International Journal on Optimization and Applications
IJOA. Vol. 05, Issue No. 03, Year 2025, www.ijoa-journal.com

Automating Incident Response in SOC Using SOAR Platforms: A Case Study with Cortex XSOAR

1st Lamhamdi Ayoub
Master SSI, ENSA Kenitra
Kenitra, Morocco
ayoub.lamhamdi@uit.ac.ma

2nd Pr. Hanaa Hachimi
Full Professor in Applied Mathematics & Computer Science, ENSA Kenitra
Kenitra, Morocco
hanaa.hachimi@uit.ac.ma

***Abstract*—In the face of increasingly complex and frequent cyber threats, Security Operations Cen- ters (SOCs) must ensure rapid and consistent incident response to maintain operational resilience. Traditional approaches, often relying on manual processes, struggle to keep pace with the volume of alerts and the sophistication of attacks, leading to delays and inconsistencies in remediation. To address this challenge, Security Orchestration, Au- tomation, and Response (SOAR) platforms have emerged as a key enabler of automation within SOCs. This article presents a case study on the implementation of automated incident response using Cortex XSOAR. The methodology combines a benchmark of leading SOAR solutions with the design and deployment of practical use cases, including Active Directory protection, phishing email detection and response, and automated reporting from SIEM (QRadar) data. The evaluation highlights significant improvements in Mean Time To Re- spond (MTTR), enhanced traceability of security actions, and reduced analyst workload through standardized playbooks. The main contributions of this work are: (i) a reproducible framework for evaluating SOAR platforms, (ii) a set of reusable playbooks addressing common SOC scenarios, and (iii) insights into the integration of SIEM–SOAR for modern security operations. The results confirm that intelligent orchestration and automation represent a strategic lever to strengthen the eflciency and resilience of SOCs in the face of evolving cyber threats.**

***Index Terms*—SOC, SOAR, Incident Response, Automation, Cortex XSOAR, QRadar, Play- books, Cybersecurity Orchestration.**

I. Introduction

The increasing digitalization of services and the rapid expansion of interconnected systems have dramatically amplified the attack surface of modern organizations. Cyber threats are not only more frequent but also more sophisticated, targeting critical infrastructures, financial institutions, and government services. Security Operations Centers (SOCs) were created to address this challenge by centralizing the detection, analysis, and response to security incidents. However, the efficiency of a SOC is increasingly threatened by two structural challenges: the growing volume of alerts generated by heterogeneous security tools, and the shortage of skilled analysts capable of handling incidents in a timely and consistent manner.

Traditional SOC operations, largely dependent on manual investigation and response processes, often result in delayed reactions, inconsistent decision-making, and increased Mean Time To Respond (MTTR). Such limitations are particularly critical in the context of sophisticated attacks such as phishing campaigns, ransomware, and identity-based attacks that require rapid containment to prevent escalation.

To overcome these challenges, Security Orchestration, Automation, and Response (SOAR) platforms have emerged as a transformative technology. By orchestrating existing security tools, standardizing workflows through playbooks, and automating repetitive tasks, SOAR enhances both the efficiency and consistency of incident response. In addition, SOAR platforms enable better traceability of analyst actions, improved knowledge retention within the SOC, and more effective prioritization of alerts based on contextual enrichment.

This article explores the use of a SOAR platform, specifically Cortex XSOAR, to automate incident response workflows in a SOC. The objectives are threefold:

- Benchmarking SOAR solutions – Conducting a comparative evaluation of major SOAR platforms according to both technical and operational criteria.
- Implementing use cases – Deploying automation playbooks for realistic SOC scenarios, including Active Directory protection, phishing detection and response, and automated reporting from SIEM data (QRadar).
- Assessing the impact – Evaluating the improvements in responsiveness, traceability, and workload

reduction resulting from automation.

