Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 4, Issue 5, 2026

TOWARD INTELLIGENT AND AUTONOMOUS SOCs: ENABLING LLM-DRIVEN, MCP-INTEGRATED, MULTI-AGENT SECURITY OPERATIONS

[1]Hamad Moiz Chodhry, [2]Naveed Naeem Abass, [3]Amina Naseem

[1]Department of Computer Science, Air University, Multan, Punjab
[2]Department of Computer Science, Air University, Multan, Punjab
[3]Department of Information and Communication Engineering, The Islamia University of Bahawalpur

[1]hamadmoizchodhry@gmail.com, [2]naveed.abbas@aumc.edu.pk, [3]aminanaseem101@gmail.com

DOI:

Keywords
Security Operations Center (SOC), Autonomous SOC, Agentic Artificial Intelligence, Multi-Agent Systems, Model Context Protocol (MCP), Alert Triage, Cybersecurity Automation, Large Language Models (LLMs), SIEM, SOAR.

Article History
Received on: 14 April 2026
Accepted on : 07 May 2026
Published on: 08 May 2026

Corresponding Author:

Abstract

The daily influx of alerts, high false positives, disjointed investigation processes, and the continuously groing cyber threats are continuing to put pressure on Security Operations Centers (SOCs). The old model of SOC is reactive, signature-based, and manually intensive SOAR rule books, which are slow to adjust to new Indicators of Compromise (IOCs). It has been observed in empirical research that a considerable number of security alert events go uninvestigated, and those that are investigated are often inaccurately and consistently defined as false positives, which is a leading cause of analyst fatigue, dwell time, and uneven incident response. The recent developments in artificial intelligence (AI) and distributed cyber defense solutions suggest that smarter and autonomous SOC paradigms are evolving into existence. Combined with agentic reasoning and multi-agent coordination architectures, large language models (LLMs) exhibit great potential in Tier-1 alert triage, contextual evidence correlation, automated rule generation and adaptive response planning. There are also interoperability standards like Model Context Protocol (MCP) which allows tool invocation and exchange of contextual data between SIEM, SOAR, TIP and case management systems. It is a review of the existing research on SOC automation, the challenges that persist, and the opportunities that exist in the future to achieve explainable, closed-loop, and autonomous security operations.

I. Introduction

SOCs are operational units that act as the catalyst of real-time monitoring of threats, [1] [2] analysis of alerts, and response to incidents within enterprise networks. The discipline is extensively strained because organizational infrastructures are growing all over the cloud, endpoint, [3] and hybrid settings where it creates immense amounts of security telemetry. The current SIEM and XDR platforms regularly generate thousands of alerts daily [4], and only a fraction of them are further examined and a significant percentage is generally determined as false positives. [5] This alert overload along with the swiftly changing opponent tactics, enhances the dwell time of the attacker and compromises the consistency of incident handling results [3] [4]. Traditional SOC workflows are getting increasingly limited [2][6]. The existing SOC environments are founded on disjointed tool ecosystems where SIEM, SOAR, threat intelligence platforms and case management systems all act as functional silos. [1] The correlation of evidence between these systems is done manually by the analysts, and this is time consuming, cognitively challenging and can lead to gaps in the investigation. Also, the manual engineering of detection rules and correlation logic introduces latency in the process of updating to new Indicators of Compromise (IOCs), allowing repeat attacks within the signature development window. Such bottlenecks are also aggravated by a lack of cybersecurity talent globally and more operational demands on Tier- 1 and Tier-2 analysts. [7] [8] These systemic constraints of scalability and adaptability of the traditional SOC models are operational, structural, and workforce constraints. In line with this, the interest of industry and academia in automation- based solutions that would enable the efficiency of alert triage, enhance the contextual correlation among tools, and decrease the reliance on manual detection engineering is on the rise. This review studies the contemporary state of SOC operational issues and surveys the research trends in more autonomous and learning security operations [9] [10].The paper focuses on how rule-based and procedural approaches to more intelligent and autonomous models of operations have developed SOC automation [11] [12]. It examines and identifies shortcomings in the construction and operation of the most modern automation paradigms, including SOAR, machine learning-based detection, and LLM-assisted investigation. The paper's discussion of emergent agentic architectures, multi-agent coordination strategies, and interoperability methods like the Model Context Protocol (MCP) as supporting elements for next-generation SOCs is predicated on these pillars. Consolidating current trends and creating a roadmap for elucidative, closed-loop, and reasoning-driven security measures are the goals of this.

II. Background and Traditional SOC Challenges

Background details regarding the structure, functional divisions, and inherent limitations of traditional Security Operations Centers (SOCs) are provided in this section. To grasp the concerns of scalability, flexibility, and integration in the following sections, it is essential to consider the architectural, procedural, and organizational aspects of the classic SOC models. The next subsections examine the core SOC operations, tools ecosystems, detection strategies, and early automation projects that lay the groundwork for the emergence of autonomous paradigms.

A. Security Operations Centers (SOC)

Security Operations Centers (SOCs) are primary locations for the monitoring, detection, and response of cybersecurity threats in business environments [13]. To triage warnings, investigate issues, and impose responses in real time on cloud, network, endpoint, and on-premises systems, they

combine human experience, security tools, and standard procedures.

