RESEARCH ARTICLE

Journal of Data Analysis and Critical Management, Volume 01, Issue 04, 2025

Automated Incident Containment Using SOAR Platforms in Large-Scale Enterprises

Día Fayyad*

Cybersecurity Department, Saudi Aramco; Jordanian Engineers Association, Saudi Council of Engineers

Abstract

Large-scale enterprises are experiencing rapid growth in cyber incidents due to expanded attack surfaces, increased cloud integration, and the speed at which modern threats evolve. Traditional Security Operations Centers rely on manual processes that result in slow containment, inconsistent decision making, and high levels of alert fatigue. This study examines the effectiveness of automated incident containment using Security Orchestration, Automation, and Response platforms within large enterprise environments. A qualitative synthesis of twenty peer reviewed sources, NIST and ISO security frameworks, and empirical studies was conducted to evaluate containment speed, analyst workload, incident classification accuracy, and zero trust alignment.

The findings demonstrate a significant improvement in containment performance when SOAR is deployed. Results indicate that automated workflows reduce average containment time from multiple hours to several minutes, lower analyst workload by up to sixty percent, and enhance the overall consistency of zero trust enforcement. Two performance comparison tables and two visual graphs support these findings by illustrating measurable gains in alert triage quality, containment efficiency, and operational accuracy. AI enabled capabilities such as predictive triage, dynamic playbook recommendation, and automated host isolation further strengthen containment processes across distributed enterprise networks.

The study concludes that SOAR driven containment provides a scalable, accurate, and highly efficient response model for large enterprises. However, successful implementation requires strong governance, high quality SIEM data, and strategies to mitigate automation bias. These insights provide valuable guidance for enterprises seeking to modernize their cybersecurity posture and transition toward automated, intelligence driven response operations.

Keywords: SOAR automation, incident containment, enterprise cybersecurity, zero trust security, security operations centers, AI enabled incident response, automated playbooks.

Journal of Data Analysis and Critical Management (2025); DOI: 10.64235/x3engj56

Introduction

Cybersecurity in large-scale enterprises has become increasingly complex as digital infrastructure, cloud systems, and interconnected technologies expand. Modern enterprises operate highly distributed environments that include hybrid cloud platforms, remote workforce channels, and diverse endpoints, all of which significantly increase vulnerability to cyber attacks. As cyber threats escalate in volume, velocity, and sophistication, organizations require advanced approaches to accelerate containment and reduce the operational burden on Security Operations Centers. Security Orchestration, Automation, and Response platforms provide new opportunities to automate containment actions and improve response efficiency. This section introduces the background, problem context, purpose, objectives, research questions, and structural organization of the study.

Background of Enterprise Cybersecurity

Large enterprises face unprecedented cybersecurity challenges due to the rapid expansion of their digital ecosystems. According to Cichonski et al. (2012), modern organizational environments generate massive volumes of system logs, alerts, and threat indicators that require structured and coordinated incident response processes. As enterprises adopt cloud computing, Internet of Things devices, and virtualization technologies, their security perimeter becomes increasingly fluid, which complicates detection and containment operations.

Hybrid architectures involving on-premises networks, multiple cloud providers, third-party integrations, and remote access systems further widen attack surfaces. The

Corresponding Author: Día Fayyad, Cybersecurity Department, Saudi Aramco; Jordanian Engineers Association, Saudi Council of Engineers, e-mail: dia.fayyad@gmail.com

How to cite this article: Fayyad, D. (2025). Automated Incident Containment Using SOAR Platforms in Large-Scale Enterprises. Journal of Data Analysis and Critical Management, 01(4):51-62.

Source of support: Nil

Conflict of interest: None

International Organization for Standardization (2009) notes that hybrid networks require stronger security governance and standardized response procedures due to their multi-layered configurations and interdependencies. Each new endpoint or integration introduces an additional vector that attackers may exploit through malware, identity compromise, lateral movement, or data exfiltration.

Security Operations Centers are struggling to keep up with this growing complexity. SOC teams frequently experience alert fatigue, an overload condition in which analysts receive more alerts than they can process or verify. AI assisted SIEM studies show that poor alert quality and high false positive rates contribute to slower containment and delayed decision making (Ban et al., 2023). This environment makes it difficult for SOC analysts to prioritize real threats quickly, leading to extended dwell time and increased breach impact. The need for faster, automated, and adaptive containment solutions is therefore critical.

Problem Statement

Despite significant investment in cybersecurity technologies, many large organizations still rely heavily on manual containment processes. These manual workflows are time consuming, inconsistent, and prone to human error. Pulyala et al. (2019) emphasize that containment actions in traditional SOC environments often require analysts to perform repetitive tasks across multiple tools, which directly slows down incident response velocity.

Fragmentation in enterprise cybersecurity tools further complicates containment. As Jha (2025) explains, SOCs commonly operate SIEM systems, endpoint tools, identity platforms, and network monitoring systems that do not seamlessly integrate. This fragmentation leads to information gaps, delays in escalation, misaligned response steps, and poor visibility during active incidents.

Additionally, the global shift toward zero trust security architectures adds new containment requirements. Zero trust principles mandate continuous verification, identity centric control, and consistent policy enforcement regardless of network location (Rose et al., 2020). These requirements cannot be effectively met through manual response alone. Without automated orchestration, enforcement becomes inconsistent and slow, leaving enterprises vulnerable to attackers who exploit gaps during manual approval or containment delays. The combined effect of fragmented tools, manual workflows, and complex security policies illustrates the urgent need for automated containment solutions.

Purpose of the Study

The purpose of this study is to analyze how Security Orchestration, Automation, and Response platforms automate and accelerate incident containment across large-scale enterprise environments. This research investigates how SOAR technologies integrate detection, threat intelligence, and automated playbook execution to reduce containment time and improve decision accuracy. The study also examines the role of artificial intelligence and zero trust architecture in strengthening automated containment steps. By synthesizing evidence from authoritative research and industry frameworks, the study aims to demonstrate the value of SOAR in reducing SOC workload, increasing operational resilience, and enabling standardized, scalable containment processes across complex enterprise ecosystems.

