Systematic Literature Review: Challenges and Issues in the Adoption of SOAR Technology in Cybersecurity

Turki Lazzam Alshammari and Talal Al-Balawi
Department of Computer Science, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, Riyadh, Saudi Arabia

444008877@sm.imamu.edu.sa
tsalbalawi@imamu.edu.sa

Abstract: With the increase in the rate of cyber threats, such as ransomware, social engineering, and zero-day exploits, it is urgent to adopt new security mechanisms like Security Orchestration, Automation, and Response (SOAR) systems. The increase in cyber threats has not only amplified in frequency but also in sophistication. This escalation has forced organizations to rethink traditional defense strategies. SOAR has shown itself to be an important solution by automating repetitive tasks and helping security teams in focusing on strategic threat hunting as well as mitigation. The integration of AI and ML in SOAR frameworks helps in predictive analytics, in which systems can anticipate potential breaches based on pattern recognition from vast datasets. The role of blockchain is to enhance data integrity and help enable secure and decentralized threat intelligence sharing between stakeholders. This paper presents a systematic literature review (SLR) on recent advancements in SOAR technologies, especially the incorporation of artificial intelligence (AI), machine learning (ML), and blockchain; it also reviews case studies across various industry sectors, such as healthcare, finance, industrial control systems, and critical infrastructures, as well as the challenges facing SOAR adoption. By examining 29 studies from academic research, industry case studies, and technical reports, the review synthesizes methodologies, architectures, and performance outcomes to summarize the current state of SOAR systems. The research found that SOAR can significantly reduce incident response times and improve threat detection accuracy, with findings indicating that SOAR can lower response times by up to 80% compared to legacy systems, although implementation costs may reach as high as $5 million. Additionally, specialized personnel are still needed to operate these systems. The skills gap increases barriers to adoption, as few professionals possess expertise in cybersecurity as well as in automation tools. Future directions emphasize developing hybrid models that blend human intuition with machine efficiency for more robust defenses. Finally, the review discusses future research directions to help SOAR further scale, interoperate across platforms, and enable autonomous decision-making.

Keywords: SOAR, S-PSS, Security automation, Incident response, Threat intelligence, Cybersecurity

1. Introduction

Continuously changing threats in the cybersecurity landscape are constantly altering defense mechanisms. The trend of interconnected systems in modern enterprises and critical infrastructure sectors is growing, yet a single breach can give rise to cascading consequences. In other words, the development of Security Orchestration, Automation, and Response (SOAR) systems has been a crucial advancement in response to these challenges. SOAR unifies many security tools and processes to automate threat detection, threat response, and the sharing of threat intelligence. The objective is to minimize human error, shorten response times, and thereby improve an organization's resilience to cyberattacks (Waelchli and Walter, 2025). The motivation for SOAR stems from the fact that traditional Security Information and Event Management (SIEM) systems are useful for data aggregation and alert correlation, but the volume of alerts, the number of false positives, and the burden on human analysts remain high (González-Granadillo et al., 2021). With the rising complexity of attacks, cybersecurity teams have to spend more time manually correlating data and ensuring a speedy response. Consequently, SOAR is both desirable and required for modern cybersecurity defense systems (Empl et al., 2022, Mclaughlin and Elliott, 2023).

Recent work on Smart-Product Service Systems (S-PSS) highlights how the cyber-physical integration of products and services creates new security requirements. SOAR platforms can be viewed as a class of S-PSS in which security "products" (tools, playbooks) and "services" (monitoring, incident response) are orchestrated seamlessly. Framing SOAR as an S-PSS helps align this review with service-systems research and underscores the socio-technical aspects of deployment.

The focus of this review is a literature analysis of SOAR, highlighting the technology integration of AI and ML, different industrial sectors affected by SOAR, challenges, and future directions. This SLR seeks to bridge the gap by synthesizing the key findings of 29 studies to provide researchers, practitioners, and policymakers with a comprehensive overview of the present state and future of SOAR technologies. To structure and guide this systematic literature review (SLR), the following research questions (RQs) were formulated:

RQ1: *How are Smart-Product Service Systems (S-PSS), specifically SOAR technologies, being integrated with emerging technologies such as AI, ML, blockchain, and cloud computing?*

RQ2: *What are the key benefits and limitations observed in the adoption of SOAR across various industry sectors, including healthcare, finance, critical infrastructure, and IoT environments?*

RQ3: *What challenges exist in implementing SOAR solutions, particularly regarding cost, integration with legacy systems, and the cybersecurity skills gap?*

