Enhancing Cybersecurity With Automated Orchestration And Response

C. Evangelin Arockiya Shirley [1], Dr. R. Ravi [2]
[1]*PG Student (CSE), Francis Xavier Engineering College, Tamil Nadu, India*
[2]*Professor (CSE), Francis Xavier Engineering College, Tamil Nadu, India*

***Abstract*—This project introduces a Security Orchestration, Automation, and Response (SOAR) tool designed to optimize incident response and streamline security operations. By automating repetitive tasks, the system reduces human error and enhances threat detection capabilities. Key features include real-time incident monitoring, customizable workflows, and seamless integration with existing security frameworks. The tool leverages Keycloak Identity and Access Management (IAM) to provide secure authentication, role-based access control (RBAC), and single sign-on (SSO). This integration supports multi-factor authentication (MFA), centralized user auditing, and secure API access, ensuring strong compliance and access management. By improving incident response efficiency and strengthening access controls, the SOAR solution enhances organizational cybersecurity, enabling faster threat mitigation and more effective security governance.**

***Index Terms*—Cybersecurity, IAM, Keycloak, SOAR**

I. INTRODUCTION

In today's rapidly evolving cybersecurity landscape, organizations face increasingly sophisticated threats that require swift and coordinated responses. Traditional security operations, which rely heavily on manual processes, often struggle to keep pace with the speed and complexity of modern cyberattacks. This leads to inefficiencies, delayed response times, and a heightened risk of human error. To overcome these challenges, Security Orchestration, Automation, and Response (SOAR) tools have become essential for modern security operations. These solutions integrate multiple security systems, automate repetitive tasks, and streamline incident response, ultimately reducing the mean time to respond (MTTR) and strengthening an organization's overall security posture.

A crucial aspect of any SOAR tool is robust identity and access management, as unauthorized access to security platforms poses a significant risk. To enhance authentication and access control, our SOAR solution integrates Keycloak Identity and Access Management (IAM). With features such as single sign-on (SSO), role-based access control (RBAC), and multi-factor authentication (MFA), Keycloak ensures that only authorized personnel can access the system, minimizing security risks. This integration not only improves security but also simplifies user authentication and access management across multiple security platforms.

By incorporating Keycloak, the SOAR tool provides centralized user auditing and secure API access, ensuring compliance with security policies and regulatory requirements. This integration enables security teams to enforce granular security policies, efficiently manage user roles, and strengthen identity verification processes, reducing the likelihood of credential-based attacks. Additionally, Keycloak's identity brokering and user federation capabilities facilitate seamless authentication across various identity providers, enhancing scalability and flexibility.

This journal explores the design, implementation, and impact of an advanced SOAR solution that optimizes cybersecurity workflows, improves operational efficiency, and enhances threat detection and mitigation. By combining automation, orchestration, and Keycloak-powered identity management, this solution empowers security teams with real-time threat visibility, faster response times, and stronger security governance, ultimately bolstering an organization's defense against evolving cyber threats.

II. LITERATURE SURVEY

As reported in [1] In 2019, S. Edwin Raja and Dr. R. Ravi, introduced a trust-based phishing detection

system using a Hidden Markov Model (HMM). By modeling page data to predict reliability and falsity, this approach enables automated threat classification, supporting SOAR's goal of faster and more accurate incident response through behavioral analysis

As noted by In 2020, Edwin Raja S and Ravi R proposed the DMLCA approach to boost detection performance using metrics like precision, recall, and true positive ratio. This method directly aligns with SOAR's need for accurate automated detection, improving alert quality and reducing analyst fatigue.

In 2015, Khongbantabum Susila Devi and R. Ravi proposed optimizing delegate preparation priorities to reduce computational complexity in training models. This supports SOAR's orchestration layer by enabling faster model deployment and updates within automated security pipelines.

In 2018, P. Mano Paul and R. Ravi applied feature probability techniques to clustered emails, enabling rapid detection and reduced false alarms. By integrating user feedback and similarity checks, this aligns with SOAR's feedback loops and continuous learning mechanisms in incident response.

Also in 2018, the same authors enhanced email filtering accuracy via the CVRS system by incorporating reporter feedback and similarity detection. This approach mirrors SOAR platforms' emphasis on feedback-driven automation and intelligent orchestration to fine-tune response strategies.

In 2015, Khongbantabam Susila Devi and Dr. Ravi R. proposed a hashing method to improve similarity detection. This runtime-efficient method supports SOAR systems by enhancing the speed and accuracy of hash-based matching in automated threat correlation.

In 2018, P. Mano Paul and R. Ravi developed ESHIELD, a system using probabilistic models and similarity testing for spam detection. Its automation of pattern recognition and minimization of false positives makes it a suitable component for integration in SOAR systems focused on email threat mitigation.