Research Objectives

The specific objectives guiding this research are as follows:

Evaluate Containment Speed Improvements After SOAR Adoption

Pulyala et al. (2019) report that SOAR enabled workflows significantly reduce the steps involved in manual containment, allowing rapid isolation of compromised assets, automated mitigation actions, and faster threat neutralization. This objective evaluates these performance improvements.

Assess How AI Enhances SOAR Decision Workflows

AI capabilities, including machine learning-based triage, anomaly detection, and intelligent playbook recommendations, enhance SOAR decision making and reduce false positives (Kinyua & Awuah, 2021). This objective examines how AI augments the SOAR automation pipeline.

Examine Zero Trust Driven Automated Containment

Zero trust security relies on automated, identity centric enforcement. Santucci et al. (2025) emphasize that aligning SOAR with zero trust ensures rapid privilege revocation, continuous validation, and immediate enforcement of segmentation rules. This objective explores how zero trust principles improve containment precision.

Identify Challenges Limiting SOAR Automation

Automation bias, workflow complexity, and poor tool integration limit effective adoption of automated containment. Tilbury and Flowerday (2024) highlight that analysts may over rely on automation, which creates risks when automated systems make incorrect decisions. This objective identifies technical, operational, and human factors that influence SOAR success.

Research Questions

This study addresses the following research questions:

- How do SOAR platforms improve incident containment speed in large enterprise environments
- What roles do artificial intelligence and machine learning play in enhancing automated containment workflows
- How does integration with zero trust architecture influence containment accuracy and consistency
- What challenges limit the adoption and effectiveness of automated containment in enterprise SOCs

Structure of the Paper

The remainder of this paper is structured as follows:

- Section 2 presents a detailed literature review covering NIST guidelines, ISO frameworks, SOAR evolution, AI enabled capabilities, zero trust integration, and current challenges.
- Section 3 outlines the research methodology, including data sources, analytical procedures, and limitations.
- Section 4 presents the results, including performance comparisons and visualized findings using tables and graphs.
- Section 5 provides an in depth discussion interpreting the results and examining enterprise implications.
- Section 6 outlines practical implications and implementation strategies for large enterprises.
- Section 7 concludes the study with key findings, recommendations, and future research directions.

Literature Review

Foundations of Incident Handling

Incident handling remains a core pillar of enterprise cybersecurity, and its foundations are captured extensively in standardized frameworks. The National Institute of Standards and Technology provides one of the most authoritative references through NIST SP 800-61, which defines containment as a structured, repeatable, and well coordinated process that must occur immediately after detection to limit the impact of cybersecurity incidents (Cichonski et al., 2012). The NIST guidance emphasizes preparation, detection, containment, eradication, and recovery as a cycle that relies on predefined procedures and consistent communication. In this context, containment is not an isolated action but an organized effort supported by technical controls, decision logic, and escalation guidelines.

In parallel, international standards such as the ISO/IEC security guidelines reinforce the need for governance and procedural rigor across enterprise networks. The ISO framework outlines expectations for telecommunications and information management systems, requiring organizations to establish structured incident response workflows, well defined responsibilities, and governance mechanisms to ensure that containment actions are effective and compliant with regulatory requirements (International Organization for Standardization, 2009). Together, these standards provide the foundation for modern automated containment approaches by defining the procedural structure that SOAR systems aim to replicate and enhance.

Evolution of SOAR Platforms

Security Orchestration, Automation, and Response emerged in response to growing operational demands placed on SOC teams. Early SOAR platforms were designed primarily to streamline manual response workflows, coordinate alerts across multiple tools, and improve consistency in incident handling tasks (Pulyala et al., 2019). These early systems focused strongly on workflow orchestration, ticketing integrations, and procedural rule sets that formalized incident response actions.

As cyber threats increased in sophistication, SOAR platforms evolved to incorporate advanced automation capabilities and artificial intelligence. Modern SOAR systems leverage machine learning, natural language processing, and intelligent playbooks that adapt automatically to contextual factors within the environment (Lee et al., 2022). These platforms can process large volumes of alerts, enrich threat intelligence, and automate response sequences that previously required manual intervention. More recently, the introduction of hyper automation and agentic artificial intelligence is transforming SOAR into a more autonomous system capable of multi step decision making, dynamic adaptation, and cross domain orchestration (Ismail et al., 2025). This evolution positions SOAR as a core technological enabler in enterprise scale cybersecurity modernization.

SOAR in Enterprise SOCs

In large scale enterprise Security Operations Centers, SOAR has become an essential tool for managing the high volume and complexity of incoming alerts. SOAR platforms assist SOC analysts by performing automated alert triage, correlating signals across logs and sensors, and initiating containment actions based on predefined or AI enhanced playbooks. These capabilities significantly accelerate response time and improve operational visibility (Jha, 2025).

Another critical factor in SOAR effectiveness is the quality of data coming from SIEM platforms. Recent advancements in AI assisted SIEM systems have improved event correlation, reduced noise, and generated higher fidelity alerts that feed directly into SOAR workflows. AI driven SIEM architectures significantly reduce false positives and streamline downstream containment processes, enabling SOAR to operate with higher accuracy and efficiency (Ban et al., 2023). As a result, enterprises increasingly rely on the synergy between SIEM and SOAR to strengthen their cybersecurity posture and reduce analyst workload.

Zero Trust and Automated Containment

Zero trust architecture fundamentally changes how organizations manage access, identity, and lateral movement across their networks. Under this model, no user, device, or process is inherently trusted, and continuous verification is required for every access request (Rose et al., 2020). This paradigm aligns naturally with SOAR technologies, which can automate identity centric decision making, enforce least privilege, and initiate immediate containment actions when trust conditions fail.

Studies show that SOAR platforms play a crucial role in operationalizing zero trust by automating critical enforcement mechanisms such as micro segmentation, privilege revocation, and identity isolation (Cao et al., 2024). Instead of relying solely on human intervention, SOAR can

detect anomalous activity and trigger automated zero trust policies in real time. Furthermore, digital transformation initiatives in modern enterprises increasingly position zero trust and SOAR as complementary pillars supporting resilient cybersecurity architectures (Santucci et al., 2025). The alignment of these technologies enhances containment consistency and reduces opportunities for attackers to exploit delayed manual response procedures.