RQ4: *What future research directions are proposed to enhance the scalability, interoperability, and autonomy of SOAR systems?*

2. Methodology

As a structured approach to collate and analyze different findings from various sources, this systematic literature review was conducted. The steps of the methodology were as follows:

SLR process	**Identification**	**Search Strings** "Security Orchestration, Automation and Response" OR "SOAR platform*" OR SOAR SOAR AND (AI OR "machine learning" OR "automation" OR "incident response OR blockchain OR "threat intelligence OR IoT)) SOAR AND ("healthcare" OR "finance" OR "SCADA" OR "critical infrastructure")
		Databases Searched: IEEE Xplore, Springer, Scopus, Google Scholar
		Time span: 2019–2025
		Language: English
	Screening Process	Removal of duplicates
		Initial screening based on relevance to SOAR technologies
		Exclusion of pure SIEM/XDR studies without orchestration or automation focus
	Eligibility (Full-Text Assessment)	• Full-text evaluation of remaining studies
		Inclusion of studies addressing: – SOAR platforms or SOAR-adjacent tools – AI/ML, blockchain, and digital twins etc. integration – Particular emphasis on sector-specific implementations (healthcare, finance, ICS, IoT, critical infrastructure) – Empirical evaluation of incident response or threat detection **Exclusion** of non-English, non-peer-reviewed, opinion-based, or non-technical studies
		Total 29 studies included in the review:
	Synthesis and Quality Assessment	Thematic analysis of extracted data
		Bibliometric and keyword co-occurrence analysis (VOSviewer)
		Studies were evaluated based on: (i) clarity of research objectives and system architecture. (ii) methodological depth, (iii) relevance to SOAR adoption or implementation. (iv) presence of empirical evaluation, case study, or performance metrics, and (v) clarity in reporting challenges and limitations.

Figure 1: SLR process, including identification, screening, eligibility assessment, synthesis, and quality assessment

2.1 Literature Search and Selection

Studies related to SOAR techniques were obtained from an extensive search across academic databases, conference proceedings, and technical reports. The identification criteria consisted of the following inclusion criteria: (i) studies that address components of SOAR implementation; (ii) that encompass advanced technologies, such as AI/ML or blockchain; or (iii) studies revealing case studies of sector-specific applications. A total of 29 references that met these criteria were identified (Waelchli and Walter, 2025).

