and NIST Cybersecurity Frameworks. In a related study, Ismail et al. (2025) examine agentic AI in multi-step remediation with approval gates. There are also signs of convergence between independent research groups in terms of other AI-powered, explainable automated response architectures, like those proposed by Charla (2025) and Paduraru, Dumitru, and Stefanescu (2025). Moreover, this approach is reinforced by the industry analysis, as it is moving away from the traditional reliance on SIEM and towards orchestration through which EDR, SOAR and AI copilots work in unison to coordinate automated actions and analyst reasoning, with SIEM continuing to play a role in retention and compliance. In addition, Mellen et al. (2024) highlight automated investigation and guided response as some of the important differentiators offered by vendors, thus reemphasizing the significance of orchestration.

4.3. Digital Forensics and Evidentiary Traceability in AI-Augmented Investigations

The third discovery is around the need to combine digital forensics with AI-enabled SIEM functionality that will enable the production of operationally actionable and legally defensible incident conclusions. In the NIST incident handling framework, evidence preservation and post-incident analysis are explicit lifecycle stages, and response outcomes often have legal and regulatory ramifications that require strict evidence chain-of-custody practice (Cichonski et al., 2012). However, traditional forensic investigation is still a labor-intensive task, because analysts have to manually match the volatile and non-volatile artifacts on the potentially vast number of affected hosts.

Dimitriadis, Lykou, Kalogeraki and Gritzalis (2023) show that ontological reasoning with the support of AI algorithms can significantly speed up this task. They have a Fronesis approach to modelling with rule-based reasoning, over a purpose-built ontology, relating collected artifacts to techniques from MITRE ATT&CK and then mapping those techniques to the phasing of the Cyber Kill Chain. Their phishing case study demonstrates that this can be done by detecting an intrusion in progress via partial artifact patterns that begin to match technique combinations that follow along the known phishing kill chain before a pattern actually appears in a signature. This reflects a bigger trend: if AI systems basing their forensic reasoning on a set of pre-defined adversary models, instead of a case-by-case review, they can produce more interpretable and faster-to-produce conclusions about the evidence.

In an integrated SIEM-based solution, forensic traceability acts as the foundation of evidence that ties real time detection and response back to a defensible historical record. Each correlation, triage decision and orchestrated response action produces metadata that, when correctly structured, can directly enter the post-incident forensic timeline, thus minimizing duplicate effort and heightening the velocity and clarity of reporting in compliance with regulatory and legal requirements.

4.4. Kill-Chain-Aware Threat Mapping and Predictive Situational Awareness

The fourth finding is that the Cyber Kill Chain and MITRE ATT&CK are being used not just as descriptive, after-the-fact, taxonomies, but as structuring inputs for detection and prediction through the use of AI. The Cyber Kill Chain was initially conceived by Hutchins, Cloppert and Amin (2011) as a model to help defenders slow down intrusions at the earliest possible stage, preventing the attackers from enjoying the incremental benefits

of more advance stages. MITRE ATT&CK was then formalized in 2018 by Strom et al. into a granular catalog of adversary tactics and techniques, one that is continuously updated, and that maps well onto the kill chain's phases, with increased technical detail in the later stages when adversary actions are being taken. Rithchea (2025) further shows that the fourteen tactics in ATT&CK align well with the kill chain phases, with increased technical detail in later stages where adversary actions are being taken; and newer versions of ATT&CK are being created by Strom et al. (2018) as a granular, continuously updated catalog of adversary tactics and techniques.

This convergence is directly realized in recent advances of machine learning research. Singh, Dhanraj, and Huang (2025) propose a phase-aware, multi-model approach to semantic mapping of ATT&CK techniques to the seven phases of the kill chain using a specialized language model, and train an ensemble of gradient boosting, transformer, and graph neural network architectures to model inter-phase dependencies and predict attacker progression, yielding high classification performance across all phases, proving that it is possible to reliably model the progression to support proactive prioritization. This is complemented by Bolton, Elluri, and Joshi (2023), which structure ATT&CK as a knowledge graph and allow for automated reasoning over relationships between ATT&CK techniques that can be embedded into detection pipelines.