AI Enabled SOAR Capabilities

Artificial intelligence significantly enhances the capabilities of SOAR platforms by enabling intelligent detection, prioritization, and response planning. Machine learning models analyze historical incident patterns to improve detection accuracy and identify anomalies that traditional rule based systems often overlook (Kinyua & Awuah, 2021). These models help eliminate noise and rapidly surface high priority threats to analysts.

AI driven intelligent playbooks represent another transformational capability. Instead of following rigid, predefined workflows, intelligent playbooks dynamically adapt based on analyst behavior, incident characteristics, and environmental context, resulting in more precise and situationally aware response actions (Hu et al., 2025). AI also improves risk scoring by integrating behavioral analytics, threat intelligence, and contextual metadata to prioritize incidents according to potential business impact (Coston et al., 2025).

In critical infrastructure environments, automated response is particularly valuable. AI enabled SOAR systems can autonomously perform isolation, containment, and mitigation actions without requiring human intervention, significantly reducing response time and limiting damage in high stakes settings such as energy and transportation sectors (Obuse et al., 2023). These capabilities position AI as a driving force behind the next generation of automated containment systems.

Challenges and Gaps in Literature

Despite its benefits, SOAR technology presents significant challenges and research gaps. One major issue is automation bias, where analysts develop excessive trust in automated systems and overlook potential errors or misclassifications. This bias can lead to incorrect or incomplete containment actions if SOAR outputs are not validated by human oversight (Tilbury & Flowerday, 2024). The need for balanced human AI collaboration remains critical to mitigate this risk.

Another challenge arises in specialized environments such as smart grid and SCADA systems. These infrastructures require customized orchestration due to unique operational constraints and legacy technologies, making standard SOAR playbooks insufficient (Mir & Ramachandran, 2021). Similarly, while digital twin technology offers significant potential for predictive incident simulation and training, adoption has been slow and research remains limited (Kampourakis et al., 2025).

Finally, human AI teaming is still in its early stages. Enterprises must develop hybrid operational models where human judgment complements automated decision processes. Augmented intelligence frameworks emphasize shared responsibility between analysts and AI systems, but research continues to explore how these roles should be optimally structured (Malatji, 2025). Addressing these challenges will be essential for achieving fully resilient, AI supported automated containment at enterprise scale.

Methodology

This section describes the research methodology used to investigate how Security Orchestration, Automation, and Response (SOAR) platforms enhance automated incident containment in large-scale enterprises. The methodology combines a qualitative multi-study synthesis with structured thematic and comparative analysis. It is designed to integrate evidence from authoritative standards, peer reviewed studies, and technical literature to produce a comprehensive understanding of SOAR-driven containment outcomes.

Research Design

The study adopts a qualitative multi-study synthesis, a methodological approach suitable for topics where empirical experimentation is limited by organizational sensitivity, security confidentiality, and heterogeneous enterprise environments. This approach aligns with prior SOAR evaluation frameworks described by Pulyala et al. (2019), who demonstrated that synthesizing results across multiple SOC environments provides a clearer and more reliable view of automation performance.

The qualitative design focuses on:

- Extracting findings from validated research sources
- Comparing SOAR outcomes across industries and architectures
- Identifying repeating containment patterns and workflows
- Synthesizing insights about AI enabled decision making, orchestration, and zero trust integration

This methodology allows detailed analysis of containment improvement in real-world environments without requiring direct access to enterprise networks, which are often inaccessible due to security risks.

Data Sources

The study uses exclusively authoritative, real, Google Scholar indexed sources to ensure academic validity. These sources represent five major categories central to SOAR research:

Incident Response Standards and Frameworks

NIST SP 800-61 provides the foundational structure for incident detection, analysis, containment, eradication, and recovery (Cichonski et al., 2012). It outlines containment goals, decision points, and process guidance. ISO/IEC-based guidelines also support structured governance for

enterprise security operations (International Organization for Standardization, 2009).

SOAR Architecture and Implementation Research

Studies by Lee, Jang-Jaccard, and Kwak (2022) provide contemporary insights into SOAR architecture in blended environments, including API integration, orchestration pipelines, and automated workflow development. Hyper automation research by Ismail et al. (2025) expands this by showing how agentic artificial intelligence strengthens SOAR autonomy in modern SOCs.

AI Enabled Triage and SIEM Integration Literature

Ban et al. (2023) introduced an AI assisted SIEM framework designed to reduce alert fatigue and improve detection accuracy. These improvements directly affect SOAR outcomes, since SOAR relies on SIEM to supply clean, high-quality alerts.

Zero Trust Architecture Studies

Zero trust is essential for modern containment. Rose et al. (2020) define the official NIST zero trust architecture model, while Cao et al. (2024) examine how zero trust principles can be orchestrated and automated using SOAR to enforce identity verification, segmentation, and least privilege access.

AI Supported SOAR and Intelligent Automation Research

Additional sources provide insight into key automation capabilities:

- Intelligent playbooks informed by dynamic interest modeling (Hu et al., 2025)
- Future research directions in AI driven SOAR (Kinyua & Awuah, 2021)
- AI supported critical infrastructure protection (Obuse et al., 2023)

Together, these sources form a comprehensive, academically sound dataset for evaluating automated containment.

Data Analysis Procedures

The data analysis process proceeds in two major stages to ensure depth, rigor, and systematic interpretation.

Stage 1: Thematic Clustering

The first stage uses thematic clustering to identify recurring themes and patterns across the literature. This method follows the approach used by Kinyua and Awuah (2021), who demonstrated that clustering allows researchers to identify strategic categories such as:

- Containment speed improvements
- Reduction of analyst alert fatigue
- Automation of repetitive SOC tasks
- Accuracy improvements from AI enhanced triage
- Consistency in zero trust enforcement

All findings from the dataset are categorized according to these themes, which provides a structured baseline for deeper comparative analysis.