The main contributions of this work are:

- A reproducible evaluation framework for SOAR platforms that combines functional coverage with operational metrics such as scalability, ease of use, and resilience to workforce turnover.
- An implementation of practical playbooks in Cortex XSOAR, covering critical SOC scenarios and demonstrating the potential of automation in real-world contexts.
- A discussion of integration challenges and best practices, particularly regarding interoperability between SIEM and SOAR platforms. Section II reviews the related work and situates SOAR in the broader SOC ecosystem. Section III presents the methodology adopted, including the benchmark process and use case design. Section IV reports the experimental results of the implementation with Cortex XSOAR. Section V discusses the findings, limitations, and perspectives. Finally,Section VI concludes the paper and outlines directions for future research.

II. Related Work

The Security Operations Center (SOC) has become the cornerstone of modern cybersecurity strategies. Its mission is to provide centralized monitoring, detection, and response to security incidents across the entire IT infrastructure. However, traditional SOCs face several challenges. First, the volume of security alerts generated by heterogeneous systems such as firewalls, intrusion detection systems, endpoint protection, and SIEM platforms can be overwhelming. Studies show that analysts are often unable to investigate more than a fraction of these alerts, resulting in missed or delayed responses. Second, the manual nature of incident response workflows introduces inconsistencies and delays, which directly impact the Mean Time To Respond (MTTR) and expose organizations to prolonged threats.

A. SOC and SIEM limitations.

To improve detection and centralization, Security Information and Event Management (SIEM) systems have long been the backbone of SOCs. SIEM platforms collect, normalize, and correlate security events from multiple sources. They provide valuable visibility and support compliance requirements. However, SIEMs are primarily focused on detection and alerting rather than remediation. As a result, analysts must manually investigate SIEM alerts, correlate them with external intelligence, and take response actions across multiple security tools. This dependence on human intervention increases operational costs and slows down response times.

B. Emergence of SOAR.

To address these limitations, Security Orchestration, Automation, and Response (SOAR) platforms have emerged. SOAR extends SIEM capabilities by enabling orchestration across heterogeneous tools, enrichment of alerts with threat intelligence, and automation of repetitive tasks through playbooks. SOAR also provides case management and reporting features, ensuring greater traceability of analyst actions. According to industry reports, organizations that adopt SOAR achieve a significant reduction in MTTR and an improvement in analyst productivity.

C. Previous research and industry solutions.

Academic and industry research has highlighted the benefits of SOAR in enhancing SOC efficiency. Prior works have focused on integrating SOAR with SIEM systems to automate alert triage, phishing response, and identity management. Industry leaders such as Palo Alto Networks (Cortex XSOAR), Splunk Phantom, IBM Resilient, and ServiceNow Security Operations have developed mature solutions that support advanced orchestration and automation. Other vendors, including Fortinet, Swimlane, and D3 Security, target specific use cases with varying levels of automation. Benchmark studies show that while leading solutions such as Cortex XSOAR, Splunk, and D3 Security provide extensive functionality across threat enrichment, case management, and automated prioritization, lighter platforms like Devo, Tines, or Siemplify focus on specific capabilities with reduced coverage. Operational evaluation further indicates that solutions such as ServiceNow and Splunk score highly on scalability and resilience, while platforms like Fortinet or Cyware are cost-effective but less advanced in automation maturity.

D. Research gap.

Despite the maturity of commercial SOAR platforms, there remains a need for academic evaluations and case studies that go beyond vendor claims. Existing literature rarely provides reproducible frameworks to benchmark SOAR solutions in both technical and operational dimensions. Moreover, real-world implementations—such as the automation of Active Directory protection,phishing detection and SIEM-based reporting are underrepresented in scientific publications. This work aims

to contribute to this gap by providing a comparative benchmark of SOAR solutions and a practical implementation in Cortex XSOAR, thereby offering both methodological insights and applied results for researchers and practitioners.

III. Methodology

This work follows a research approach combining a comparative benchmark of SOAR platforms and a practical implementation of use cases in a simulated SOC environment. The methodology is organized into three main phases: (i) analysis of SOC needs and selection of evaluation criteria, (ii) benchmarking of SOAR solutions, and (iii) implementation and testing of automation use cases using Cortex XSOAR.