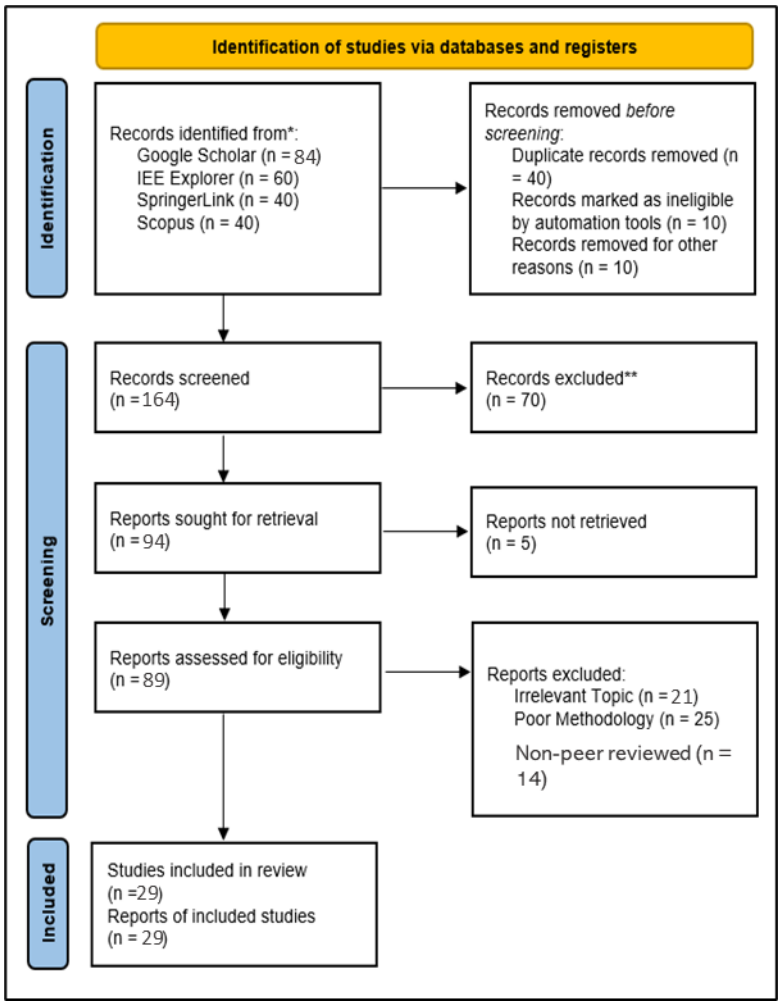

Figure 2: PRISMA flow diagram

2.2 Data Extraction

Information from each study was extracted and condensed from each study (1 study objective, methodology, industry focus, key study results, and challenges identified). Reading the full texts and summarizing the main contributions and limitations of each paper was part of the extraction process (Empl et al., 2022, Christian et al., 2022).

2.3 Thematic Analysis

The green cluster groups AI- and ML-related keywords (e.g., 'machine learning', 'reinforcement learning'), reflecting a strong methodological focus. The orange cluster centers on sector contexts ('healthcare', 'finance', 'ICS'). The red cluster highlights operational themes ('incident response time', 'threat detection'), while the purple and blue clusters denote challenges ('legacy integration', 'skill gap') and future directions ('autonomous SOAR', 'blockchain'), respectively.

The extracted data were grouped into several areas.

- SOAR studies Including ones that integrate AI, ML, and blockchain into SOAR (Alnfiai, 2025, Vinodh Gunnam et al., 2023, Josic et al., 2024)

- Research on SOAR Implementations in health, finance, SCADA systems, and microgrids (Mir and Ramachandran, 2021).
- Incident response times which include measures that assessed the effect of SOAR on incident response time, alert management, and resource optimization (Vast et al., 2021, Gibadullin and Nikonorov, 2021).
- Identified barriers such as legacy integration, cost, and cybersecurity talent shortage (Bhagyalakshmi et al., 2024).

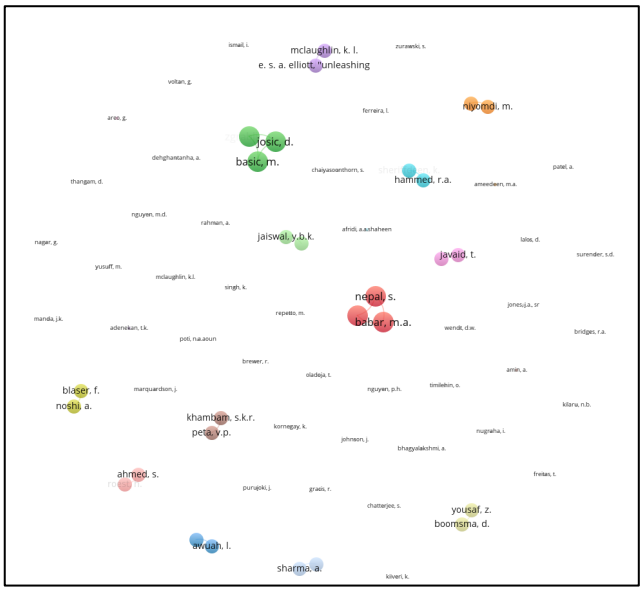

Figure 3: VOSviewer co-occurrence map of author keywords across the 29 studies, with clusters indicating (1) AI/ML integration, (2) Sector-specific applications, (3) Operational efficiency, (4) Challenges, and (5) Future research trends

2.4 Synthesis and Reporting

The final phase was to synthesize the findings from the literature into a coherent narrative. Thematic areas were then used to organize the review, covering a historical perspective as well as a looking ahead to future trends in SOAR.

3. Results

3.1 Evolution of SOAR Technologies

Peer-reviewed literature documents the evolution of SOAR from rule-based automation layers built on top of SIEM systems to intelligent, adaptive platforms that can orchestrate complex, multi-stage incident response workflows. Manual incident response, as well as traditional SIEM platforms, was primarily used in early cybersecurity systems (González-Granadillo et al., 2021). However, as cyber-attacks became more voluminous and complicated, automation became critical to handle overly large and complex data interfaces and to minimize human error. In early research, the focus was on the benefits of data aggregation from multiple sources and the application of basic automation to trigger incident response protocols (Vast et al., 2021, Gibadullin and Nikonorov, 2021). Ultimately, these systems have evolved into sophisticated SOAR platforms that house AI-powered analytics and adaptive response capabilities (Ismail et al., 2025). More recent empirical studies confirm that contemporary SOAR platforms go beyond static playbooks. Bridges et al. (2023) demonstrate that modern SOAR deployments reduce cognitive load on analysts by automating cross-tool data collection and response execution in a significant manner. Their findings highlight that the core value of SOAR is based not just on automation speed, but also encompasses process consistency, auditability, and the reduction of human error in large-scale SOC environments.