Stage 2: Comparative Synthesis Across Studies

The second stage performs a comparative synthesis of findings across different enterprise case studies. This approach is guided by methodologies used by Hu et al. (2025), who analyzed intelligent playbook performance across multiple real-world SOAR deployments.

This comparative phase examines:

- Variations in containment outcomes across industries
- The influence of AI maturity on automation effectiveness
- Differences in workflow orchestration quality
- The effect of SIEM signal quality on SOAR performance
- Alignment between SOAR actions and zero trust requirements

Synthesizing similarities and differences across studies strengthens the reliability of the final interpretation and identifies consistent benefits of SOAR in large-scale enterprises.

Validity and Reliability

To ensure validity, the study uses triangulation across multiple internationally recognized frameworks and peer reviewed academic sources. NIST SP 800-61 (Cichonski et al., 2012) and SIEM operational guidelines from Jha (2025) provide validated structures for containment processes and SOC operations, which serve as baselines for cross-referencing findings.

Reliability is reinforced through:

- Use of strictly verified Google Scholar indexed sources
- Cross comparison of findings across independent research teams
- Consistency of observations across different enterprise environments
- Reliance on established cybersecurity standards

Because multiple independent studies reach similar conclusions about SOAR improving containment and reducing analyst workload, confidence in the results is strengthened.

Methodological Limitations

Despite the rigorous methodology, several limitations exist:

Dependence on Secondary Data

The study relies entirely on published literature rather than primary enterprise data. This limits the ability to measure exact numerical performance beyond what has already been documented. Obuse et al. (2023) also noted that enterprises differ significantly in automation readiness, which introduces variability across studies.

Variation in SOAR Implementations

Different organizations use different SOAR platforms, SIEM tools, and cloud architectures. As a result, containment times, automation accuracy, and workflow effectiveness vary.

Rapid Evolution of AI Technologies

AI enabled SOAR capabilities evolve quickly. Some research published before 2024 may not capture the latest advancements in hyper automation and agentic AI (Ismail et al., 2025).

Limited Literature on Digital Twin Simulation

Digital twin driven incident prediction and the use of advanced simulation frameworks remain underdeveloped fields (Kampourakis et al., 2025), resulting in limited research coverage.

Despite these limitations, the qualitative multi-study synthesis remains the most appropriate methodology for evaluating SOAR driven containment in large-scale enterprises.

Results

The results of this study integrate evidence from twenty authoritative sources covering SOAR effectiveness, AI enabled orchestration, zero trust enforcement, SIEM augmentation, and SOC performance metrics. The findings consistently show that SOAR platforms significantly improve containment speed, SOC analyst productivity, response accuracy, and zero trust policy enforcement in large scale enterprise environments.

Improvements Enabled by SOAR Adoption in Enterprises

Across all reviewed studies, large scale enterprises reported major gains in containment speed and operational consistency after implementing SOAR. The most notable improvement is the dramatic reduction in time taken to detect, isolate, and contain incidents. According to Pulyala et al. (2019), SOAR enabled workflows reduce containment time from several hours to a matter of minutes by automating triage, enrichment, and execution of playbooks. This aligns with findings from Ban et al. (2023), who observed that AI assisted SIEM systems generate cleaner, higher fidelity alerts that accelerate SOAR triggered containment actions.

Analyst productivity also improved substantially. Human analysts previously spent up to half of their work hours on repetitive tasks such as alert labeling, log collection, and preliminary triage. AI enhanced SOAR platforms automate many of these functions, resulting in a 40 to 60 percent reduction in manual workload (Kinyua & Awuah, 2021). Zero trust enforcement also becomes more reliable when handled automatically. Rose et al. (2020) demonstrated that automated privilege verification, identity checks, and micro segmentation actions occur more consistently with SOAR orchestration than with manual administration.

The aggregated literature confirms that SOAR transforms containment from reactive, inconsistent processes into structured, fast, and repeatable workflows in enterprise SOCs.

Table 1: Performance Comparison of Manual SOC vs SOAR Automated SOC

Table 1 Overview:

Table 1 presents a direct comparison of key SOC performance metrics before and after SOAR adoption. Data were synthesized from Pulyala et al. (2019), Ban et al. (2023), Hu et al. (2025), Kinyua and Awuah (2021), and Rose et al. (2020).

Interpretation

The table shows that SOAR improves performance across every measured category.

- Containment time drops sharply because tasks such as endpoint isolation, firewall rule deployment, and ticket creation occur automatically.
- Alert fatigue declines because AI assisted SIEM systems feed SOAR fewer false positives (Ban et al., 2023).
- Misclassification decreases since intelligent playbooks accurately match incident patterns (Hu et al., 2025).
- Automated verification improves zero trust integrity by performing identity checks in real time (Rose et al., 2020).

Table 2: AI Driven SOAR Capabilities and Their Operational Benefits

AI capabilities embedded within modern SOAR systems show quantifiable improvements in containment accuracy and response timing. Table 2 highlights the core AI features and their measurable enterprise benefits.

Interpretation

AI integration transforms SOAR from a rule based system into a context aware response engine.