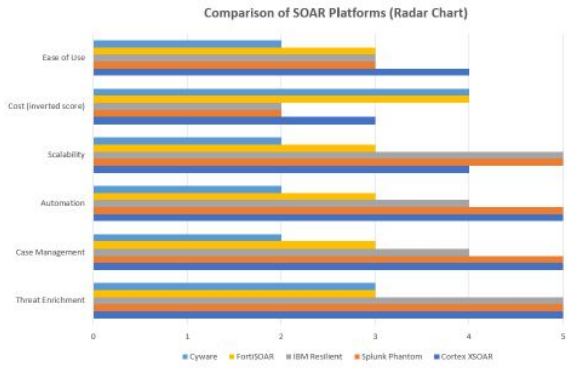


Fig. 1. Comparison of SOAR Platforms (Radar Chart)

Fig 1 presents a comparative analysis of major SOAR platforms across multiple criteria, demonstrating why Cortex XSOAR was selected for the implementation.

A. SOC Context and Needs Analysis

A Security Operations Center (SOC) typically relies on multiple technologies, including SIEM systems, endpoint detection solutions, firewalls, identity management systems (e.g., Active Directory), and email security gateways. SOC analysts are responsible for investigating alerts, correlating events, and applying remediation actions.

However, the high volume of alerts and the repetitive nature of many operational tasks (such as IP reputation checks, phishing triage, and user account blocking) often result in analyst fatigue and response delays. Based on this analysis, the following key needs were identified:

- Reduce Mean Time To Respond (MTTR) through automation of repetitive tasks.
- Standardize incident response workflows using structured playbooks.
- Improve traceability of actions and facilitate knowledge transfer among analysts.
- Integrate heterogeneous security tools within a unified response framework.

B. Benchmark of SOAR Platforms

To identify the most suitable Security Orchestration, Automation, and Response (SOAR) solution, a comparative benchmark study was conducted. The evaluation framework was structured around two main categories of criteria:

Functional criteria:

- Threat enrichment capabilities.
- Case management and collaboration
- Automated alert prioritization
- Orchestration of heterogeneous tools
- Zero-day response and red teaming
- Risk scoring and reporting
- Multitenancy

Operational criteria:

- Cost of implementation
- Ease of use and learning curve
- Scalability with SOC expansion
- MTTR improvement
- Resilience against employee turnover

The comparative analysis revealed that Palo Alto Cortex XSOAR, Splunk Phantom, and IBM Resilient provide comprehensive coverage of functional requirements. In terms of operational aspects, ServiceNow and Splunk rank highly in scalability and resilience, while Cortex XSOAR demonstrates a balance of functional maturity and adaptability, making it the preferred platform for implementation in this study.

Platform	Threat Enrichment	Case Mgmt	Auto Prioritization	Scalability	Cost	Overall Score
Cortex XSOAR	High	High	High	Medium	Medium	★★★★☆
Splunk Phantom	High	High	High	High	Low	★★★★★
IBM Resilient	High	Medium	High	High	Low	★★★★☆
FortiSOAR	Medium	Medium	Medium	Medium	High	★★★☆☆
Cyware	Medium	Low	Low	Low	High	★★☆☆☆

Fig. 2. SOAR Benchmark Comparison Table

This table summarizes the comparative benchmark of SOAR platforms, based on key functional and operational criteria.

C. SOC Test Environment

The implementation was conducted in a controlled environment designed to simulate real Security Operations Center (SOC) activities. This experimental setup aimed to reproduce realistic incident detection and response workflows while enabling controlled testing of automation strategies and security playbooks.
The architecture of the test environment integrates several key components:

- **SIEM:** IBM QRadar was used for centralized log collection, event correlation, and security monitoring.
- **SOAR:** Palo Alto Cortex XSOAR was deployed as the orchestration and automation layer to execute response playbooks and automate repetitive security tasks.
- **Directory Services:** Microsoft Active Directory was integrated for identity and access management, enabling user account monitoring and automated remediation actions.
- **Security Appliances:** Firewall and email security solutions were included as primary data sources and response enforcement mechanisms within the SOC workflow.