[14] In order to improve security, mature SOCs incorporate different telemetry data, travel with tiered analyst designs (Tier-1 triage, Tier-2 inquiry, and Tier-3 threat hunting), and have active capabilities (threat hunting, adversary emulation, and lessons-learned) [2] [6] [15]

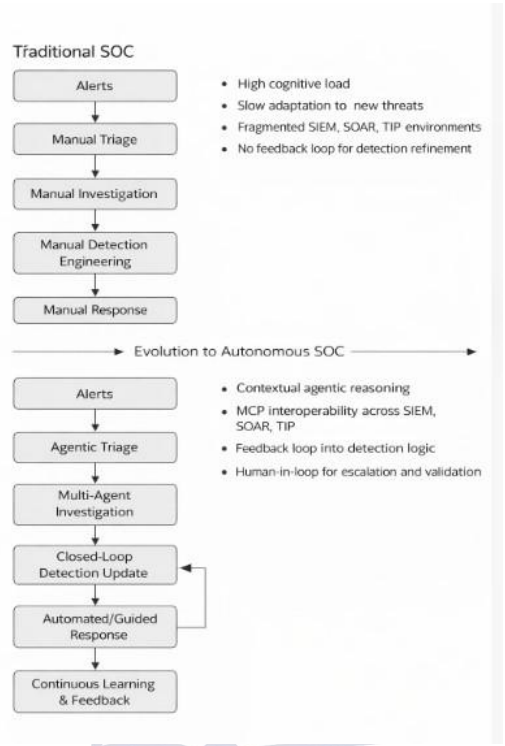

Fig. 1. Transition from traditional SOC workflow to autonomous SOC operations.

B. SOC Tooling Ecosystem

Contemporary SOCs have diverse security tools to assist in discoveries and inquiries. TIPs provide threat intelligence, XDR provides visibility across many zones, SOAR automates predefined response tasks, SIEM collects and associate's data, and case administration tools facilitate teamwork. However, these technologies are often siloed, which increases the cognitive load and divides context among analysts. [6]

C. Rule-Driven Detection and Alert Fatigue

Traditional strategies of SOC detection are based on rules of correlation, signatures, and heuristic logic utilizing established patterns of attack. New or modified threats require the analysts to manually develop and update the detection rules, which delays the detection of new tactics. Such a reactive methodology elevates levels of alerts, false positives, and results in alert fatigue and ineffective analysts. Overall, the use of fixed rules restricts flexibility and imposes a lot of strain on the functioning of SOC teams [16] [17]

D. Early Automation and SOAR Limitations

To manage repetitive and time intensive processes, initial automation initiatives provided SOAR platforms that can execute deterministic processes, including alert enrichment, ticket creation and response execution. These systems are more efficient under correct conditions, but they are basically procedural and lack the capability to think and learn. SOAR systems do not have the capability to generate investigative hypotheses, match evidence in different fields or develop new detection logic. Consequently, the existing

automation systems are lessening the load of executions but not addressing the bigger cognitive and analytical issues presented by the modern large-scale SOCs. [18] [19] [20].

III. Challenges in Modern SOC Operations

A. Alert Overload and False Positives

One of the biggest problems of the contemporary SOCs is the large number of alerts generated by SIEM and XDR among other sites. Very little of these alerts are really investigated and quiet numbers are false positives. This leads to alert fatigue, resource wastage and chances of missing the important cases. Increasingly, this imbalance is becoming unsustainable as the infrastructure and telemetry sources keep on increasing. [21]
[22] [23]

B. Fragmented Investigative Context Across Tools

Successful SOC inquiry must entail association of SIEM, SOAR, TIPs, XDR and case management system evidence. Because these tools tend to be used in isolation, analysts are forced to manually integrate the information, leading to delays, cognitive overload, and the possibility of blind spots, particularly in cases where the volume of alerts is large. [24]

C. Slow Adaptation of Detection Logic and Indicators

Classical SOC detection pipelines are strongly based on manually developed signatures, correlation rules and Indicators of Compromise (IOCs). With the emergence of new tactics, techniques, and procedures (TTPs) by attackers, a process of detection logic must be changed and re-deployed in a human- initiated manner. This is a reactive measure that will leave time gaps where fresh or altered attacks will circumvent the current defenses. Moreover, attackers tend to modify observable artifacts to circumvent fixed signatures, and this makes detection engineering efforts more challenging and constrain the adaptability of rule-based systems. [25]

D. Manual and Cognitive Bottlenecks in Investigative Work- Flows

Tier-1 and Tier-2 SOC investigators work on monotonous investigative assignments, including alert prioritization, log querying, enhancement, and IOC correlation. Although the tasks are required in the operations, they are time consuming and do not scale well with the increase in the number of alerts. Manual workflows burden the mental capacity of the analysts and limit their capabilities of concentrating on higher-order reasoning, threat hunting, and intricate incident examination. These bottlenecks increase the dwell times and reduce the investigative throughput as the number of alerts increases [26]
[27].

E. Workforce Shortages and Skill Asymmetry

Cybersecurity workforce is still in a shortage of qualified professionals, especially investigative and threat intelligence roles and incident response [28] [29]. The nature of the SOC operation demands skills in various fields such as networking, OS, threat analysis, malware behavior, as well as digital forensics and hence it is hard to train new employees fast [30] [31]. The large alert volumes and the lack of talent make analysts feel more burnt out, the turnover is high, and it also makes the organization less resilient to a long-lasting or a coordinated attack.