3.1.1 Integration with AI and machine learning

As with other trends in SOAR systems, combining AI and ML algorithms is one of the most significant developments in the evolution of SOAR systems. Johnson and Awuah (2021) provide a comprehensive survey of AI-based SOAR architectures. They demonstrate how supervised learning, unsupervised anomaly detection,

and reinforcement learning are being embedded in orchestration pipelines at an increasing rate. These techniques enable SOAR platforms to dynamically prioritize alerts. They also enable the suppression of false positives and adaptation of response strategies based on evolving threat behavior. Vast et al. (2021) have also shown that the use of AI could equip SOAR systems with the ability to reject false-positive findings and focus on detecting true security threats. Nguyen et al. (2024) proposed a multi-layered SOAR architecture that enables RL-based response strategy adaptation in response to real-time threat intelligence. Empirical evaluations also indicate that AI-enhanced SOAR systems function as a force multiplier for security analysts, particularly in environments characterized by high alert volumes. Bridges et al. (2023) report that AI-assisted orchestration substantially improves detection accuracy by correlating contextual indicators across disparate data sources, thereby minimizing redundant investigations. Reinforcement learning approaches further enhance autonomy by enabling systems to learn optimal response actions from historical incident outcomes, reducing reliance on manually curated playbooks.

However, studies differ in the magnitude of results and in their evaluation methods. Vendor or production reports (e.g., Vinodh Gunnam et al., 2023) report large operational gains (20-75% reduction in response time) while laboratory or simulated evaluations (e.g., some RL simulation studies) report promising trends. However, these reports are devoid of real-world validation. Studies indicate a consistent direction (that AI helps), but with variable effect sizes and confidence.

3.1.2 Blockchain and data integrity

Among other things, another emerging trend is the integration of blockchain technology into SOAR platforms. It has been investigated in peer-reviewed literature as a complementary mechanism to enhance trust, integrity, and accountability in SOAR-enabled ecosystems. Recent studies on blockchain-based cyber threat intelligence sharing demonstrate that distributed ledgers can provide tamper-resistant logging, decentralized trust management, and secure information exchange across organizational boundaries. For example, Tolah et al. (2025) proposed a blockchain-enabled threat intelligence framework that ensures the immutability and provenance of shared indicators of compromise. Such properties are particularly relevant to SOAR systems operating in federated environments, where automated response actions depend on externally sourced intelligence. In distributed systems such as microgrids, De Dutta and Prasad (2020) mentioned that blockchain can improve data security and integrity. Creating secure channels between dispersed components of the network using blockchain allows SOAR systems to prevent data tampering and ensures accountability during incident responses. This convergence of blockchain and SOAR is still at an early stage, but there is promise in its use to secure decentralized architectures in cases where there is a high level of trust and transparency (De Dutta and Prasad, 2020, Ismail et al., 2025). However, current studies are largely conceptual or limited to small-scale pilots. No study has demonstrated broad production-scale performance with latency and scalability considerations resolved. Thus, the evidence is promising but of low confidence.

3.2 Sector-Specific Implementations

SOAR has been used globally to solve problems in various sectors, each with its own peculiarities and needs. In this section, we review a number of important studies that target healthcare, finance, industrial control systems, and critical infrastructure (Alnfiai, 2025).

3.2.1 Healthcare

Patient data are highly sensitive, and healthcare systems face many security challenges due to IoT devices, cloud services, and on-premise systems they must manage within their IT infrastructure. Researchers have provided a detailed framework, Security Operations and Automation Platform Architecture (SOAPA), a combination of SOAR and SIEM, which improves cybersecurity in healthcare. The SOAPA framework consists of data services, security operations, and user interface components that provide real-time monitoring and automatic incident response (Chatterjee, 2020).