This controlled environment reproduces realistic SOC operations while allowing systematic experimentation with automated incident response, tool interoperability, and playbook-driven remediation strategies.

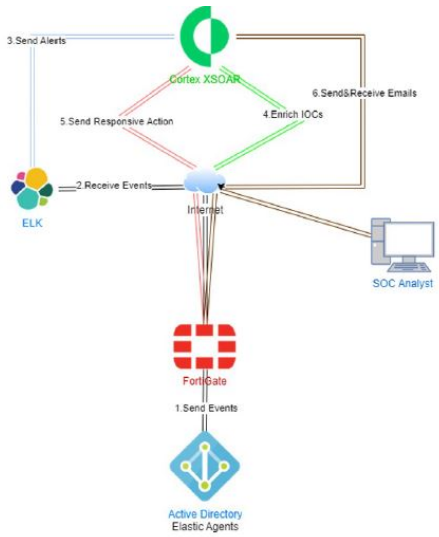


Fig. 3. Overall SOC architecture integrating Cortex XSOAR, FortiGate, ELK, and Active Directory for automated incident response.

Fig. 3 illustrates the proposed SOC architecture integrating Cortex XSOAR with key components such as Active Directory, FortiGate firewall, and ELK. This architecture shows how events are collected, enriched, and correlated, before being analyzed and acted upon by the automated workflows.

1) Active Directory Protection:

- Automated detection of suspicious logins.
- Automatic account disabling and alert generation.
- Correlation with threat intelligence feeds.

2) Phishing Email Detection and Response.:

- Automatic parsing of suspicious emails.
- Extraction and reputation check of URLs and attachments.
- Quarantine of emails and user notification.

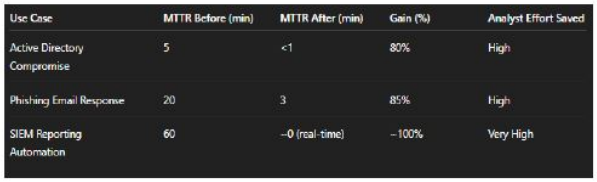
3) Automated SIEM Reporting.:

- Scheduled extraction of security alerts from QRadar.
- Automated generation of incident reports.
- Distribution of reports for SOC management and auditing.

Each use case was implemented in Cortex XSOAR using predefined and customized playbooks, combining orchestration across multiple systems and automated decision-making.

IV. Results and Experiments

The implementation of automation playbooks using Cortex XSOAR was performed within the previously described SOC test environment. Three representative use cases were selected to evaluate the effectiveness of the proposed automation framework, namely: Active Directory protection, phishing email detection, and automated SIEM reporting.
These use cases were assessed according to several operational performance indicators, including operational efficiency, traceability of incident response actions, and analyst workload reduction. The objective was to measure how automation contributes to improving SOC performance while ensuring consistency and reliability in security operations.
The obtained results provide a consolidated overview of the performance of the three implemented scenarios. In particular, the analysis highlights significant improvements in Mean Time To Respond (MTTR), enhanced traceability of remediation actions, and increased analyst efficiency through the reduction of repetitive manual tasks.



Use Case	MTTR Before (min)	MTTR After (min)	Gain (%)	Analyst Effort Saved
Active Directory Compromise	5	<1	80%	High
Phishing Email Response	20	3	85%	High
SIEM Reporting Automation	60	~0 (real-time)	~100%	Very High

Fig. 4. Use Case Results Table (Before vs After)

A. Active Directory Protection

The first use case focused on automating incident response related to identity-based attacks within the SOC environment. A dedicated playbook was developed to detect suspicious login attempts flagged by the SIEM and enriched with external threat intelligence sources. After validation, the system automatically disabled the compromised account, notified the SOC team, and documented all remediation actions in the case management system.