F. Lack of Closed-Loop Learning Mechanisms

Although cyber-attacks have been known to be repetitive and iterative, the traditional SOC architecture lacks effective closed-loop learning capabilities [32]. Investigation-related information, such as new attacker behavior, a detection gap, or an inadequate reaction, is usually recorded but not routinely added back into threat intelligence databases, enrichment logic, or detection policies.

Due to this absence of unceasing learning, the identical threat items are identified again once more, and defensive enhancements are delayed, which makes traditional SOC models fundamentally responsive [33].

IV. Existing Automation and AI Approaches in SOC

A. SOAR-Based Procedural Automation

Deterministic automation was added to SOC environments through Security Orchestration, Automation, and Response (SOAR) platforms that enable execution of predefined play- books of operations such as alert enrichment, case creation, ticket escalation, and containment actions [34] [35]. The play- books cut manual labor on repetitive and procedural tasks and allow analysts to execute standard response workflows more effectively. SOAR systems however lack adaptive reasoning and cannot correlate new contexts between multiple sources or generate new logic used to detect something [36]. They depend fully on human-written instructions, which means that their contribution is more to the efficiency of execution, as opposed to making their analysis more scalable and their decision- making more independent [37].

B. Machine Learning and Anomaly Detection in SOC Pipelines

The main areas of machine learning (ML) research in cyber- security have been anomaly detection methods, behavioral modeling, classification algorithms with the aim of differentiating legitimate and malicious activities [38] [39] . These solutions are supplementary to signature-based detection, and they detect statistical anomalies of network, endpoint and cloud telemetry. In most SOC deployments, alerts, cluster related events, or learning previously unknown attack patterns are scored by supervised and unsupervised models [40] [41]. Although machine learning techniques can improve the detection coverage and pattern recognition, they typically require considerable domain-specific tuning and retraining to remain effective in dynamic contexts. In practice, they can also result in extremely high false positive rates, which wears analysts out rather than relieves them. These are also frequently employed only in isolation from investigative procedures and do not assist rule-making, multi-source evidence connection, or post-detection reasoning. Therefore, while ML broadens the scope of detection, its contribution to end-to-end investigative automation and workload reduction is limited. [42]

C. Threat Intelligence Automation and IOC Enrichment

Threat Intelligence Platforms (TIPs) is an automated system of gathering, correlating and sharing Indicators of Compromise (IOCs) based on commercial, open-source, and community- driven intelligence feeds. Enrichment pipelines, which are automated, attach contextual metadata to alerts like IP reputation, malware classification, campaign attribution, and so on, which enhance the sense of situational awareness in the analyst. Irrespective of these benefits, TIPs are generally independent information stores that are not closely linked with SOC investigative decision-making. Logical bottlenecks cannot be solved via enhancement, nor can autonomous detection logic changes be made without significant analyst interaction.

D. Large Language Models as Analyst Assistants

Recent advances in large language models (LLMs) have been used to optimize SOC processes in the form of natural language interfaces, summarizing logs, and guided investigative assistance [43] [44] [45]. These systems help analysts to interpret alerts, build case summaries, extract useful in- formation in large quantities of logs and transfer knowledge between teams. Elsewhere, LLMs are applied to interpret detection logic into a human-

understandable explanation or to help generate response documentation [46] [47].

However, the main operational functions of LLMs are those of an analyst copilot, but not independent functioning elements. They neither autonomously trigger investigation processes, employ security solutions, test conjectures to live telemetry, or revise detection regulations without human oversight. Moreover, their products can be influenced by timely structure and situational input, which brings the issue of consistency, verification, and the operational integrity [48] [49]. In this way, although they enhance usability and efficiency in investigations, LLMs are not so far capable of offering fully reasoning-based, closed-loop, and tool-integrated automation in SOC settings.

Table I: ***Comparison of Automation and AI Approaches in SOC***

Approach	Core Strength	Primary Limitation	Typical Use in SOC	Adaptability Level	Ref.
SOAR	Automates predefined playbooks and response procedures	Lacks reasoning and relies on static rules	Response execution and workflow orchestration	Low	[31] [50]
ML	Detects anomalies and statistical patterns across telemetry	High false positives; require retraining and do main tuning	Alert scoring, anomaly detection, pattern classification	Medium	[51]
LLM	Provides contextual understanding, summarization, and language reasoning	Requires supervision and may produce inconsistent outputs	Alert triage, log interpretation, case summarization	Medium	[52] [53]
Agentic AI	Coordinates multiple tools and tasks with goal-driven reasoning	Early-stage maturity; governance and safety concerns	End-to-end investigation and adaptive response	High	[54]

V. Limitations of Existing Approaches

Although there have been progressive advancements in detection, enrichment and workflow execution, the current SOC automation and AI-based solutions have intrinsic flaws, preventing them to scale and adequately satisfy the operational complexity of current cyber defense environments [55] [56].

To begin with, SOAR-based automation generally is confined to the implementation of procedural operations and does not include the ability to formulate a hypothesis of the investigation, perform correlations between the existing facts of the context and support decisions [15], [19]. These systems operate according to predetermined playbooks without becoming familiar with the circumstances of the investigation, which means that they still need a human operator to monitor them when an unforeseen or changing threat situation occurs [6], [10].

Second, machine learning (ML) and anomaly detection methods enhance coverage of detection

but have no considerable impact on reducing investigative work. False positives are very high, data drift can affect the performance, and it is less interpretable, which makes the models less effective in realistic SOC settings [4], [21]. Whereas ML-based systems generate additional alerts, they are not useful in terms of downstream investigative reasoning, evidence synthesis, and automated rule updates [15].