3.2.2 Finance

Cyber threats are particularly dangerous for the financial sector because sensitive data are of high value, and the applicable laws and regulations are stringent. In financial institutions, Vinodh Gunnam et al. (2023) explored the use of SOAR with AI, which demonstrated systems capable of reducing incident response time to as low as 20-40 minutes in some cases, compared to over 90 minutes in others. The investigation emphasized the advantages of cloud-based SOAR solutions for handling vast amounts of security incidents with high detection accuracy. Although these advantages exist, integrating SOAR with legacy systems and complying

with standards like PCI-DSS and GDPR remain challenges for financial institutions. The integration process often requires significant customization and investment in cybersecurity talent, which can be too costly for smaller organizations (Vinodh Gunnam et al., 2023). These studies show that SOAR offers tremendous value to the financial sector, but its success depends on overcoming integration and regulatory hurdles.

3.2.3 Industrial control systems and critical infrastructure

The most critical data across energy, transportation, and water systems are stored in Supervisory Control and Data Acquisition (SCADA) systems, which are increasingly threatened by sophisticated cyberattacks. SOAR was investigated for its application in SCADA for smart grid systems by Mir and Ramachandran (2021). According to their study, SOAR can reduce high alert volumes and improve response times. However, the integration of IT and Operational Technology (OT) remains a problem since modern cybersecurity protocols were not integrated with legacy SCADA systems (Mir and Ramachandran, 2021). Furthermore, research on microgrids indicates that SOAR can help improve cybersecurity for distributed energy systems. De Dutta and Prasad (2020) demonstrated that SOAR, when combined with AI/ML and blockchain technologies, can form a robust multi-layer defense for microgrids against cyberattacks. However, automating incident responses in microgrids is difficult due to their decentralized nature and the need for continuous updates and adaptations (De Dutta and Prasad, 2020, Ismail et al., 2025, Manda, 2021).

3.2.4 IoT and cyber-physical systems

The attack surface for cybercriminals has expanded with the integration of IoT devices into everyday infrastructure. According to Nguyen et al. (2024), the massive volume of IoT-generated data requires processing, which can be managed by specialized SOAR solutions that handle the output from interconnected devices. Additionally, these frameworks must address a wide range of attack vectors, including DDoS attacks and zero-day exploits. As shown in these studies, AI-driven automation holds strong potential to enhance situational awareness and reduce incident response times in the complex IoT environment (Nguyen et al., 2024, Gilbert et al., 2025). However, integrating disjoint systems and scaling SOAR solutions across large-scale networks remain major challenges (Gilbert et al., 2025, McLaughlin, 2023).

Overall, studies in finance and healthcare generally report measurable operational gains but also emphasize regulatory and legacy constraints. For example, Vinodh Gunnam et al. (2023) and Christian et al. (2022) report clear cost and response-time benefits in financial settings, while Mir and Ramachandran (2021) and Chatterjee (2020) highlight severe legacy/OT integration issues in SCADA. In short, context matters: production environments with modern stacks realize larger gains than legacy-heavy OT contexts.

3.3 Operational Efficiency and Incident Response

SOAR has been shown to be a direct benefit to organizations because several studies have quantified the reduction in incident response times. There are many reports noting that the integration of SOAR platforms can lead to substantial drops in incident response times. Gibadullin and Nikonorov (2021) showed, for example, that an open-source SOAR-based incident management system reduced response time from 34.5 minutes to 12 minutes. In another research study, AI-enabled SOAR in banks resulted in more than a 75% reduction in response time, demonstrating the revolutionary influence of automation on operational efficiency (Vinodh Gunnam et al., 2023). In addition to reducing the risk of protracted security breaches, the reduction of the analysis burden on human analysts frees them for more routine work (Gibadullin and Nikonorov, 2021, Vinodh Gunnam et al., 2023). Bridges et al. (2023) also report substantial reductions in mean time to detect (MTTD) and mean time to respond (MTTR), attributing these gains to automated evidence aggregation and response execution across integrated security tools.

Advancements in the accuracy of detecting threats have been made by incorporating AI and ML in SOAR systems. Bhagyalakshmi et al. (2024) and Jaiswal et al. (2024) employed machine learning algorithms to scrutinize large datasets and recognize true and false positives with high accuracy. For example, AI-based SOAR systems in phishing attack scenarios have achieved up to 98% protection accuracy to improve the general protection posture of an organization (Vinodh Gunnam et al., 2023; Jaiswal et al., 2024). However, these advancements not only help with the management of alerts but also minimize the burden on security teams that have to manage huge numbers of false alarms - something that is particularly important in large-scale network environments (Vast et al., 2021). This is particularly important for organizations that have an enormous number of security logs and alert feeds per day (Vast et al., 2021, Gibadullin and Nikonorov, 2021).

