IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, July 2026
Impact Factor: 8.2

SOAR Automation Platform for Cybersecurity Incident Response

Bhumika A R[*1], Jhanavi H N [*2], Prof. Thejaswini M N[*3]
[*1,2]Students, Department of Computer Application
[*2]Assistant Professor, Department of Computer Application
Maharaja Institute of Technology, Mysore, Karnataka, India

Abstract: *Increasing numbers of cyberattacks led to increasing workload for Security Operations Centers (SOCs). SOC analysts are inundated with hundreds and thousands of alerts from SIEM, IDS/IPS, EDR, firewalls, and cloud/endpoint security systems. Manual investigation leads to alert fatigue, slow responses, and inconsistencies. This paper will focus on an AI-driven Security Orchestration, Automation and Response (SOAR) platform that involves: secure authentication, central monitoring, machine learning-based anomaly detection, Groq AI-driven incident analysis, threat intelligence enhancement, n8n workflow automation, AI chatbot, and automatic reporting. The unified platform increases efficiency, drastically reduce human effort to repetitive work, quick incident response times, enhances the quality of investigations, and provides a comprehensive view of an organizations security posture. The platform is also modular to further integrate with cloud security, SIEM, EDR, malware analysis and predictive analyses*

Keywords: *cyberattacks*

I. INTRODUCTION

Cybersecurity has become a fundamental requirement for organizations as digital technologies such as cloud computing, IoT, and web applications continue to expand. While these technologies improve connectivity and business efficiency, they also increase the risk of cyberattacks, including ransomware, phishing, malware, and distributed denial-of-service (DDoS) attacks. Protecting sensitive information and ensuring business continuity have therefore become major priorities for organizations worldwide. Security Operations Centers (SOCs) are responsible for monitoring security events, detecting threats, and responding to incidents using tools such as Security Information and Event Management (SIEM), Intrusion Detection Systems (IDS), firewalls, and Endpoint Detection and Response (EDR). However, the large volume of security alerts generated daily makes manual investigation time-consuming and often results in alert fatigue, delayed responses, and inconsistent decision-making. Recent research emphasizes the use of Artificial Intelligence (AI), Machine Learning (ML), and Security Orchestration, Automation, and Response (SOAR) to improve cybersecurity operations. These technologies enable automated threat detection, intelligent incident analysis, and faster response through workflow automation. This research proposes an AI-Driven SOAR Automation Platform for Cybersecurity Incident Response that integrates AI, ML, threat intelligence, and workflow automation into a unified web-based platform. The system provides centralized monitoring, AI-assisted incident analysis, anomaly detection, and automated response using Groq AI and n8n workflows. By reducing manual effort and improving response speed, the proposed platform enhances the efficiency, accuracy, and effectiveness of modern Security Operations Centers while providing a scalable solution for evolving cybersecurity challenges.

METHODOLOGY

The proposed methodology begins with secure user authentication using Firebase Authentication, ensuring that only authorized users can access the platform. After successful authentication, security events are collected from multiple sources, including Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) systems,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, July 2026
Impact Factor: 8.2

firewalls, and endpoint security solutions. Machine Learning models continuously analyze the incoming events to detect anomalies and identify suspicious activities. Potential security incidents are then forwarded to Groq AI, which performs incident summarization, severity classification, attack identification, and provides response recommendations. The platform further enriches incidents by integrating threat intelligence data, including malicious IP addresses, domains, CVEs, and Indicators of Compromise (IoCs). n8n automates incident response through predefined workflows such as notifications, ticket creation, escalation, and reporting. Finally, a centralized dashboard provides real-time monitoring, while an AI-powered chatbot assists security analysts during investigations and decision-making.

MODELING AND ANALYSIS

The proposed architecture follows a **multi-layered design** consisting of the **Presentation, Application, Intelligence, Automation, Data Storage, and External Integration** layers. The **Presentation Layer**, developed using **React.js**, provides an interactive dashboard for monitoring incidents, viewing alerts, generating reports, and accessing the AI chatbot. The **Application Layer** uses **Python-based REST APIs** to process requests and coordinate communication between modules. The **Intelligence Layer** integrates **Machine Learning** for anomaly detection and **Groq AI** for incident analysis, threat classification, and response recommendations. The **Automation Layer** employs **n8n** workflows to automate notifications, ticket creation, incident escalation, and response actions. **Firebase Authentication** and the database ensure secure user management and data storage, while **REST APIs** connect external threat intelligence services. This modular architecture provides scalability, maintainability, interoperability, and efficient cybersecurity operations.