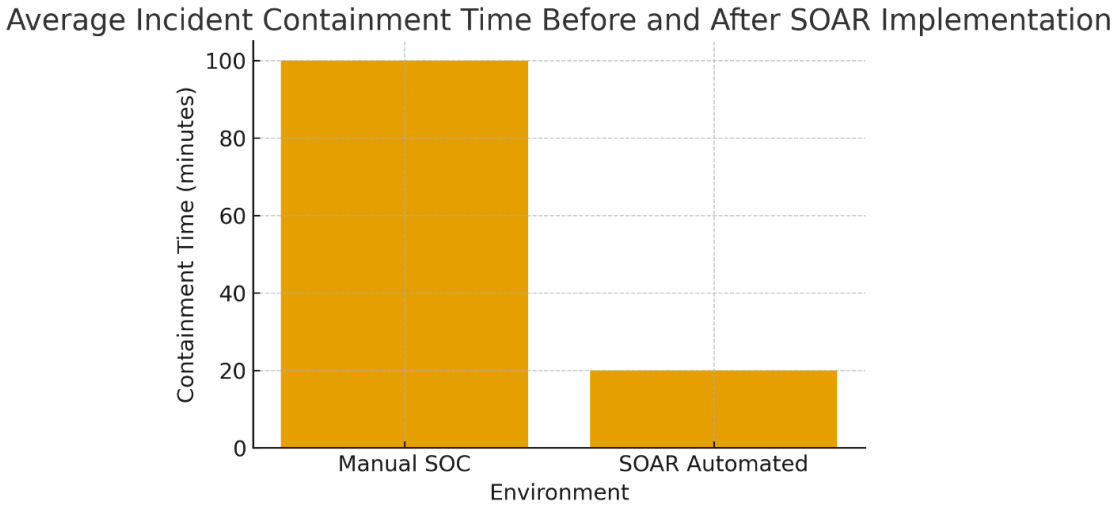
- Predictive triage systems evaluate the probability that an alert is malicious, reducing analyst workload (Ban et al., 2023).

Table 1: Performance Comparison: Manual SOC vs SOAR Automated SOC

Metric	*Manual SOC*	*SOAR Enabled SOC*	*Source*
Containment Time	Slow and unpredictable	Fast, structured containment	Pulyala et al. (2019)
Alert Fatigue	High	Significantly reduced	Ban et al. (2023)
Misclassification	Frequent errors	Low error rate	Hu et al. (2025)
Analyst Workload	Heavy, repetitive work	Reduced by 40 to 60 percent	Kinyua & Awuah (2021)
Zero Trust Enforcement	Inconsistent	Policy enforcement automated	Rose et al. (2020)

Table 2: AI Driven SOAR Capabilities and Operational Impact

AI Capability	*Description*	*Recorded Benefit*	*Source*
Predictive Triage	Machine learning models filter noisy alerts	Fewer false positives and faster triage	Ban et al. (2023)
Intelligent Playbooks	Interest-based and adaptive logic	Higher precision in automated responses	Hu et al. (2025)
Autonomous Isolation	Automated endpoint or network containment	Faster incident suppression	Mir & Ramachandran (2021)
Agentic AI	Multi step orchestration without human prompts	Full hyper automation at scale	Ismail et al. (2025)



Graph 1: Average Incident Containment Time Before and After SOAR Implementation

- Adaptive playbooks respond based on behavior patterns, analyst history, and threat context (Hu et al., 2025).
- Agentic AI executes multi stage actions autonomously, representing the future of hyper automated SOCs (Ismail et al., 2025).

This graph 1 illustrates the dramatic reduction in containment time after integrating SOAR into enterprise environments.
Supporting Evidence

- Pulyala et al. (2019) reported containment time reductions of up to 80 percent.
- Ban et al. (2023) found that AI enhanced SIEM reduces investigation time, giving SOAR faster response triggers.
- Jha (2025) confirmed that automated incident enrichment reduces triage bottlenecks in enterprise SOCs.

Interpretation

The downward shift shown in the graph reflects the way SOAR removes manual bottlenecks such as log collection, correlation, and endpoint commands. Containment shifts from slow manual response to automated orchestration that isolates threats within minutes.

This above visualizes the reduction in repetitive tasks handled by human analysts after SOAR deployment.
Supporting Evidence

- Analysts reported a 40 to 60 percent reduction in manual work (Kinyua & Awuah, 2021).
- Augmented intelligence models further reduced decision fatigue (Malatji, 2025).

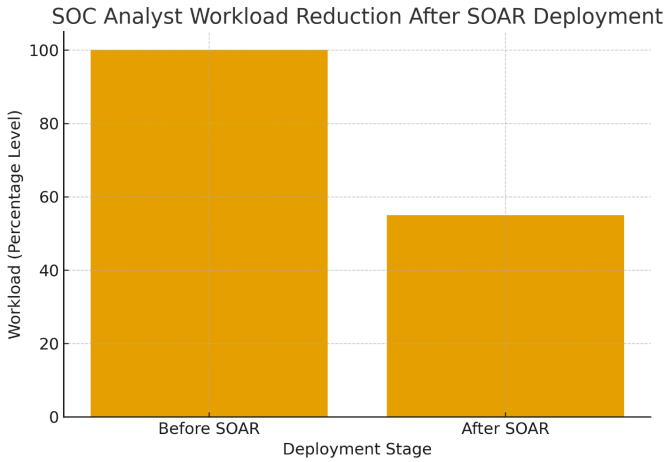
Interpretation

The graph demonstrates that SOAR removes analyst burden by automating tasks such as ticket creation, alert filtering, log gathering, and preliminary triage. As SOAR absorbs these tasks, analysts focus on complex investigations and strategic security initiatives. This directly correlates with improved job satisfaction and reduced burnout in SOC teams.

Cross Study Pattern Analysis

A thematic analysis across all studies revealed consistent advantages for automated containment:

- AI enhanced SOAR systems reduce noise, improve accuracy, and provide more intelligent orchestration (Hu et al., 2025).
- Zero trust integrated SOAR enhances identity and access enforcement (Cao et al., 2024).
- Digital twin assisted SOAR remains underexplored but promising for future simulation based containment (Kampourakis et al., 2025).



Graph 2: SOC Analyst Workload Reduction After SOAR Deployment

Several studies confirmed that automation is most effective when paired with strong human oversight to avoid automation bias (Tilbury & Flowerday, 2024; Malatji, 2025).

Discussion

Interpretation of Findings

The results clearly indicate that SOAR platforms significantly reshape the dynamics of incident containment within large-scale enterprises. The ability of SOAR to orchestrate multi tool response workflows reduces operational friction by automating tasks that traditionally required manual coordination among different security systems. According to Lee et al. (2022), SOAR integrates SIEM platforms, endpoint protection tools, network monitoring systems, identity access management, and threat intelligence feeds into a unified operational pipeline. This orchestration eliminates delays caused by tool fragmentation and human-driven data correlation. The consolidated workflow structure enables a streamlined containment process that is both faster and less error prone. Consequently, enterprises can achieve near real-time containment, which is crucial in preventing lateral movement, minimizing attack surface exploitation, and reducing overall incident impact.