In an AI-powered SIEM, kill-chain-aware threat mapping turns individual alerts from events into placed observations in a likely intrusion story. When the correlated incident is automatically classified with its most likely kill-chain phase and associated ATT&CK techniques, analysts quickly have context about possible severity and likely next steps to take, allowing them to undertake more targeted containment. This is in a significant contrast to the usual practice that involved post hoc manual mapping.

Table 2. Comparison of traditional rule-based SIEM and AI-driven SIEM across the incident management lifecycle

Lifecycle stage	Traditional rule-based SIEM	AI-driven SIEM
Detection and correlation	Static, manually authored correlation rules and signatures; limited adaptability to novel attack patterns.	Machine learning-based correlation that identifies statistical and behavioral patterns across heterogeneous telemetry, reducing detection drift.
Triage and prioritization	Manual analyst review of high alert volumes; limited automated ranking of severity.	Context-aware, risk-ranked prioritization that surfaces the highest-consequence incidents first.
Response and orchestration	Manually executed or narrowly scripted response actions; playbooks authored and maintained by hand.	AI-assisted or agentic playbook generation and execution, with analyst approval gates preserved for high-impact actions.
Forensic investigation	Manual artifact correlation across hosts; time-intensive timeline reconstruction.	Ontology- and AI-assisted artifact correlation mapped to adversary techniques, accelerating defensible timeline reconstruction.
Threat contextualization	Kill-chain and ATT&CK mapping performed manually, typically after incident resolution.	Automated, near real-time mapping of incidents to kill-chain phases and ATT&CK techniques as a direct pipeline output.

4.5. Human-AI Collaboration and the Limits of Automation

The fifth discovery, and another that is common across all literature analyzed, is that the purpose of an SIEM designed with AI is to augment—rather than supplant—human SOC analysts. Nguyen and Choo (2021) and Ganesan (2026) explicitly integrate explainable AI into a human in the loop vulnerability detection system, asserting that AI recommendations that lack interpretability risk eroding analyst trust in the process, thereby defeating the purpose of having the AI in the first place. “Requirements for Playbook-assisted Response” by Akbari Gurabi et al. (2024) also explores the need for playbook-assisted response, noting that automation should work on a “need to” basis, not on an “always” basis, because of the importance of defining approval gates for consequential actions, such as system isolation.

This focus on guided automation, rather than full automation, is confirmed by industry evaluation. While the market is focused on automated investigation and guided response as the key differences that enterprise buyers appreciate among xDRs, Mellen et al. (2024) argue that these tools are not necessarily unsupervised remediation, and that the market wants to see xDRs that are helping analysts make better decisions faster, not taking them out of the equation completely. This aligns with the overall body of literature, in which the most advanced usage of AI in correlation, triage, orchestration and forensics is used to assist rather than replace the analyst's judgment, especially when decisions have major consequences.

This discovery has significant implications for the design of SIEM systems using AI. The literature indicates a range of levels of automation that can be applied based on the consequence and reversibility of the action, and moves from an all-or-nothing approach to a "spectrum" with low-consequence, reversible actions, like enriching an alert or closing a confirmed false positive, suitable for full automation, and higher-consequence actions, like network isolation or credential revocation, better suited to AI-generated recommendations that must be confirmed by an analyst. This keeps automation efficient without sacrificing analysts' accountability and context in complex, high-stakes situations.

4.6. Toward an Integrated Framework for AI-Driven SIEM and Intelligent Incident Management

An additional aspect of this study is the integrated framework, also known as the integrated framework, presented in Table 3, which incorporates AI-enabled SIEM as a coordination layer within a unified architecture to link SOC detection engineering, response orchestration, digital forensics, and situational awareness that is aware of the kill chain. The integration framework shows that although there is a sequence from intelligent correlation to contextual incidents, these incidents form the input for the next stage in the sequence, which is triage and response orchestration, which forms the input for the next stage of forensic evidence management, and so forth.