Third, the automation of threat intelligence and enhancement of IOC are useful in enriching situational awareness, although they largely represent parallel informational pipelines. The reason why Threat Intelligence Platforms (TIPs) are not tightly integrated with detection logic and rule engineering workflows is why there are delays in responding to new threats. Consequently, enhanced intelligence is not always used and fails to render into prompt defensive benefits [6], [15].

Lastly, the existing applications of large language models to SOCs are fundamentally the form of analyst-facing aid, as opposed to fully autonomous functions [48], [54]. These systems do not automatically initiate an investigative process and are based on user prompts, call on security tools or integrate evidence sources into meaningful defensive updates. LLM-based assistance is only advisory and not operational until there are established ways to access SOC tooling eco sites [50], [53].

Combined, these shortcomings indicate that current automation originally are focused on single functional areas of operation and not the entire investigative and defensive life cycle. This means that current SOC automation remains execution focused, reactive, and significantly reliant on human intervention, with the result that alert triage, detect logic adjustment, and ongoing defensive learning remain an unsolved and human-intensive problem.

VI. From Procedural Automation to Autonomous Operations

Procedural automation constraints, coupled with a subsequent rise in the number of alerts, fragmented context in investigations, and sluggish upgrades to detection pipelines has given rise to the development of increased interest in autonomous SOC paradigms. These new methods put reasoning, synthesizing conclusions, and lifelong defensive learning among the operational capabilities instead of efficiency in the execution [57].

A. Agentic AI for Investigative Reasoning

The latest studies consider agentic AI systems that emu- late Tier-1 and Tier-2 SOC studies. These systems have the capability to automatically triage alerts, generate hypotheses and correlated evidence on endpoint, network, and cloud data [58]. These frameworks are aimed at reducing workload among analysts, cutting the time spent on alert dwells, and enhancing scalability. Initial research indicates that LLMs are quite effective at interpreting logs, summarizing alerts, and reasoning. Nevertheless, many systems nowadays perform like an analyst copilot, but not as entirely autonomous. Operational autonomy needs to be achieved through formal tools interfaces, execution governance and safety constraints to ensure that the decisions are correct and responsible [59].

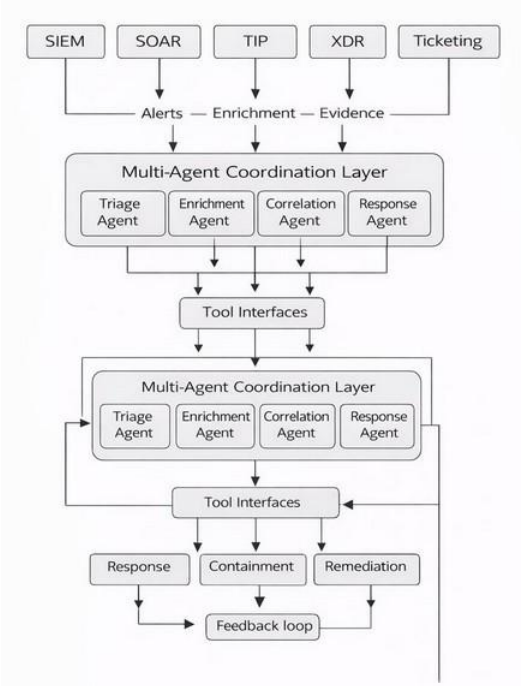

Fig. 2. Multi-agent architecture for autonomous SOC investigations.

B. Closed-Loop Cyber Defense

New Indicators of Compromise (IOCs) must be manually updated because traditional SOCs rely on fixed detection models. [15], [25] This leaves gaps of vulnerability against which fresh threats pass without detection. Closed loop cyber defense can solve this issue by relying on the feedback of proven incidents to automatically change detection pipelines, threat intelligence and IOC workflows [30]. SOCs can be adapted more quickly with less human effort by using automated rule generation and validation and can shift operations to more proactive and learning-oriented security [17], [44].

C. Interoperability and the Model Context Protocol (MCP)

One of the significant barriers to sophisticated SOC automation is the inability to interface security tools. SIEM, SOAR, TIP and case management systems tend to operate independently and as such, automation is restricted to small, procedural processes. Tool invocation and structured context exchange between AI agents and SOC platforms are made safe via the Model Context Protocol (MCP). This allows cross system workflows to be made but keeps context and access control. MCP addresses the integration problems by harmonizing the interactions between agents and tools, facilitating end-to-end coordinated investigative and response operations, and fostering towards autonomous and reasoning-based SOC operations [60] [61].