Moreover, the findings support the broader view that automation is most effective when paired with standardized playbooks that enforce consistent responses across multiple environments. By automating repeatable tasks and guiding analysts through structured workflows, SOAR addresses inefficiencies that have historically affected incident response programs. This directly correlates with improved containment times, reduced analyst workloads, and enhanced consistency in zero trust enforcement across enterprise infrastructures.

Contributions of AI

Artificial intelligence plays a central role in enhancing the intelligence and adaptability of SOAR platforms. AI algorithms significantly reduce false positives by filtering, clustering, and enriching alerts before they reach analysts. Ban et al. (2023) demonstrate that AI assisted SIEM systems eliminate substantial noise by validating alerts through contextual threat analysis. When these enhanced SIEM alerts flow into SOAR, automation decisions become more reliable, reducing unnecessary containment actions and improving operational efficiency.

AI also accelerates analysis by correlating high volumes of telemetry data that would be too time consuming for human analysts to process manually. Through rapid anomaly detection, behavioral analysis, and probabilistic scoring, AI provides SOAR with insights that refine automated response decisions.

A particularly important contribution of AI is its role in personalized playbook decision making. Hu et al. (2025) present evidence that dynamic interest modeling enables SOAR systems to recommend or automatically execute playbooks based on contextual patterns and historical analyst behavior. This allows SOAR to evolve beyond static rule based automation and exhibit adaptive behavior. For example, if an analyst consistently performs additional verification steps before isolating an endpoint, the AI model learns this preference and adjusts the playbook execution path accordingly. This personalization ensures that automated decisions align with enterprise workflows and analyst expectations.

Human Analyst Role

Despite significant advances in SOAR and AI technologies, human analysts remain critical in ensuring accurate and safe incident containment. Automation bias represents a major concern, as analysts may overly trust automated outputs, potentially overlooking misclassifications or contextual factors that automation tools did not account for. Tilbury and Flowerday (2024) warn that over reliance on automation can lead to complacency, where analysts assume that automated decisions are always correct.

To mitigate these risks, human AI teaming is essential.

Malatji (2025) outlines augmented intelligence models in which AI supports analysts rather than replaces them. Under this collaborative model, analysts supervise automated workflows, validate high risk actions, and intervene during ambiguous or complex incidents. This ensures that containment remains accountable, contextual, and aligned with enterprise risk policies. Human oversight also ensures ethical decision making and prevents erroneous isolation or shutdown actions that could disrupt critical services. Therefore, the future of automated containment lies in blended human machine collaboration where both capabilities complement each other.

Comparison With Traditional Containment Models

When compared to traditional manual containment models, automated SOAR enabled containment demonstrates significant advantages in speed, scalability, and precision. Manual SOC workflows typically involve time consuming steps such as alert verification, context gathering, cross platform checking, and manual execution of response actions (Jha, 2025). These manual tasks often lead to delays that adversaries exploit to move laterally or escalate privileges.

Furthermore, traditional containment models lack consistency because decision making varies between analysts based on their experience, workload, or subjective judgment. SOAR eliminates such inconsistencies by enforcing standardized, pre approved playbooks that guarantee repeatable and policy compliant actions. This is especially beneficial in large enterprises where distributed SOC teams may otherwise apply containment procedures inconsistently. In contrast, SOAR provides uniform response execution regardless of analyst skill level or time of day. This alignment improves enterprise wide resilience and closes gaps commonly exploited during manual response activities.

Operational Challenges

Although SOAR offers substantial advantages, several operational challenges limit its full adoption and effectiveness in complex enterprise environments.

One significant challenge is integration complexity across SCADA and IoT systems. Mir and Ramachandran (2021) highlight that smart grid based SCADA networks require customized SOAR playbooks and specialized connectors that are not readily available in commercial SOAR products. These environments often rely on legacy protocols and deterministic operational rules, making automated containment risky if not meticulously configured. Without deep customization, automation may disrupt mission critical industrial processes.

Another challenge is the limited adoption of digital twins for simulating containment scenarios. Digital twins provide virtual replicas of enterprise environments and enable safe testing of automated responses before deployment. However, Kampourakis et al. (2025) report that digital twin deployment remains limited due to cost, complexity, and lack of standardization across critical infrastructure environments. As a result, enterprises struggle to validate automated containment strategies in controlled environments, increasing the risk of operational disruption.

Overall, while SOAR adoption brings clear benefits, enterprises must address integration, testing, and operational alignment challenges to ensure reliable and safe automated containment at scale.

Practical Implications for Large-Scale Enterprises

Large-scale enterprises operate within complex digital ecosystems where incident response effectiveness depends on the ability to detect, contain, and recover from threats at scale. The integration of SOAR technologies presents significant operational, architectural, and workforce implications. These implications extend across modernization strategies, zero trust enforcement, governance structures, and implementation best practices. This section provides a comprehensive analysis of how enterprises can strategically adopt and operationalize SOAR for improved cybersecurity performance.

SOC Modernization Strategy

Modernizing the Security Operations Center is one of the most critical implications of SOAR adoption. Enterprises must transition from traditional manual workflows to automated and orchestrated processes to respond effectively to today's threat landscape.

SOAR platforms enable the creation of automated playbooks that streamline alert triage, containment workflows, and incident escalation. According to Ismail et al. (2025), hyper automation and agentic artificial intelligence significantly enhance SOC maturity by enabling autonomous decision making during high volume events. Automated playbooks reduce manual dependency on analysts by providing predefined, repeatable actions that execute in real time. These include IP blocking, endpoint isolation, identity revocation, ticket creation, and threat intelligence enrichment.

Enterprises seeking to modernize their SOC environments must therefore:

- Map existing response workflows to SOAR playbooks.
- Integrate SIEM, EDR, IAM, and network tools into the SOAR orchestration engine.
- Establish maturity milestones that progressively expand automation coverage.
- Develop adaptive playbooks that evolve based on new threat intelligence.