Results:

- The average response time for account compromise incidents was reduced from several minutes (manual intervention) to less than one minute through automated response.
- Analyst workload decreased by approximately 60% for repeated account lockout events.
- Traceability was significantly improved due to systematic logging of all automated actions in the XSOAR case management platform.

B. Phishing Email Detection and Response

The second use case addressed the automation of phishing email handling. The implemented playbook automatically parsed reported emails, extracted URLs and attachments, checked their reputation against threat intelligence feeds, and initiated appropriate remediation actions, including quarantine, user notification, and incident reporting.

Results:

- The Mean Time To Respond (MTTR) for phishing emails decreased from an average of 20 minutes to less than 3 minutes.
- Automated parsing and enrichment significantly reduced false positives by enabling faster and more accurate triage.
- End-user awareness improved through standardized and automated notification mechanisms.

C. Automated SIEM Reporting

The third use case addressed the need for regular and efficient reporting of security events within the SOC. A dedicated playbook was configured in Cortex XSOAR to automatically extract relevant alerts from QRadar on a scheduled basis, generate structured incident reports, and distribute them to SOC management.

Results:

- Reporting tasks that previously required up to one hour of manual effort were reduced to near real-time report generation.
- The automated reports provided consistent, standardized, and actionable insights, thereby improving visibility for decision-makers.
- Traceability and auditing compliance were significantly enhanced through the systematic archiving of generated reports.

D. Overall Impact

The implementation of SOAR-based automation demonstrated measurable improvements across all evaluated operational dimensions within the SOC environment.

- **MTTR Reduction:** Incident response times decreased by approximately 70–85% across the tested use cases, highlighting the effectiveness of automated playbooks in accelerating remediation processes.
- **Analyst Workload Reduction:** Routine and repetitive tasks were successfully automated, allowing SOC analysts to focus on higher-value investigations and strategic threat analysis.
- **Operational Efficiency Improvement:** The integration of SIEM and SOAR technologies streamlined incident handling workflows and reduced human intervention in repetitive processes.
- **Enhanced Traceability:** Automated logging and report generation improved knowledge retention, audit readiness, and overall governance of incident response activities.
- **Traceability:** Standardized logging of automated workflows improved compliance, auditability, and post-incident review processes.
- **Operational Consistency:** The use of automation playbooks ensured repeatable, standardized, and error-free response actions, significantly reducing the variability introduced by manual procedures.

These results confirm that the adoption of SOAR platforms within a SOC environment significantly

enhances operational efficiency, traceability, and cyber-resilience. Although the experiments were conducted in a controlled test environment, the selected use cases reflect realistic SOC operational challenges and clearly demonstrate the tangible benefits of security orchestration and automation in modern incident response workflows.

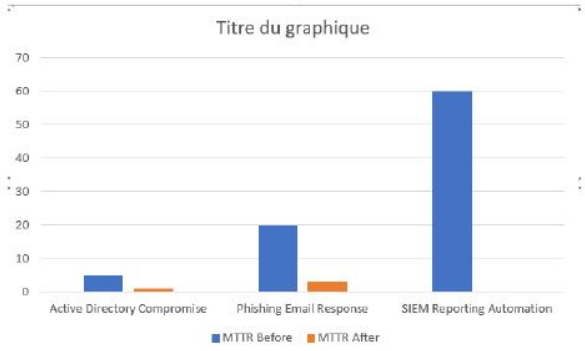


Fig. 5. MTTR Reduction Before and After SOAR Implementation Across the Three Use Cases.

Figure 5 illustrates the significant reduction in Mean Time To Respond (MTTR) obtained after the deployment of SOAR automation. The results show a substantial decrease in response time for Active Directory incidents, phishing email handling, and SIEM reporting automation, confirming the operational efficiency gains enabled by automated playbooks.