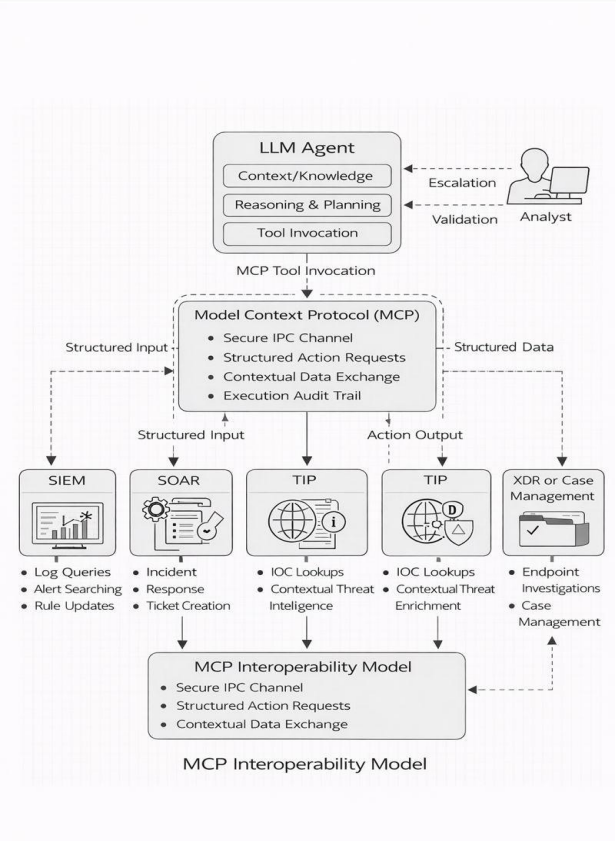

Fig. 3. Model Context Protocol enabling structured interoperability across SOC tool ecosystems.

VII. Research Opportunities and Open Challenges

Considering the encouraging developments in agentic AI, interoperability protocols, and closed-loop defense, there are still numerous gaps on the way to autonomous SOC functions. Sealing these gaps is critical to transitioning towards more advisory automation to more resilient and fully reasoning SOC architectures.

A. Explainability and Analyst Trust

The interpreting ability challenges in LLM-based reasoning and coordination between agents may impact operational trust in SOCs. To support incident reaction and investigation, security operations should contain auditable decision-making procedures, a clear justification, and evidence correlation. Explainable AI is a research area that remains underdeveloped, and it should not stop at the general explanations to allow analysts to validate and replicate AI-driven decisions.

B. Reliability and Hallucination-Resistance

Autonomous investigative systems must control ambiguity, steer clear delusional conclusions, and guarantee the ac- curacy of created rules, hypotheses, and IOC outputs. Unlike classic LLM standards, evaluating dependability in hostile and high-volume operational situations has special issues. To avoid operational misfires and preserve incident response integrity, strong governance procedures, verification layers, and anomaly detection are necessary.

C. Adversarial Robustness and Threat Modeling

AI-based SOC architecture operates in adversarial settings in which the threat agents are most likely to intentionally seek to exploit vulnerabilities in the detection models, reasoning or interoperability interfaces. The recent studies in adversarial

machine learning are directly related to prediction problems, which creates knowledge gaps on risk peculiar to investigative automation. Future efforts should focus on threat modeling of AI-generated SOC agents and identifying methods to enhance the resilience of multi-agent workflows against manipulation or deceit.

D. Human-in-the-Loop Integration

Completely autonomous SOC models are improbable to totally supplant analyst involvement. Human supervision is crucial for escalation, validation, rule governance, and exception management. Developing hybrid operational models that integrate machine autonomy with human decision-making, while reducing cognitive load, is a significant area of research. Optimal human-agent interaction models must be developed to ensure trust, accountability, and operational reliability.

E. Evaluation Metrics and Benchmarking

The current evaluation systems of SOC performance pre- dominantly encompass indicators related to the volume of warnings, dwell time and false positive rates. Autonomous investigative systems necessitate novel metrics and benchmarking methods to assess the quality of reasoning, closed-loop learning, and agent coordination. Experimentally Lack of standard datasets and testbeds that can be reproduced across systems causes the systems to be hard to compare empirically and this necessitates common evaluation models.

F. Interoperability Standards and Protocol Maturity

While the Model Context Protocol (MCP) introduces promising interoperability mechanisms, the maturity of security automation standards remains limited. SOC ecosystems require consistent models for action authorization, auditability, data exchange, and execution safety. Long-term viability depends on community adoption, standardization, and deep in- tegration across diverse tooling ecosystems to support secure, coordinated autonomous operations.

VIII. Conclusion

Due to numerous warnings, malfunctioning workflows, manual rules, and inadequate learning, SOC workloads are increasing. Although they are helpful, tools like SIEM, XDR, and SOAR still require human input.

By enhancing reasoning, context comprehension, and feedback, new technologies like agentic AI, LLMs, multi-agent coordination, and MCP can make SOCs more intelligent and self-sufficient. Explainability, dependability, and human oversight continue to be problems.

References

[1]B. Gelman, S. Taoufiq, T. Vo¨ro¨s, and K. Berlin, "That escalated quickly: An ml framework for alert prioritization," 2023. [Online]. Available: https://arxiv.org/abs/2302.06648

[2]M. Vielberth, "Security operations center (soc)," in Encyclopedia of Cryptography, Security and Privacy, S. Jajodia et al., Eds. Springer, Berlin, Heidelberg, 2021. [Online]. Available: https://www.researchgate. net/publication/349312209 Security Operations Center SOC

[3]M. Turcotte, F. Labre`che, and S.-O. Paquette, "Automated alert classification and triage (aact): An intelligent system for the prioritisation of cybersecurity alerts," 2025. [Online]. Available: https://arxiv.org/abs/2505.09843

[4]S. Tariq, M. B. Chhetri, S. Nepal, and C. Paris, "Alert fatigue in security operations centres: Research challenges and opportunities," ACM Computing Surveys, vol. 57, no. 9, pp. 1–38,