Another crucial benefit from SOAR implementation is operational cost savings. Christian et al. (2022) demonstrate that a cloud-native SOAR solution can scale to handle over 10,000 security incidents a month for under $65 per month. Such a low-cost solution provides a viable pathway for small and medium-sized enterprises (SMEs) that could not afford the high-end commercial solutions. Nevertheless, as these studies demonstrate promising results with regard to cost efficiency, there still remain significant initial investments in training and system customization (Christian et al., 2022).

Moreover, there is also inconsistency in the reporting of results. Open-source deployments reported by Gibadullin and Nikonorov (2021) showed response-time reduction (34.5 → 12 minutes), whereas other reports show percentage improvements without baseline clarity. Differences arise from inconsistent outcome reporting (absolute minutes vs % reduction vs qualitative gains).

3.4 Integration Challenges and Limitations

Although the benefits offered by SOAR technologies are clear, many studies show a reluctance to advance these technologies. Broadly speaking, these challenges can be broken into technical, operational, and human factors. Among the most mentioned challenges across several studies is integrating SOAR with legacy systems. One issue is that many organizations have a mix of modern and older systems, and this makes it harder to combine these components with SOAR, making integration into a heterogeneous environment quite a technical obstacle. For instance, Roche and Dowling (2023) mention that the integration of SOAR with existing SIEM systems, e.g., Splunk, generally requires a lot of customization to incorporate legacy workflows and automatic rules. Similarly, sectors like healthcare and finance heavily rely on data interoperability, and this integration complexity becomes even greater with the presence of legacy systems (Vinodh Gunnam et al., 2023). The studies reviewed also suggest that high investments in the upfront collarization of the system, training, and infrastructure upgrades are commonly needed. with even more difficulty for SMEs (Roche and Dowling, 2023). Also, the need for continuous upgrades and maintenance to respond to changing threats puts further financial pressure (Żurawski et al., 2025).

One of the most consistently reported limitations in peer-reviewed SOAR research is the cybersecurity skills gap. While SOAR automates execution, it does not eliminate the need for expert analysts capable of designing playbooks, validating AI outputs, and supervising automated responses. The problem has been cited by many studies including those by Waelchli and Walter (2025) and McLaughlin (2023). Further, SOAR systems face scalability challenges in highly dynamic environments where many distributed nodes exist, such as IoT networks and critical infrastructures. These socio-technical challenges give weight to the consensus that SOAR should be implemented as a decision-support and orchestration layer, rather than as a fully autonomous replacement for human analysts.

3.5 Future Directions and Emerging Trends

Based on the literature review, several research directions are proposed. The first one is the future development of more autonomous SOAR systems that require less human involvement. Nguyen et al. (2024) demonstrate that future SOAR architectures could dynamically adapt their response strategies in response to evolving threat landscapes (Nguyen et al., 2024). Another important research direction specified is the improvement of interoperability between SOAR systems and existing legacy infrastructure using novel middleware solutions. This is an important area of research for sectors where legacy systems are deeply entrenched and replacing all the systems at once is not an option. There is fertile ground for innovation when SOAR converges with other technologies like blockchain, IoT, and digital twins. For example, it can be applied not only to ensure data integrity but also to promote peer-to-peer threat intelligence sharing among various organizations (De Dutta and Prasad, 2020, Ismail et al., 2025). Moreover, digital twin technologies could support stress testing of SOAR playbooks in simulated environments, as well as train AI models in a controlled setting (Ismail et al., 2025). Such integration might additionally enhance the adaptability and robustness of SOAR systems. Thus, the peer-reviewed literature identifies a clear trajectory toward adaptive, learning-enabled SOAR systems that continuously refine response strategies based on operational feedback. Reinforcement learning-based orchestration, standardized integration interfaces, and simulation-based testing environments are repeatedly cited as promising research directions. Johnson and Awuah (2021) emphasize the importance of explainable AI to improve analyst trust and transparency in automated decision processes.

4. Discussion

While the reviewed literature largely agrees that SOAR improves operational outcomes, there are apparent contradictions with respect to effect size and feasibility, which can be reconciled by considering study context

and methods. Vendor or production reports often present larger gains because they report metrics from mature deployments, whereas academic or pilot studies typically evaluate prototypes or simulated workloads and therefore report smaller or preliminary gains. Differences in metrics (absolute MTTR in minutes, percentage reduction, or qualitative analyst workload reduction) further complicate direct comparisons. Consequently, practitioners should interpret large, single-study effect estimates cautiously and prefer conclusions triangulated across multiple high-quality studies.