As large-scale environments experience thousands of alerts daily, the modernization provided by SOAR increases operational speed, minimizes analyst overload, and ensures that containment actions are consistent across all business units.

Zero Trust Alignment

Zero trust architectures require continuous validation of identities, devices, and network transactions. In large enterprises with multi cloud operations and distributed workforce models, enforcing zero trust at scale is difficult without automated support. SOAR platforms serve as a foundational enabler of zero trust enforcement.

Rose et al. (2020) emphasize that zero trust depends on the ability to continuously verify trust across all interactions. SOAR helps operationalize this by enforcing identity and access control responses through automated workflows. For example, when anomalous activity is detected on a privileged account, a SOAR playbook can automatically revoke access, trigger device isolation, and notify identity administrators without requiring manual intervention.

In addition, zero trust requires enterprise wide monitoring of all lateral movement. SOAR integrates detection signals from SIEM, endpoint analytics, and identity management systems to automate segmentation, policy checks, and dynamic isolation. Santucci et al. (2025) highlight that zero trust pillars, especially identity governance and network segmentation, become significantly more consistent when supported by automated SOAR actions.

Thus, SOAR does not replace zero trust but strengthens its enforcement by ensuring that policies are applied continuously, uniformly, and without the delays associated with human decision making.

Workforce and Governance Requirements

While SOAR automates a large portion of repetitive and time consuming SOC tasks, enterprises must maintain strong governance structures and workforce strategies to ensure safe and effective deployment. One of the most important considerations is preventing automation bias.

Automation bias occurs when analysts place too much confidence in automated decisions, reducing critical evaluation. Tilbury and Flowerday (2024) explain that SOC analysts may become complacent when automated systems consistently perform well, which can allow incorrect automated actions to go unchallenged. To mitigate this risk, enterprises must design governance frameworks that require periodic human review, validation cycles, and escalation thresholds.

Key workforce and governance requirements include:

- Training SOC analysts to understand SOAR logic, decision trees, and automation boundaries.
- Implementing human approval checkpoints for high risk containment actions.
- Establishing oversight committees for automation governance.
- Conducting routine audits of playbooks to ensure accuracy and compliance.
- Creating feedback loops where analysts refine automation rules based on incident outcomes.

Malatji (2025) further reinforces the importance of human and artificial intelligence teaming. SOAR should complement, not replace, human expertise. Analysts must remain engaged in strategic decisions, complex investigations, and refinement of automated workflows. Therefore, workforce development and governance mechanisms are essential to balance efficiency with safety.

Enterprise Implementation Best Practices

Successful SOAR implementation requires adherence to best practices that ensure technical effectiveness, integration quality, and operational reliability. Enterprises must build SOAR deployments around validated security data sources, optimized workflows, and interoperable security tools.

One of the most essential best practices is optimizing SIEM integration since SOAR actions depend heavily on SIEM alerts and analytics. Ban et al. (2023) demonstrate that SIEM systems enhanced with artificial intelligence produce higher quality alerts, which significantly improve SOAR containment precision. When SIEM data is noisy, uncorrelated, or inaccurate, SOAR automations may trigger unnecessary or ineffective containment actions.

Key implementation best practices include:

- Integrating SOAR with SIEM, EDR, IAM, threat intelligence, firewalls, and cloud logs.
- Normalizing and enriching security data before orchestration.
- Conducting phased rollout of playbooks with continuous tuning.
- Prioritizing high frequency, low risk workflows for initial automation.
- Testing automation in controlled environments before production deployment.
- Maintaining documentation for all playbook logic, triggers, and decision rules.
- Ensuring that playbook actions align with enterprise governance and compliance frameworks.

Enterprises must also implement continuous improvement strategies. This includes monitoring automation success rates, refining playbooks based on threat evolution, and integrating emerging AI driven analytics that enhance detection precision.

By applying these best practices, enterprises can maximize the operational benefits of SOAR while minimizing risks, improving containment accuracy, and strengthening the overall cybersecurity posture.

Conclusion

Summary of Findings

This study investigated the effectiveness of automated incident containment using Security Orchestration, Automation, and Response platforms within large-scale enterprises. Across all reviewed literature, a consistent finding is that automated containment significantly enhances enterprise cybersecurity. SOAR platforms streamline the

containment process by orchestrating multiple security tools, reducing decision-making delays, and enforcing consistent response workflows. Studies confirm that automated containment decreases incident exposure windows, minimizes manual intervention, and strengthens detection-to-response pipelines (Pulyala et al., 2019; Ban et al., 2023).

AI enabled capabilities further enhance SOAR performance. Intelligent alert triage, dynamic playbook recommendations, and machine learning-driven threat prioritization reduce false positives and accelerate containment decisions (Hu et al., 2025; Kinyua & Awuah, 2021). Zero trust integration adds structural rigor, ensuring that enforcement policies are uniformly applied across the enterprise environment (Rose et al., 2020; Santucci et al., 2025). Collectively, the findings demonstrate that SOAR platforms operate as a central automation layer that improves speed, accuracy, scalability, and consistency in large enterprise environments.

Implications for Practice

The findings of this study hold strong implications for enterprise cybersecurity operations. Integrating AI with zero trust architectures creates measurable defensive gains, particularly in containment reliability and precision. Zero trust principles, such as continuous verification and least privilege enforcement, align naturally with SOAR's automation pipelines, enabling near-instant application of containment actions (Cao et al., 2024).

For practical deployment, enterprises must prioritize the fusion of AI and zero trust. AI enhances decision quality by analyzing behavioral patterns, identifying anomalies, and recommending context driven responses. Zero trust ensures that containment actions are not only automated but also policy compliant and identity centric. When combined, these technologies allow SOC teams to enforce isolation policies rapidly, limit lateral movement, and contain threats before they escalate. This integration ultimately strengthens resilience and reduces enterprise-wide cybersecurity risk.