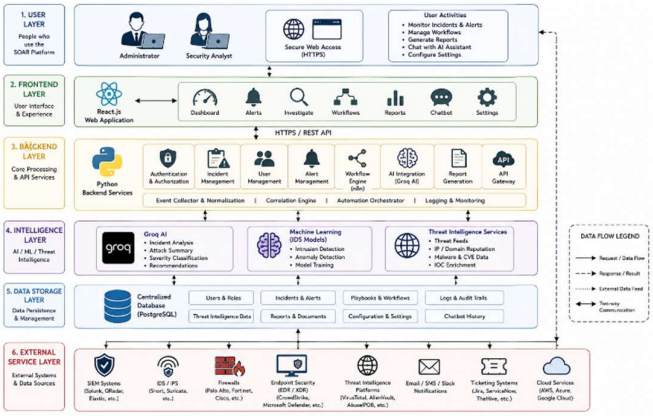


Figure 1: System Architecture

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, July 2026
Impact Factor: 8.2

DATAFLOW DIGRAM

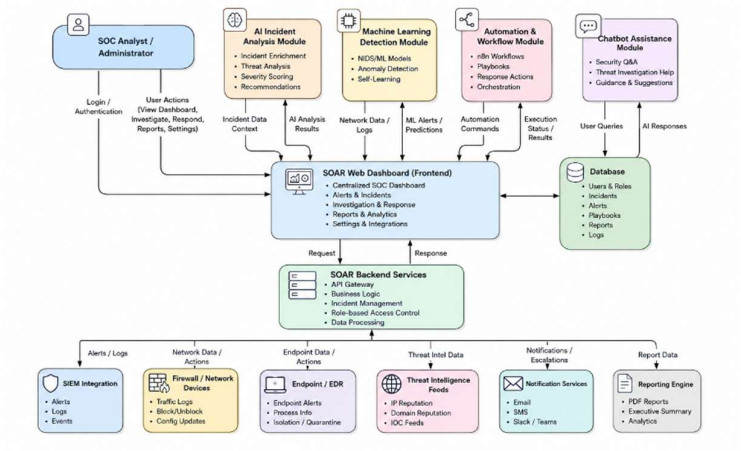
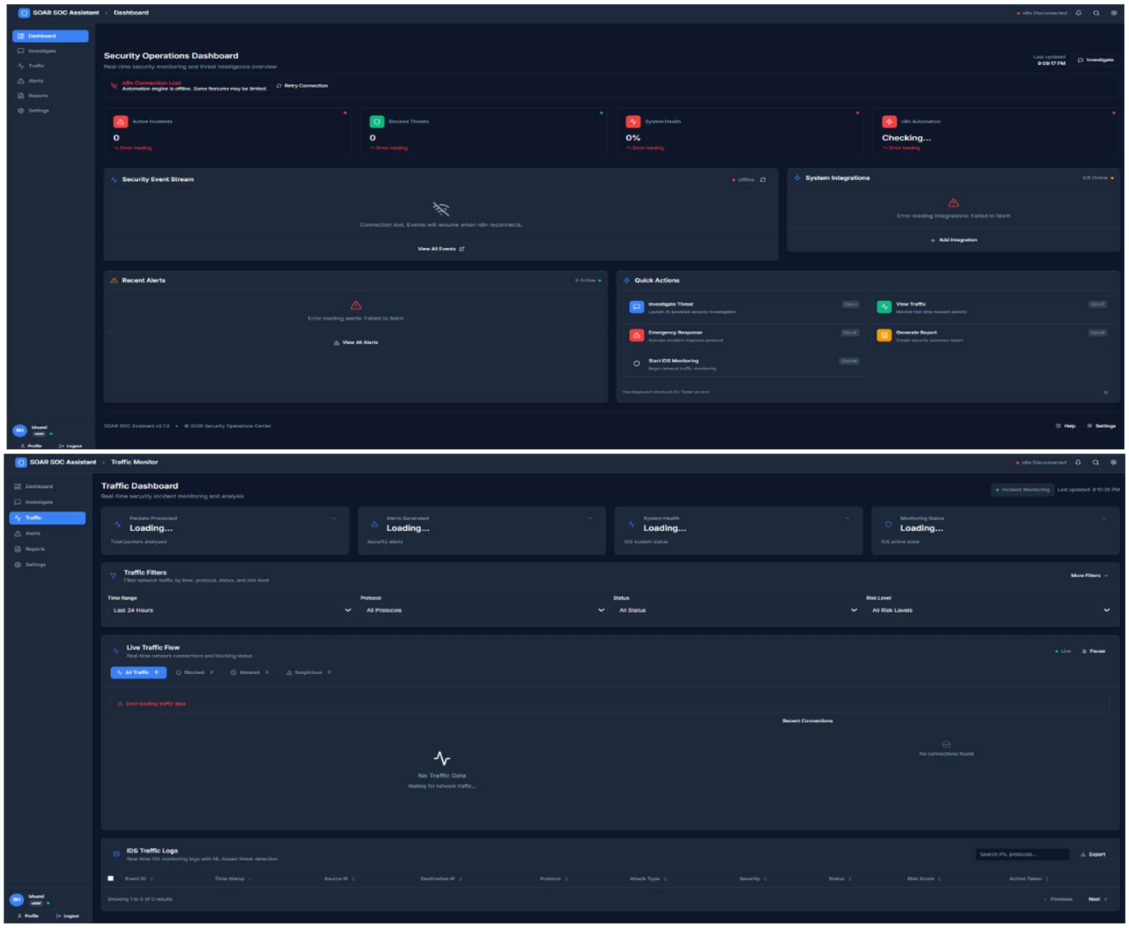
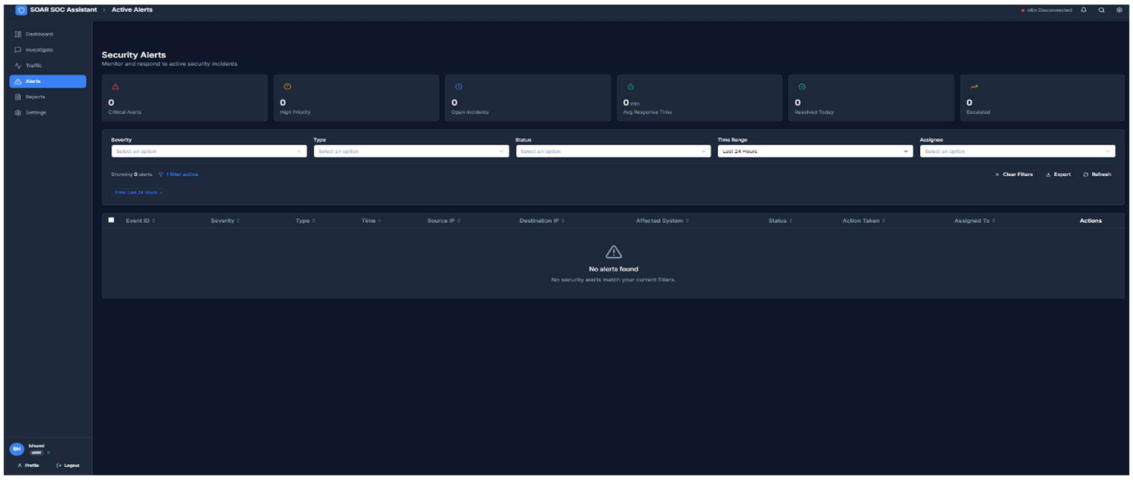