Some of the implications of this integrative approach for SOC design and future research are the following. In assessing AI-powered SIEM solutions, organizations need to pay attention to the degree of architecture integration of the detection, response, forensic and threat mapping capabilities to find out whether they are standalone solutions or integrated into one product. The training of the analysts needs to be centered around the interpretation and validation of AI recommendations in the full life cycle rather than particular tools. Furthermore, the importance of kill-chain and ATT&CK mapping as a useful but rarely utilized structuring layer for the improvement of interpretability of AI-generated alerts and recommendations is emphasized by the proposed framework. Finally, future research will have to empirically test the graduated automation concept taking into account the effect of analyst's autonomy on the response time, forensic defensibility and analyst's trust.

Table 3. An integrated framework for AI-driven SIEM and intelligent incident management

Framework component	Primary AI function	Kill-chain relevance	Implication for SOC practice
Detection and correlation layer	Behavioral and statistical correlation of heterogeneous telemetry into contextualized incidents.	Surfaces early-phase indicators (reconnaissance, delivery, exploitation) before later-phase impact occurs.	Reduces alert volume reaching analysts and improves early detection coverage.
Triage and orchestration layer	Risk-ranked prioritization and AI-assisted or agentic playbook execution with approval gates.	Directs response effort toward incidents positioned at high-consequence kill-chain phases.	Shortens mean time to detect and respond while preserving analyst control over high-impact actions.
Forensic evidence layer	Ontology- and AI-assisted correlation of volatile and non-volatile artifacts into defensible timelines.	Reconstructs the sequence of adversary actions across kill-chain phases for legal and regulatory reporting.	Accelerates post-incident reporting while preserving chain-of-custody rigor.
Threat-mapping layer	Automated mapping of incidents and artifacts	Provides direct, real-time alignment between	Enables predictive prioritization and more

Framework component	Primary AI function	Kill-chain relevance	Implication for SOC practice
	to kill-chain phases and ATT&CK techniques.	detections and the adversary's likely progression.	targeted containment strategies.
Human-AI collaboration layer	Explainable recommendations, confidence scoring, and graduated automation calibrated to action consequence.	Preserves analyst judgment for ambiguous or high-stakes incidents at any kill-chain phase.	Maintains accountability, trust, and organizational defensibility of automated decisions.

5. Conclusion

This research paper focuses on how artificial intelligence can be utilized in areas such as SIEM-powered detection, SOC management, incident response orchestration, digital forensics, and kill chain-based threat mapping to achieve intelligent incident management. Instead of treating each of these disciplines separately, the researcher has chosen to take a holistic perspective based on modern literature on AI-enabled correlation, orchestration, reasoning, and adversary-oriented models like the Cyber Kill Chain and MITRE ATT&CK matrix. The review shows that SIEM capabilities powered by AI can be viewed from five interrelated dimensions: intelligent correlation of alerts, automation of triaging and response orchestration, forensic traceability, kill-chain-oriented threat mapping, and human-AI-based decision making. These dimensions are not independent but rather complementary to one another, with outputs of the detection process becoming inputs for the response orchestration process, outputs of which become inputs for forensics, and outputs of forensics becoming inputs for threat mapping, and so on. One observation is that advanced AI-powered security systems are always created with the idea of assisting, not replacing, human SOC experts, with the automation level being determined by the consequences and reversibility of the action.

One significant outcome of this study includes the introduction of an integrated framework wherein AI-enabled SIEM serves as the coordinating mechanism between the aforementioned five dimensions to form an architecture in alignment with the sequence defined within the Cyber Kill Chain model and at various stages of well-established incident handling frameworks.

The limitations of this study include its conceptual approach and lack of empirical examination, given that this research draws primarily on published literature. This study neither benchmarks any particular models of AI technology, SIEM solutions, or SOC architectures, but rather serves as a theoretical basis upon which future empirical research may be conducted.

Future research can build on this work through empirical evaluation of AI-driven SIEM implementations, attack simulation testing with measurement of mean time to detection and response, as well as analysis of analyst workload, trust, and forensics effectiveness as functions of degree of automation.

DECLARATIONS

Funding

No specific funding was received for this study.

Conflict of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Author Contributions

All authors contributed collaboratively to the conceptualization, methodology, investigation, formal analysis, writing of the original draft, and review and editing of the manuscript. All authors have read and approved the final version of the manuscript.