2025. [Online]. Available: https://doi.org/10.1145/3723158

[5]L. Layman and W. Roden, "A controlled experiment on the impact of intrusion detection false alarm rate on analyst performance," 2023. [Online]. Available: https://arxiv.org/abs/2307.07023

[6]C. Onwubiko and K. Ouazzane, "Challenges towards building an effective cyber security operations centre," 2022. [Online]. Available: https://arxiv.org/abs/2202.03691

[7]K. T. W. Teuwen, T. Mulders, E. Zambon, and L. Allodi, "Ruling the unruly: Designing effective, low-noise network intrusion detection rules for security operations centers," 2025. [Online]. Available: https://arxiv.org/abs/2501.09808

[8]HostingJournalist.com. (2024, Oct) Study: Socs struggle with tool overload and alert fatigue. Accessed: 2026- 01-21. [Online]. Available: https://hostingjournalist.com/news/ study-socs-struggle-with-tool-overload-and-alert-fatigue

[9]J. Oliver, R. Batta, A. Bates, M. A. Inam, S. Mehta, and S. Xia, "Carbon filter: Real-time alert triage using large scale clustering and fast search," 2024. [Online]. Available: https://arxiv.org/abs/2405.04691

[10]A. Mohsin, H. Janicke, A. Ibrahim, I. H. Sarker, and S. Camtepe, "A unified framework for human ai collaboration in security operations centers with trusted autonomy," 2025. [Online]. Available: https://arxiv.org/abs/2505.23397

[11]A. Mareedu, "Autonomous security operations centers (soc): Ai agents for threat triage, response, and orchestration," International Journal of Emerging Research in Engineering and Technology (IJERET), vol. 6, no. 2, pp. 63–70, May 2025. [Online]. Available: https://ijeret.org/index.php/ijeret/article/view/170

[12]N. Ali and G. Wallace, "The future of soc operations: Autonomous cyber defense with ai and machine learning," ResearchGate Preprint, February 2025. [Online]. Available: https://www.researchgate.net/publication/ 389319612 The Future of SOC Operations Autonomous Cyber Defense with AI and Machine Learning

[13]I. P. E. D. Nugraha, "A review on the role of modern soc in cybersecurity operations," International Journal of Current Science Research and Review, vol. 4, no. 5, pp. 408–414, May 2021. [Online].Available: https://ijcsrr.org/wp-content/uploads/2021/05/13-15-2021.pdf

[14]K. Demertzis, P. Kikiras, N. Tziritas, S. L. Sanchez, and L. Iliadis, "The next generation Cognitive security operations center: Network flow forensics using cybersecurity intelligence," Big Data and Cognitive Computing, vol. 2, no. 4, p. 35, 2018. [Online]. Available: https://www.mdpi.com/2504-2289/2/4/35

[15]M. Vielberth, F. Bo¨hm, I. Fichtinger, and G. Pernul, "Security operations center: A systematic study and open challenges," IEEE Access, vol. 8,pp. 227 756–227 779, 2020.

[16]G. Yang, C. Tang, and X. Liu, "Dualacnn: Revisiting and alleviating alert fatigue from the detection perspective," Symmetry, vol. 14, no. 10,p. 2138, 2022. [Online]. Available: https://www.mdpi.com/2073-8994/ 14/10/2138?[17]X. Wang, X. Yang, X. Liang, X. Zhang, W. Zhang, and X. Gong, "Combating alert fatigue with alertpro: Context-aware alert prioritization using reinforcement learning for multi-step attack

detection," Computers & Securit, vol. 137, p. 103583, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823004935?[18]Ismail, R. Kurnia, Z. A. Brata, G. A. Nelistiani, S. Heo, H. Kim, and

H. Kim, "Toward robust security orchestration and automated response in security operations centers with a hyper-automation approach using agentic artificial intelligence," Information, vol. 16, no. 5, p. 365, 2025. [Online]. Available: https://www.mdpi.com/2078-2489/16/5/365

[19]R. A. Bridges et al., "Testing soar tools in use," Computers & Security, 2023, available from: ttps://www.sciencedirect.com/science/article/pii/S0167404823001116. [Online]. Available: https://www.sciencedirect.com/science/article/pii/ S0167404823001116

[20]S. U and R. D, "Adaptive open cyber intelligence for soar: Reduced false positives in low-resource environments," International Journal of Advanced Computer Science and Applications, vol. 16, no. 11,p. 105, 2025. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2025.01611105

[21]L. Layman and W. Roden, "A controlled experiment on the impact of intrusion detection false alarm rate on analyst performance," arXiv preprint arXiv:2307.07023, 2023. [Online]. Available: https://arxiv.org/abs/2307.07023

[22]W. Mullins, "Alert fatigue crippling security operation centers," Security Magazine, 2026. [Online]. Available: https://www.securitymagazine.com/articles/97400-alert-fatigue-crippling-security-operation-centers

[23]M. W. Eckhoff, P. M. Flydal, S. Peters, M. Eian, J. Halvorsen,V. Mavroeidis, and G. Grov, "A graph-based approach to alert contextualisation in security operations centres," arXiv preprint arXiv:2509.12923, 2025. [Online]. Available: https://arxiv.org/abs/2509. 12923

[24]H. Team, "Study: Socs struggle with tool overload and alert fatigue," HostingJournalist.com, 2024. [Online]. Available: https://hostingjournalist.com/news/ study-socs-struggle-with-tool-overload-and-alert-fatigue