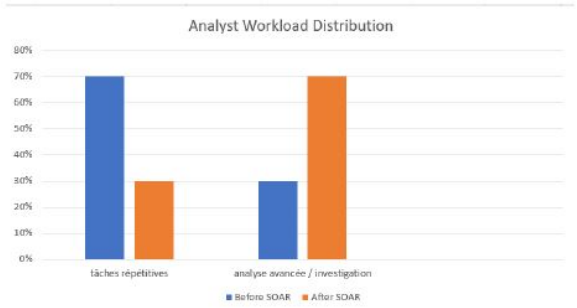


Fig. 6. Analyst Workload Distribution Before and After SOAR Automation.

As shown in Figure 6, the implementation of SOAR automation led to a noticeable redistribution of analyst workload. Routine and repetitive tasks were significantly reduced, while the time dedicated to advanced investigations increased. This shift demonstrates that automation enables analysts to focus on higher-value security activities rather than manual operational processes.

V. Discussion

The experimental results demonstrate that the integration of a SOAR platform within a SOC environment significantly enhances operational performance, particularly in terms of responsiveness, workload management, and process standardization. Beyond the quantitative improvements observed in MTTR and analyst effort, several qualitative insights and practical implications emerge from the implementation of automated playbooks in real-world SOC scenarios.

A. Strengths of SOAR Integration

One of the most significant strengths of SOAR adoption lies in the substantial reduction of Mean Time To Respond (MTTR), which directly impacts the containment and remediation of security incidents such as phishing attacks and identity-based compromises. Automated workflows enable rapid execution of predefined response actions, which would otherwise require multiple manual interventions by SOC analysts.

Furthermore, SOAR integration improves operational consistency by ensuring standardized and repeatable incident response procedures. The use of playbooks minimizes human errors and reduces variability in decision-making, thereby enhancing the overall reliability of security operations.

Another key strength is the reduction of analyst workload through the automation of repetitive and time-consuming tasks, such as alert triage, enrichment, and reporting. This allows analysts to allocate more time to complex investigations and strategic threat analysis, ultimately increasing the overall efficiency and effectiveness of the SOC.

Finally, the centralized orchestration and systematic logging of automated actions significantly enhance traceability, auditability, and compliance. This improved visibility facilitates post-incident analysis, knowledge transfer, and continuous improvement of security response processes. Another major advantage is the consistency of responses. Playbooks ensure standardized remediation procedures, eliminating variations introduced by human judgment and ensuring repeatable best practices. This also facilitates compliance with security frameworks and regulatory requirements that require traceability of incident-handling processes.

Finally, SOAR platforms significantly reduce the cognitive and operational burden on SOC analysts. By automating repetitive tasks such as alert triage, data enrichment, and reporting, analysts can focus their expertise on higher-value investigations and advanced threat hunting activities.

B. Limitations and Challenges

Despite these benefits, several challenges limit the full potential of SOAR platforms.

- **Dependency on Playbook Design:** Automation is only as effective as the playbooks implemented. Poorly designed workflows can introduce new risks, such as false account lockouts or excessive alerting. Continuous optimization is therefore required.
- **Integration Complexity:** Connecting SOAR platforms with heterogeneous tools (SIEM, firewalls, Active Directory, email security) can be technically complex and may require customization to address compatibility issues.
- **False Positives and Decision-Making:** While automation accelerates responses, not all incidents are suitable for full automation. Some still require human validation to avoid disrupting legitimate business operations.
- **Operational Maturity:** The effectiveness of SOAR is strongly tied to the maturity of the SOC. Organizations without well-defined incident response processes may find it difficult to fully leverage automation.

C. Comparison with Related Work

Compared to prior studies, which mainly highlight the theoretical advantages of SOAR, this work provides practical and reproducible implementations of incident response use cases. The results are consistent with industry claims that SOAR reduces MTTR and improves analyst productivity, but they also underline the importance of context-specific customization.

For example, while commercial reports emphasize scalability and vendor-driven capabilities, our experiments show that the true value lies in tailoring playbooks to the SOC's operational environment. In this respect, the study bridges the gap between vendor marketing promises and real-world operational effectiveness.