Acknowledgments

The authors would like to express their sincere gratitude to the reviewers for their valuable comments and constructive suggestions, which significantly improved the quality and readability of this manuscript.

Ethical Approval

This study was based exclusively on secondary sources and did not involve human participants or animals. Therefore, ethical approval was not required.

Informed Consent

Not applicable.

Data Availability Statement

No new empirical data were generated or analyzed in this study. All materials and sources used are publicly available and are appropriately cited in the reference list.

Statement on the Use of Generative AI

Generative artificial intelligence (AI) tools were used solely for grammar and language editing, stylistic refinement, and manuscript formatting. The authors take full responsibility for the accuracy, integrity, interpretation, and conclusions presented in this manuscript.

References

1. Ahmad, S., & Alshuaibany, Y. (2026). Implementing AI-Driven Decision Support Systems in Data Management. *Precision Journal of Information Technology and Scientific Innovation*, 1(1), 1-15.
2. Akbari Gurabi, M., Nitz, L., Bregar, A., Popanda, J., Siemers, C., Matzutt, R., & Mandal, A. (2024). Requirements for playbook-assisted cyber incident response, reporting and automation. *Digital Threats: Research and Practice*, 5(3), 1-11.
3. Ali, M., & Ullah, I. (2026). Hybrid CNN-LSTM intrusion detection framework for industrial IoT security. *Majestic International Journal of AI Innovations*, 1, 1-15.
4. Alsuhaibany, Y. (2026). Enhancing data security in cloud-based information systems: A systematic literature review.
5. Balasundram, B. S., Chinthala, P., Sait, R. A. M., Mallampati, Y. S., Geneshan, C. P., & Katta, S. (2026, February). Harnessing Machine Learning for Predictive Analytics in Big Data-Driven Marketing Strategies. In *2026 2nd International Conference on Cognitive Computing in Engineering, Communications, Sciences and Biomedical Health Informatics (IC3ECSBHI)* (pp. 468-472). IEEE.
6. Bolton, J., Elluri, L., & Joshi, K. (2023). An overview of cybersecurity knowledge graphs mapped to the MITRE ATT&CK framework domains. *arXiv preprint*.
7. Charla, R. R. (2025). AI-enhanced automated incident response in SIEM with explainability for SOC analysts. In *Proceedings of the 20th International Joint Symposium on Artificial Intelligence and Natural Language Processing (iSAI-NLP)*. IEEE.
8. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide (NIST Special Publication 800-61, Revision 2). National Institute of Standards and Technology.
9. Dimitriadis, A., Lykou, G., Kalogeraki, E.-M., & Gritzalis, D. (2023). Fronesis: Digital forensics-based early detection of ongoing cyber-attacks. *IEEE Access*, 11.
10. Ganesan, C. (2026). A Policy-Aligned Agentic RAG Framework for Risk-Aware Decision Support in Enterprise Customer Relationship Management. *Journal of Intelligent Decision Making and Information Science*, 3(8s), 1409-1443.
11. Ganesan, C. (2026). Ai-Driven Fraud Detection In Multi-Cloud Financial Systems: A Rag-Based Security Architecture. *Scientific Culture*, 12(4). 278-292
12. Hubbard, P. R., & Singer, P. W. (2017). The unified kill chain. Retrieved from <https://www.unifiedkillchain.com/>
13. Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1(1), 80-106.
14. Iqbal, T. (2026). AI-Driven Decision-Support Framework for Cybersecurity Consulting Under Zero-Trust.
15. Ismail, Kurnia, R., Brata, Z. A., Nelistiani, G. A., Heo, S., Kim, H., & Kim, H. (2025). Toward robust security orchestration and automated response in security operations centers with a hyper-automation approach using agentic artificial intelligence. *Information*, 16(5), Article 365.