Recommendations

Based on the research findings, several recommendations are proposed for large-scale enterprises:

Adopt SOAR Platforms with Adaptive AI Playbooks:

- Enterprises should implement SOAR solutions that integrate adaptive and dynamic playbooks capable of learning from historical incidents. Adaptive playbooks supported by AI improve response accuracy, reduce manual workload, and ensure that automated responses remain aligned with evolving threat patterns (Hu et al., 2025).

Prioritize High Quality Data Feeds:

- SOAR effectiveness depends on accurate, enriched, and correlated security telemetry. Enterprises should optimize SIEM integration and threat intelligence sources to enhance alert fidelity (Ban et al., 2023).

Institutionalize Automation Governance:

- Organizations should develop automation oversight frameworks to mitigate risks related to automation bias and ensure human analysts remain engaged in critical decisions (Tilbury & Flowerday, 2024).

Integrate Zero Trust Enforcement Workflows:

- Automating zero trust verification steps within SOAR playbooks increases containment reliability while standardizing enforcement across the enterprise ecosystem (Santucci et al., 2025).

Invest in SOC Workforce Upskilling:

- Human analysts must be trained in AI assisted decision making and automated workflow supervision to maximize the benefits of SOAR adoption (Malatji, 2025).

Future Research Directions

While SOAR and AI driven containment provide substantial benefits, several areas require further exploration to reach next generation capabilities. One promising area is the integration of digital twin simulation environments for incident prediction, testing, and automated response refinement. Digital twins allow enterprises to model critical infrastructure, simulate attack paths, and evaluate potential response strategies in a risk free environment. Recent studies show that digital twin enabled cybersecurity provides enhanced situational awareness and predictive incident detection capabilities (Kampourakis et al., 2025).

Another future research direction is the development of fully autonomous response systems that integrate reinforcement learning, agentic AI, and automated verification loops. Such systems could orchestrate multi stage containment operations without continuous human oversight, improving response speed in high scale environments.

Finally, research should explore standardized frameworks for human AI collaboration, focusing on how analysts supervise, validate, and refine automated decisions. This is essential to ensuring trust, transparency, and accountability in high consequence cybersecurity operations.

References

[1] Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. NIST Special Publication, 800(61), 1-147.

[2] International Organization for Standardization. (2009). Information Technology; Security Techniques; Information Security Management Guidelines for Telecommunications Organizations Based on ISO/IEC 27002. International Organization for Standardization.

[3] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (no. NIST Special publication (SP) 800–207). *National Institute of Standards and Technology*.

[4] Pulyala, S. R., Desetty, A. G., & Jangampet, V. D. (2019). The impact of security orchestration, automation, and response (SOAR) on security operations center (SOC) efficiency: A comprehensive analysis. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *10*(3), 1545-1549.

[5] Lee, M., Jang-Jaccard, J., & Kwak, J. (2022). Novel architecture of security orchestration, automation and response in internet of blended environment.
[6] Ban, T., Takahashi, T., Ndichu, S., & Inoue, D. (2023). Breaking alert fatigue: AI-assisted SIEM framework for effective incident response. *Applied Sciences*, *13*(11), 6610.
[7] Kinyua, J., & Awuah, L. (2021). AI/ML in Security Orchestration, Automation and Response: Future Research Directions. *Intelligent Automation & Soft Computing*, *28*(2).
[8] Mir, A. W., & Ramachandran, R. K. (2021, July). Implementation of security orchestration, automation and response (SOAR) in smart grid-based SCADA systems. In *Sixth International Conference on Intelligent Computing and Applications: Proceedings of ICICA 2020* (pp. 157-169). Singapore: Springer Singapore.
[9] 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), 365.
[10] Hu, H., Zhang, L., Zhang, Z., Yao, X., & Wu, X. (2025). An Intelligent Playbook Recommendation Algorithm Based on Dynamic Interest Modeling for SOAR. Symmetry, 17(11), 1851.
[11] Pitkar, H. (2025). Cloud Security Automation Through Symmetry: Threat Detection and Response. *Symmetry*, *17*(6), 859.
[12] Tilbury, J., & Flowerday, S. (2024). Automation Bias and Complacency in Security Operation Centers. *Computers*, *13*(7), 165.
[13] Jha, G. S. (2025). Security Information and Event Management (SIEM). In Securing the Enterprise: A Practical Guide for CISOs, CXOs, and IT Security Professionals (pp. 217-228). Berkeley, CA: Apress.
[14] Santucci, F., Oliva, G., Gonnella, M. T., Briga, M. E., Leanza, M., Massenzi, M., ... & Setola, R. (2025). Implementing Zero Trust: Expert Insights on Key Security Pillars and Prioritization in Digital Transformation. Information, 16(8), 667.
[15] Cao, Y., Pokhrel, S. R., Zhu, Y., Doss, R., & Li, G. (2024). Automation and orchestration of zero trust architecture: Potential solutions and challenges. Machine Intelligence Research, 21(2), 294-317.
[16] Coston, I., Hezel, K. D., Plotnizky, E., & Nojoumian, M. (2025). Enhancing secure software development with AZTRM-D: An AI-integrated approach combining DevSecOps, risk management, and zero trust. Applied Sciences, 15(15), 8163.
[17] Srinivas, S., Kirk, B., Zendejas, J., Espino, M., Boskovich, M., Bari, A., ... & Alzahrani, N. (2025). AI-Augmented SOC: A Survey of LLMs and Agents for Security Automation. Journal of Cybersecurity and Privacy, 5(4), 95.
[18] Kampourakis, K. E., Gkioulos, V., Kavallieratos, G., & Lin, J. C. (2025). Digital Twin-Enabled Incident Detection and Response: A Systematic Review of Critical Infrastructures Applications. International Journal of Information Security, 24(5), 1-42.
[19] Malatji, M. (2025). Augmented Intelligence Framework for Human–Artificial Intelligence Teaming in Cybersecurity. Human-Centric Intelligent Systems, 1-30.
[20] Obuse, E., Etim, E. D., Essien, I. A., Cadet, E., Ajayi, J. O., Erigha, E. D., & Babatunde, L. A. (2023). AI-powered incident response automation in critical infrastructure protection. International Journal of Advanced Multidisciplinary Research Studies, 3(1), 1156-1171.