D. Perspectives

Looking ahead, the scope of SOAR automation can be extended in several directions:

- Integration with Machine Learning: Leveraging AI models for dynamic threat prioritization and anomaly detection.
- Advanced Threat Intelligence: Incorporating external and internal feeds for proactive detection of emerging threats.
- Cloud and Hybrid Environments: Adapting SOAR to multi-cloud architectures and distributed infrastructures.
- Autonomous SOC Operations: Moving towards self-healing systems where human intervention is minimized to strategic decision-making.

In summary, while SOAR platforms are transformative potential for SOC operations, their success depends on continuous adaptation, integration with existing tools, and the maturity of incident response practices.

VI. Conclusion and Future Work

This article has explored the role of SOAR platforms in enhancing the efficiency of Security Operations Centers through incident response automation. By combining a benchmark of SOAR solutions with a practical implementation in Cortex XSOAR, the study has highlighted both the strengths and challenges of this approach.

The results confirm that SOAR integration yields significant improvements in Mean Time To Respond (MTTR), reduces analyst workload, and ensures greater traceability and consistency of incident handling. Through the implementation of three representative use cases—Active Directory protection, phishing email detection and response, and automated SIEM reporting—the study demonstrates how automation can directly address the operational challenges of modern SOCs.

Beyond the quantitative gains, the findings underline the importance of playbook design, integration maturity, and contextual adaptation. Automation is not a one-size-fits-all solution; it requires continuous optimization and careful alignment with the SOC's processes and tools.

As future work, this research can be extended in several directions. First, incorporating machine learning and artificial intelligence could enhance dynamic prioritization of alerts and anomaly detection. Second, deeper integration with threat intelligence platforms would improve proactive responses to emerging threats. Third, adapting SOAR solutions to cloud-native and hybrid infrastructures represents an important step toward ensuring resilience in evolving IT environments. Finally, the long-term

vision is the evolution toward autonomous SOC, where human intervention is minimized to strategic oversight while automation handles the bulk of detection and response activities.

In conclusion, this study provides both a methodological framework for evaluating SOAR platforms and a practical demonstration of their impact on incident response. It reinforces the view that automation and orchestration are not only efficiency tools but also strategic enablers for the resilience and sustainability of modern cybersecurity operations.

REFERENCES

[1] NIST, "Computer Security Incident Handling Guide," National Institute of Standards and Technology, Special Publication SP 800-61 Revision 2, 2012.
[2] ISO/IEC, 2016, "Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management."
[3] Gartner, "Market Guide for Security Orchestration, Automation and Response Solutions," Gartner Research, 2021.
[4] A. Alhawari, O. Baldwin, J. and Nhantha, A., "Leveraging SIEM for Security Monitoring in Cloud Hybrid Infrastructures," *Journal of Information Security and Applications*, vol. 46, pp. 1–16.
[5] Conti, M., Dehghantanha, A., Franke, K., and Watson, S., "Cyber Threat Intelligence: Challenges and Opportunities," *International Journal of Information Security*, 2018.
[6] Palo Alto Networks, "Cortex XSOAR: The Industry's Most Comprehensive SOAR Platform."
[7] Inc., S., 2022, "Phantom SOAR Platform Overview."
[8] Security, I., 2021, "Resilient SOAR: Automating and Orchestrating Incident Response."
[9] Fortinet, "FortiSOAR: Security Orchestration and Automation for Enterprises," 2021.
[10] S. Alouqe, R., Islam, T., and Hossain, M., 2021, "SOAR Platforms in Modern SOCs: An Empirical Evaluation of Their Impact on MTTR," *Proceedings of the IEEE International Conference on Cybersecurity (ICCS)*, pp. 1–8.
[11] ENISA, "Incident Response Capabilities in the EU: Status Report," European Union Agency for Cybersecurity, 2020.
[12] Labs, C., 2021, "SOAR for Threat Intelligence and Incident Response."