[25]K. T. W. Teuwen, T. Mulders, E. Zambon, and L. Allodi, "Ruling the unruly: Designing effective, low-noise network intrusion detection rules for security operations centers," arXiv preprint arXiv:2501.09808, 2025. [Online]. Available: https://arxiv.org/abs/2501.09808

[26]M. Kukkonen, "Competency requirements for tier-1 soc analyst," Master's thesis, Laurea University of Applied Sciences, 2024, bachelor's thesis, Theseus.fi open repository. [Online]. Available: https://www.theseus.fi/handle/10024/875604

[27]E. Elfving and K. Forslund, "Security operation centers: The human experience of security analysts," Master's thesis, Lulea˚ University of Technology, 2025, master's thesis, Department of Engineering Sciences and Mathematics, Lulea˚ University of Technology. [Online]. Available: https://www.diva-

portal.org/smash/record.jsf?pid=diva2:1958979

[28]"Norma@nci library - national college of ireland repository," https://norma.ncirl.ie/7883/, 2026, accessed: 2026-02-18.

[29]S. Furnell, "The cybersecurity workforce and skills," Computers & Security, vol. 100, p. 102080, 2021, accessed: 2026-02-18. [Online]. Available: https://www.sciencedirect.com/science/article/pii/ S0167404820303539

[30]O. Akinrolabu, I. Agrafiotis, and A. Erola, "The challenge of detecting sophisticated attacks: Insights from soc analysts," in Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018). Hamburg, Germany: Association for Computing Machinery, 2018, pp. 1–9, accessed: 2026-02-18. [Online]. Available: https://doi.org/10.1145/3230833.3233280

[31]M. A. Majid and K. A. Z. Ariffin, "Model for successful development and implementation of cyber security operations centre (soc)," PeerJ Computer Science, vol. 7, p. e689, 2021, pMCID: PMC8604312, Accessed: 2026-02-18. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC8604312/

[32]F. Hussain, S. Khan, W. Chen, Y. Wang, A. Ahmed, andF. K. Hussain, "A data-driven intrusion detection approach for live networks with efficient feature engineering and selection," IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 1275–1310, 2023, accessed: 2026-02-18. [Online]. Available: https://ieeexplore.ieee.org/document/10815048

[33]S. A. Chamkar, Y. Maleh, and N. Gherabi, "Security operations centers: Use case best practices, coverage, and gap analysis based on mitre adversarial tactics, techniques, and common knowledge," Journal of Cybersecurity and Privacy, vol. 4, no. 4, pp. 777–793, 2024, accessed: 2026-02-18. [Online]. Available: https://www.mdpi.com/2624-800X/4/ 4/36

[34]F. Jentsch and P. A. Hancock, Eds., Cognitive Systems Engineering in Process Control: From Research to Practice. Boca Raton, FL, USA: CRC Press, 2010, accessed: 2026-02-18. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=V1RyhTamPkgC&oi=fnd&pg=PA53

[35]R. Jones, "An introduction to soar as an agent architecture," ResearchGate, Tech. Rep., accessed: 2026-02-18. [Online]. Available: https://www.researchgate.net/profile/Randolph-Jones-2/publication/228398068 An introduction toSoar as an agent architecture/links/00b7d51a8a879f2b68000000/ An-introduction-to-Soar-as-an-agent-architecture.pdf

[36]M. L. Cole, J. M. Stavros, J. Cox, and A. Stavros, "Measuring strengths, opportunities, aspirations, and results: Psychometric properties of the 12-item soar scale," Frontiers in Psychology, vol. 13,p. 854406, 2022, accessed: 2026-02-18. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fpsyg.2022.854406

[37]T. Kempf, W. Herfs, and C. Brecher, "Soar-based sequence control for a flexible assembly cell," in Proceedings of the IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications (MESA). IEEE, 2009, pp. 293–298, accessed: 2026-02-

18. [Online].Available: https://ieeexplore.ieee.org/document/5347001

[38]M. O¨ zkan-Okay, E. Akin, O. Aslan, S. Kos¸unalp, T. Iliev, I. Stoyanov, and I. Beloev, "A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions," IEEE Access, vol. 12, pp. 12 229–12 256, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10403908

[39]A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, vol. 9, no. 4, 2019. [Online]. Available: https://wires.onlinelibrary.wiley.com/doi/10.1002/widm.1306

[40]M. Khayat, E. Barka, M. A. Serhani, F. Sallabi, K. Shuaib, and

H. M. Khater, "Empowering security operation center with artificial intelligence and machine learning: A systematic literature review," IEEE Access, vol. 13, pp. xxxx–xxxx, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/10850912/

[41]S. K. Sawant, S. Gawade, and M. Shrimali, "Survey of recent approaches in ontology matching," in Smart Innovation, Systems and Technologies. Springer Nature, 2025, pp. 491–509. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-96-1206-2 38

[42]H.-D. Lin, H.-L. Wu, and C.-H. Lin, "A deep transfer learning-based visual inspection system for assembly defects in similar types of manual tool products," Sensors, vol. 25, no. 6, p. 1645, 2025. [Online]. Available: https://www.mdpi.com/1424-8220/25/6/1645

[43]M. Tehranipoor, K. Z. Azar, N. Asadizanjani, F. Rahman, H. M. Kamali, and F. Farahmandi, "Large language models for soc security," in Hard- ware Security. Springer, Cham, 2024, pp. 255–299. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-58687-3 6 [44]M. Khayat, E. Barka, M. A. Serhani, F. Sallabi, K. Shuaib, and