16. Ismail, Kurnia, R., Widyatama, F., Wibawa, I. M., Brata, Z. A., Ukasyah, Nelistiani, G. A., & Kim, H. (2025). Enhancing security operations center: Wazuh security event response with retrieval-augmented-generation-driven copilot. *Sensors*, 25(3), Article 870.
17. Kraeva, I., & Yakhyeva, G. (2021). Application of the metric learning for security incident playbook recommendation. In 2021 IEEE 22nd International Conference of Young Professionals in Electron Devices and Materials (EDM) (pp. 475–479). IEEE.
18. Kremer, R., Wudali, P. N., Momiyama, S., Araki, T., Furukawa, J., Elovici, Y., & Shabtai, A. (2023). IC-SECURE: Intelligent system for assisting security experts in generating playbooks for automated incident response. *arXiv preprint arXiv:2311.03825*.
19. Liu, Y., Shu, X., Sun, Y., Jang, J., & Mittal, P. (2022). RAPID: Real-time alert investigation with context-aware prioritization for efficient threat discovery. In *Proceedings of the 38th Annual Computer Security Applications Conference* (pp. 827–840).
20. Mellen, A., Blankenship, J., Morana, S., & Belden, M. (2024). The Forrester Wave: Extended detection and response platforms, Q2 2024. Forrester Research.
21. Memon, M. (2026). Graph Neural Network Model for Identifying Anomalous User Behaviour in Enterprise Access Logs. *Majestic Journal of Information Technology* 1(1). 1-24.
22. Nguyen, T. N., & Choo, R. (2021). Human-in-the-loop XAI-enabled vulnerability detection, investigation, and mitigation. In *Proceedings of the 36th IEEE/ACM International Conference on Automated Software Engineering (ASE)*.
23. Paduraru, C., Dumitru, B., & Stefanescu, A. (2025). Automated generation of cybersecurity response playbooks via large language models. *Procedia Computer Science*, 270, 2987–2996.
24. Rithchea, P. (2025). Cyber kill chain and MITRE ATT&CK framework analysis. *AIJR Books*.
25. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, C., & Liu, D. (2020). A survey on machine learning techniques for cyber security in the last decade. *IEEE Access*, 8, 222310–222354.
26. Singh, C., Dhanraj, M., & Huang, K. (2025). KillChainGraph: ML framework for predicting and mapping ATT&CK techniques. *arXiv preprint arXiv:2508.18230*.
27. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE Symposium on Security and Privacy (pp. 305–316). IEEE.
28. Strom, B. E., Applebaum, A., Miller, D., Nickels, D., Pennington, A., & Thomas, C. (2018). MITRE ATT&CK: Design and philosophy. MITRE Corporation.
29. Tendikov, N., Rzayeva, L., Saoud, B., Shayea, I., Azmi, M. H., Myrzatay, A., & Alnakhli, M. (2024). Security information event management data acquisition and analysis methods with machine learning principles. *Results in Engineering*, 22, Article 102254.
30. Ullah, I., Ullah, I., & Ullah, N. (2026). Federated learning framework for privacy-preserving threat detection in distributed IT systems.
31. Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. *IEEE Access*, 8, 227756–227779.
32. Oudetallah, J., Alharbi, R., Rawashdeh, S., Batiha, I. M., Amourah, A., & Sasa, T. (2025). Nearly Lindelöfness in (N^{th}) -Topological Spaces. *International Journal of Analysis and Applications*, 23, 140-140.
33. Bilal, M., Alawaideh, Y. M., Rehman, S. U., Yousif, M. A., Younas, U., Baleanu, D., & Mohammed, P. O. (2025). Gross-Pitaevskii systems of fractional order with respect to multicomponent solitary wave dynamics. *Scientific Reports*, 15(1), 24337.
34. Aburuz, M. E., Maloh, H. I. A. A., & Ahmed, F. R. (2025). Preoperative anxiety and depressive symptoms predicted higher incidence of delirium post coronary artery bypass graft surgery. *Nursing in Critical Care*, 30(4), e13204.
35. Aljaidi, M., Jangir, P., Agrawal, S. P., Pandya, S. B., Parmar, A., Anbarkhan, S. H., & Abualigah, L. (2025). Adaptive historical population-based differential evolution for PEM fuel cell parameter estimation. *Ionics*, 31(1), 641-674.
36. Hussein, R. M., Hadi, A. S., Hasan, S. F., Al-Haddad, L. A., Harrabi, R., Flah, A., & Sahib, I. A. A. (2025). Hybrid integral sliding mode and fuzzy logic control for omnidirectional robots: modified elephant herding optimization for trajectory tracking. *Scientific Reports*, 15(1), 35666.
37. Ibrahim, H., Moussa, I., & Abd El-Aziz, E. (2025). Imparting self-cleaning and antimicrobial properties to cellulosic fabrics using Ti (3+) self-doped rutile TiO2 nanopowder. *International Journal of Biological Macromolecules*, 304, 140783.
38. Salem, A., Masadeh, A., Nofal, B., Othman, E., Saleh, A. M., & Darawad, M. W. (2025). Self-Care management and its predictors among Jordanian patients with type 1 diabetes mellitus: Cross-Sectional study. *SAGE Open Nursing*, 11, 23779608251322603.