Figure 1: Dataflow Diagram

SNAPSHOTS



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, July 2026
Impact Factor: 8.2



II. RESULTS AND DISCUSSION

System evaluation demonstrates significant improvements in operational efficiency by integrating centralized incident management with automated investigation workflows. The platform streamlines Security Operations Center (SOC) activities by reducing manual intervention and enabling faster decision-making. AI-assisted analysis minimizes analyst workload by automatically summarizing security incidents, identifying potential threats, and recommending appropriate response actions. Machine learning enhances anomaly detection accuracy, while workflow automation executes predefined playbooks to accelerate incident response. Threat intelligence enrichment provides valuable contextual information during investigations, and the integrated dashboard offers real-time visualization of incidents, response status, security metrics, and overall cybersecurity analytics for effective monitoring and management.

III. CONCLUSION

The proposed AI-driven SOAR Automation Platform provides a comprehensive and intelligent solution for cybersecurity incident response by integrating artificial intelligence, machine learning, workflow orchestration, and threat intelligence into a unified platform. It centralizes security monitoring, automates repetitive incident response tasks, and enables faster threat detection and investigation. AI-powered analysis assists security analysts by summarizing incidents, prioritizing alerts, and recommending appropriate response actions, while machine learning improves anomaly detection accuracy. The platform enhances Security Operations Center (SOC) productivity by reducing manual effort, improving response time, and providing real-time security visibility through an interactive dashboard. Overall, the system strengthens an organization's cybersecurity posture and operational efficiency. Future enhancements include cloud-native deployment, predictive threat analytics, malware sandbox integration, advanced SIEM and EDR connectivity, and adaptive AI models for continuous threat detection and automated response.

IV. ACKNOWLEDGEMENTS

I express my gratitude to the project guide for their invaluable guidance, and unwavering support throughout the project duration. I'm equally thankful to the faculties of MIT Mandya further insightful suggestion and motivation which makes well experience in my work. I extend my sincere appreciation to the management of the institute for providing the necessary resources, that helps in achieving successful project. I'm deeply grateful to my classmates and friends for their coordination, assistance and encouragement during the process of development and I finally, acknowledged with gratitude the contribution of all those directly or indirectly

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, July 2026
Impact Factor: 8.2

REFERENCES

[1] N. Hubballi and R. Suryadevara, *"Security Orchestration, Automation and Response (SOAR): A Systematic Literature Review," 2023.*

[2] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, *"Survey of Machine Learning Techniques in Network Intrusion Detection,"* IEEE Access, vol. 9, pp. 1–25, 2021.

[3] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Pearson Education, 2021.

[4] National Institute of Standards and Technology (NIST), *Computer Security Incident Handling Guide (SP 800-61 Revision 2)*, Gaithersburg, MD, USA, 2012.

[5] MITRE Corporation, *MITRE ATT&CK® Framework for Enterprise*, MITRE ATT&CK Knowledge Base, 2024.

[6] M. Bishop, *Computer Security: Art and Science,* 2nd ed. Addison-Wesley Professional, 2018.

[7] W. Stallings and L. Brown, *Computer Security: Principles and Practice,* 5th ed. Pearson Education, 2023.

[8] E. Cole, *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization,* Syngress, 2013.