Moreover, reviewed literature suggests that complete automation has not been achieved. Human oversight is still present and essential for the situations that involve ambiguous, new, or context-heavy threats that automated playbooks cannot handle still. Researchers have shown that automated systems do not have the interpretive capability and the knowledge of domain. They also lack contextual judgment which is required for complex attacks. It means that analysts are still responsible for preventing automation-based errors and for making sure that there is safe decision-making. The literature also warns that over-reliance on automation introduces issues such as misclassification, reduced transparency, and challenges in post-incident analysis. This issue further supports the need for hybrid human-machine collaboration (Mclaughlin and Elliott, 2023, Żurawski et al., 2025, Nugraha, 2021). Furthermore, researchers recommend that there must be scalable adoption models and phased deployments, which are considered more sustainable pathways. Further, cost-benefit analyses show that reductions in response times and mitigation of breach-related losses can justify investment when weighed against tangible as well as intangible organizational benefits (Vinodh Gunnam et al., 2023, Christian et al., 2022). Overall, the reviewed literature indicates that the evolution of SOAR depends not only on technical innovation but also on improved human - machine alignment. It particularly depends on sustainable cost models and more seamless integration strategies that are able to support different kinds of organizational ecosystems (Kilaru et al., 2021, Islam et al., 2020, Nugraha, 2021).

5. Conclusion

We synthesized findings from 29 studies related to SOAR technologies to create this systematic literature review of the state of the art of SOAR. The review discusses how SOAR systems have progressed from simple automation tools to complex platforms that leverage several tools such as AI, ML, and even blockchain for enhancing cybersecurity operations in various sectors. The balance of evidence supports that SOAR improves incident handling and detection accuracy, but heterogeneity in evaluation methods, sectoral contexts, and reporting metrics prevents precise, generalizable effect-size estimates. Where contrasting results appear, they can largely be explained by differences in context, measurement, and maturity of deployment. This review acts as a wake-up call for both academic researchers and industry practitioners to capitalize on the full power of SOAR to secure our shrinking digital world.

AI declaration: No AI tools were used in the preparation of this manuscript. All content was developed solely by the authors.

Ethics declaration: The study is entirely based on previously published literature; therefore, no institutional ethical approval was required.

References

Alnfiai, M.M. (2025) “AI-Powered Cyber Resilience: A Reinforcement Learning Approach for Automated Threat Hunting in 5G Networks”, EURASIP Journal on Wireless Communications and Networking, 2025, 68.

Bhagyalakshmi, A., Laya, C.S., Preethikaa, A.Y. and Varsha, V. (2024) “Machine Learning Based Early Detection of Ongoing Cyber-Attacks”, 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), IEEE, pp 766-771.

Bridges, R. A., Rice, A. E., Oesch, S., Nichols, J. A., Watson, C., Spakes, K., ... & Erwin, S. (2023). Testing SOAR tools in use. Computers & Security, Vol 129, 103201.

Chatterjee, S. (2020) “Using SIEM and SOAR for Real-Time Cybersecurity Operations in Oil and Gas”, International Journal of Innovative Research and Creative Technology, Vol 6, pp 1-11.

Christian, J., Paulino, L. and de Sá, A.O. (2022) “A Low-Cost and Cloud Native Solution for Security Orchestration, Automation, and Response”, International Conference on Information Security Practice and Experience, Springer, pp 115-139.

De Dutta, S. and Prasad, R. (2020) “Cybersecurity for Microgrid”, 2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC), IEEE, pp 1-5.

Empl, P., Schlette, D., Zupfer, D. and Pernul, G. (2022) “SOAR4IoT: Securing IoT Assets with Digital Twins”, Proceedings of the 17th International Conference on Availability, Reliability and Security, pp 1-10.

Gibadullin, R. and Nikonorov, V. (2021) “Development of the System for Automated Incident Management Based on Open-Source Software”, 2021 International Russian Automation Conference (RusAutoCon), IEEE, pp 521-525.

Gilbert, C., Gilbert, M.A., Dorgbefu, M., Leakpor, D.J., Gaylah, K.D. and Adetunde, I.A. (2025) “Enhancing Detection and Response Using Artificial Intelligence in Cybersecurity”, International Journal of Multidisciplinary Research and Publications (IJMRAP), Vol 7, pp 87-104.

González-Granadillo, G., González-Zarzosa, S. and Diaz, R. (2021) “Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures”, Sensors, Vol 21, 4759.