39. Yadav, S. K., Gupta, A., Kumar, V., Garg, D. K., & Al-Gburi, A. J. (2025). Prediction of axial ratio using machine learning (ML) for a dual-band circularly polarized dielectric resonator antenna (DRA). *Chinese Journal of Physics*, 96, 1364-1384.
40. Rahme, C., Haddad, C., Akel, M., Khoury, C., Obeid, H., Fekih-Romdhane, F., ... & Obeid, S. (2026). The relationship between early maladaptive schemas and intimate partner violence against women: the moderating effect of childhood trauma. *Journal of Interpersonal Violence*, 41(1-2), 320-344.
41. Pata, U. K., Bozkurt, E., & Altiner, A. (2025). Driving sustainability: The role of renewable energy and foreign direct investment in shaping environmental performance index in BRICS+. *Journal of Environmental Management*, 394, 127309.
42. Wang, X., Liu, W., Sun, X., Ahmad, M., & Chen, J. (2025). Government ecological concern and its impact on synergistic pollution and carbon reduction: Evidence from China. *Gondwana Research*, 141, 180-194.
43. Khaleel, S., Osaili, T., Abdelrahim, D. N., Zeb, F., Naja, F., Radwan, H., ... & Holley, R. A. (2024). Attachment to meat and willingness towards cultured alternatives among consumers: a cross-sectional study in the UAE. *Nutrients*, 17(1), 28.
44. Abdulhameed, A. S., Al Omari, R. H., Younes, M. K., & Algburi, S. (2025). Cross-linked chitosan-adipic/zirconia (ZrO₂) nanocomposite for removal of eosin y dye: insight into physicochemical properties, adsorption modelling, isotherms, and kinetics. *International Journal of Environmental Analytical Chemistry*, 105(17), 5193-5210.
45. Abbas, M., Mahariq, I., Kanwal, H., & Abbas, A. (2025). Characteristics of elastic deformation on Cattaneo-Christov flow of Williamson based hybrid nanofluid with local thermal non-equilibrium effects. *Proceedings of the institution of mechanical engineers, part N: journal of nanomaterials, nanoengineering and nanosystems*, 23977914251319890.
46. Athamneh, T., Abuawad, A., Odat, T., Alshweiat, A., Obaidat, R., Bani Yaseen, F., ... & Gurikov, P. (2025). Investigation of the antibacterial activity of ZnO-loaded alginate/hyaluronic acid aerogels for wound dressing applications. *Polymers*, 17(4), 506.
47. Elseify, M. A., Mostafa, R. R., Hashim, F. A., Domínguez-García, J. L., & Kamel, S. (2025). Optimal scheduling of photovoltaic and battery energy storage in distribution networks using an ameliorated sand cat swarm optimization algorithm: Economic assessment with different loading scenarios. *Journal of Energy Storage*, 116, 116026.
48. Shehab, M., Shambour, M. K. Y., Abu Hashem, M. A., Al Hamad, H. A., Shannaq, F., Mizher, M., ... & Abualigah, L. (2025). A survey and recent advances in black widow optimization: variants and applications. *Neural Computing and Applications*, 37(35), 29113-29133.
49. Lee, S. W., Haider, A., Rahmani, A. M., Arasteh, B., Gharehchopogh, F. S., Tang, S., ... & Hosseinzadeh, M. (2025). A survey of Beluga whale optimization and its variants: Statistical analysis, advances, and structural reviewing. *Computer Science Review*, 57, 100740.