H. M. Khater, "Empowering security operation center with artificial intelligence and machine learning: A systematic literature review," IEEE Access, vol. 13, pp. 19 162–19 197, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/11253942/

[45]S. Muzammil, R. Reddy, V. Kamalakrishnan, H. Ahmadi, and W. U. Hassan, "Towards small language models for security query generation in soc workflows," arXiv preprint arXiv:2512.06660, 2025. [Online]. Available: https://arxiv.org/abs/2512.06660

[46]A. Bilal, D. Ebert, and B. Lin, "Llms for explainable AI: A comprehensive survey," arXiv preprint arXiv:2504.00125, 2025. [Online]. Available: https://arxiv.org/abs/2504.00125

[47]Y. Dang, K. Huang, J. Huo, Y. Yan, S. Huang, D. Liu, M. Gao, J. Zhang, C. Qian, K. Wang, Y. Liu, J. Shao, H. Xiong, and X. Hu, "Explainable and interpretable multimodal large language models: A comprehensive survey," arXiv preprint arXiv:2412.02104, 2024. [Online]. Available: https://arxiv.org/abs/2412.02104

[48]R. Singh, S. Tariq, F. Jalalvand, M. B. Chhetri, S. Nepal, C. Paris, and M. Lochner, "Llms in the soc: An empirical study of human-ai collaboration in security operations centres,"

arXiv preprint arXiv:2508.18947, 2025. [Online]. Available: https://arxiv.org/abs/2508.18947

[49]A. Gupta, S. A. Hasan, A. Kumar, and N. Pandit, "Towards efficient soc workflows using small language models: A study on latency and cost," arXiv preprint arXiv:2505.23397, 2025. [Online]. Available: https://arxiv.org/abs/2505.23397

[50]R. Ismail, Z. A. Kurnia, G. A. Brata, S. Nelistiani, H. Heo, and J. Kim, "Toward robust security orchestration and automated response in security operations centers with a hyper-automation approach using agentic artificial intelligence," 2025, in press / Preprint.

[51]D. L. Vajda, T. V. Do, T. Be´rczes, and K. Farkas, "Machine learning-based real-time anomaly detection using data pre-processing in the telemetry of server farms," 2024, in press / Preprint.

[52]A. Mohan, W. Nash, W. E. Krumholz, R. S. Cullina, and C. E. Brodley, "Soar-net: End-to-end soar orchestration using neural and symbolic planning," arXiv preprint arXiv:2302.05319, 2023, accessed: 2026-02-18. [Online]. Available: https://arxiv.org/pdf/2302.05319.pdf

[53]L. Wang, C. Ma, X. Feng, Z. Zhang, H. Yang, J. Zhang, Z. Chen,J. Tang, X. Chen, Y. Lin, W. X. Zhao, Z. Wei, and J.-R. Wen, "A survey on large language model based autonomous agents," arXiv preprint arXiv:2308.11432, 2023, accessed: 2026-02-18. [Online]. Available: https://arxiv.org/pdf/2308.11432.pdf

[54]M. A. Ferrag, F. Alwahedi, A. Battah, B. Cherif, A. Mechri, N. Tihanyi,T. Bisztray, and M. Debbah, "Generative ai in cybersecurity: A comprehensive review of llm applications and vulnerabilities," Internet of Things and Cyber-Physical Systems, 2025, accessed: 2026-02-18. [Online]. Available: https://doi.org/10.1016/j.iotcps.2025.01.001

[55]A. Mathew, "Human–ai collaboration in security operations: Measuring alert trust, automation bias, and analyst upskilling in ai-augmented soc environments," 2025, dept. of Cybersecurity, Bethany College, USA. In press / Preprint.

[56]F. Binbeshr, M. Imam, M. Ghaleb, M. Hamdan, M. Abdul Rahim, andM. Hammoudeh, "The rise of cognitive socs: A systematic literature review on ai approaches," IEEE Communications Surveys & Tutorials, vol. 25, no. ??, pp. 1–??, 2023, accessed: 2026-02-18. [Online].Available: https://ieeexplore.ieee.org/document/10858372

[57]M. Baldea, A. T. Georgiou, B. Gopaluni, M. Mercango¨z, C. C. Pantelides, K. Sheth, V. M. Zavala, and C. Georgakis, "From automated to autonomous process operations," Computers & Chemical Engineering, vol. 148, p. 107224, 2021. [Online]. Available: https://doi.org/10.1016/j.compchemeng.2021.107224

[58]K. Huang, Scaling Laws for Artificial Intelligence: A Pathway to Agentic IntelligeAvailable: https://link.springer.com/book/10.1007/978-3-031-90026-6

[59]F. Maoro and M. Geierhos, "Contestable ai for criminal intelligence analysis: Improving decision-making through semantic modeling and human oversight," 2025, in press / Preprint.

[60]A. Ehtesham, A. Singh, G. K. Gupta, and S. Kumar, "A survey of agent interoperability protocols: Model context protocol (mcp),

agent communication protocol (acp), agent-to-agent protocol (a2a), and agent network protocol (anp)," 2025, in press / Preprint.

[61]P. Venkiteela, "The new interoperability paradigm: Model context pro- tocol (mcp), apis, and the future of agentic ai," 2025, in press / Preprint.