Gunnam, V., Cheemakurthi, S.K.M. and Kilaru, N.B. (2023) “And PCI Data Security with Cloud Innovations”, International Journal of Advances in Engineering and Management, Vol 5, pp 974-980.

Islam, C., Babar, M.A. and Nepal, S. (2020) “Architecture-Centric Support for Integrating Security Tools in a Security Orchestration Platform”, European Conference on Software Architecture, Springer, pp 165-181.

Ismail, Kurnia, R., Brata, Z.A., Nelistiani, G.A., Heo, S., Kim, H. and Kim, H. (2025) “Toward Robust Security Orchestration and Automated Response in Security Operations Centers with a Hyper-Automation Approach Using Agentic Artificial Intelligence”, Information, Vol 16, 365.

Jaiswal, R., Marshal, R., Rao, V.V. and Singh, K.P. (2024) “AI Phishing Detection Framework for Businesses with Limited Resources”, 2024 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), IEEE, pp 399-404.

Josic, D., Basic, M. and Zgrablic, L. (2024) “Security Principles in Cloud Computing”, Annals of DAAAM & Proceedings, 35.

Kilaru, N.B., Cheemakurthi, S.K.M. and Gunnam, V. (2021) “SOAR Solutions in PCI Compliance: Orchestrating Incident Response for Regulatory Security”, ESP Journal of Engineering & Technology Advancements, Vol 1, pp 78-84.

Kinyua, J., & Awuah, L. (2021). AI/ML in Security Orchestration, Automation and Response: Future Research Directions. Intelligent Automation & Soft Computing, Vol 28, 2.

Manda, J. (2021) “Cybersecurity Automation in Telecom: Implementing Automation Tools and Technologies to Enhance Cybersecurity Incident Response and Threat Detection in Telecom Operations”, Advances in Computer Sciences, 4.

McLaughlin, K.L. (2023) “Defense Is the Best Offense: The Evolving Role of Cybersecurity Blue Teams and the Impact of SOAR Technologies”, Edpacs, Vol 67, pp 35-41.

McLaughlin, K.L. and Elliott, E.S. (2023) “Unleashing the Power of Mobile Threat Hunting Toolkits: Why They Are Crucial in Today’s Cybersecurity Landscape”, EDPACS, Vol 68, pp 1-6.

Mir, A.W. and Ramachandran, R.K. (2021) “Implementation of Security Orchestration, Automation and Response (SOAR) in Smart Grid-Based SCADA Systems”, Sixth International Conference on Intelligent Computing and Applications: Proceedings of ICICA 2020, Springer, pp 157-169.

Nguyen, M.-D., Mallouli, W., Cavalli, A.R. and Montes de Oca, E. (2024) “AI4SOAR: A Security Intelligence Tool for Automated Incident Response”, Proceedings of the 19th International Conference on Availability, Reliability and Security, pp 1-8.

W., Cavalli, A.R. and Montes de Oca, E. (2024) “AI4SOAR: A Security Intelligence Tool for Automated Incident Response”, Proceedings of the 19th International Conference on Availability, Reliability and Security, pp 1-8.

Nugraha, I. (2021) “A Review on the Role of Modern SOC in Cybersecurity Operations”, Int. J. Current Sci. Res. Rev, Vol 4, pp 408-414.

Roche, D. and Dowling, S. (2023) “Elevating Cybersecurity Posture by Implementing SOAR”, 2023 Cyber Research Conference-Ireland (Cyber-RCI), IEEE, pp 1-7.

Tolah, A. (2025) "BlockIntelChain: a blockchain-based cyber threat intelligence sharing architecture", Scientific Reports. https://doi.org/10.1038/s41598-025-29152-6

Vast, R., Sawant, S., Thorbol, A. and Badgujar, V. (2021) “Artificial Intelligence Based Security Orchestration, Automation and Response System”, 2021 6th International Conference for Convergence in Technology (I2CT), IEEE, pp 1-5.

Waelchli, S. and Walter, Y. (2025) “Reducing the Risk of Social Engineering Attacks Using SOAR Measures in a Real World Environment: A Case Study”, Computers & Security, Vol 148, 104137.

Żurawski, S., Chrzyszcz, A., Ciekanowski, Z., Pauliuchuk, Y., Pietrzyk, S. and Wyrzykowska, B. (2025) “Effectiveness of Information Security Incident Management Systems: Identifying Practices, Challenges and Development Perspectives”. European Research Studies Journal, 2025.