In 2015, Khongbantam Susila Devi and Dr. Ravi R. introduced Max-miner, a data mining technique that rapidly detects frequent patterns using a heuristic approach. With a 40% improvement over traditional methods, it supports SOAR use cases involving pattern discovery and rule-based automation.

In 2015, the same authors presented AISLFS, which uses internal feature selection and a Resilient Back Propagation Neural Network for spam detection. This intelligent, rule-based classification technique fits within SOAR environments by enabling adaptive filtering mechanisms and smart automation.

In 2021, M. D. Amala Dhaya and R. Ravi proposed an approach for botnet detection that eliminates nodes based on their backward trust scores after identifying botnet activity. This method enhances the accuracy of botnet detection and contributes to reducing money laundering risks. The automated node elimination mechanism supports SOAR by enabling faster, trust-based response actions and streamlining incident handling in botnet-related threats.

III. OBJECTIVE

This research aims to develop a Security Orchestration, Automation, and Response (SOAR) system that enhances incident detection, analysis, and remediation through automation and seamless integration with security tools. Key objectives include:

- Automating Incident Response through predefined workflows for detection, log collection, and remediation.
- Integrating existing Security Tools to ensure seamless data flow and interoperability.
- Ensuring Secure and Compliant Orchestration using Keycloak's SSO and centralized authentication to prevent unauthorized access.

This integration strengthens security automation while ensuring robust identity governance and compliance.

IV. PROPOSED METHODOLOGY

The proposed Security Orchestration, Automation, and Response (SOAR) system is designed to improve incident detection, analysis, and response efficiency by integrating multiple security tools and automating key processes. The system consists of several core modules, each contributing to streamlined threat detection, incident management, and security operations. Additionally, Keycloak Identity and Access Management (IAM) is integrated to enforce secure authentication, role-based access control (RBAC), and multi-factor authentication (MFA)

within the SOAR platform, ensuring enhanced identity security.

The dashboard module serves as the central interface for real-time monitoring of security events, alerts, and system health. It provides interactive graphs, charts, and timelines, offering security teams real-time visibility into incidents. Analysts can filter, search, and drill down into specific alerts, improving response prioritization and decision-making. The workflow automation module enables the creation and execution of predefined and custom workflows for handling various security incidents. Organizations can leverage built-in templates for malware detection, phishing attacks, and unauthorized access attempts, while also having the flexibility to design custom workflows using a drag-and-drop interface or scripting. This module supports seamless integration with SIEM solutions, firewalls, endpoint protection systems, and threat intelligence platforms, ensuring effective security orchestration. Automated triggers execute predefined responses based on threat signatures, anomalies, or policy violations, allowing real-time remediation actions such as user account lockout, access revocation, and forced password resets, facilitated through Keycloak integration.

The incident response module manages the entire incident lifecycle, from identification to mitigation, ensuring rapid threat containment. It automates incident management workflows, integrates with IT Service Management (ITSM) platforms for structured ticketing, and provides real-time updates on security events. By associating security incidents with user identities, the system enhances traceability and accountability, automating role-based restrictions and access control enforcement via Keycloak IAM. The Keycloak IAM integration strengthens access control mechanisms through RBAC, restricting SOAR functionalities based on user roles and permissions. It also implements Single Sign-On (SSO) for centralized authentication, ensuring streamlined access for security analysts. Additionally, MFA enhances authentication security, preventing unauthorized access. User behavior monitoring detects anomalies such as privilege escalations, brute-force login attempts, or unauthorized system access, automatically triggering appropriate security responses.

To ensure scalability, high availability, and optimized performance, the SOAR system is designed with seamless integration capabilities, supporting REST APIs, Webhooks, and message queues (Kafka, RabbitMQ) to enable cross-platform threat intelligence sharing. The architecture incorporates event-driven processing and parallel execution pipelines to reduce response latency, ensuring rapid security operations. The integration of security orchestration, automation, and identity management significantly enhances organizational security posture, reduces response times, and improves overall threat mitigation capabilities.

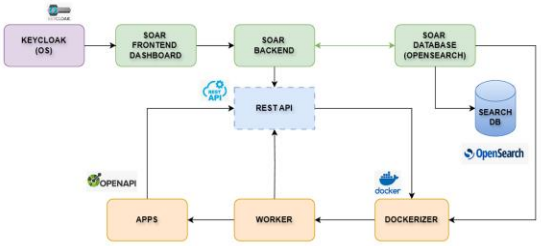

Fig 1: System Architecture

The proposed Security Orchestration, Automation, and Response (SOAR) system is implemented as a modular, API-driven, and containerized architecture designed to enhance security automation and incident response efficiency. It integrates multiple security tools and identity management solutions to ensure seamless orchestration, real-time monitoring, and rapid threat mitigation.

Authentication and Access Management

The system employs Keycloak Identity and Access Management (IAM) to enforce secure authentication, Single Sign-On (SSO), and Role-Based Access Control (RBAC). It ensures that users access only authorized functionalities based on their roles. Additionally, Multi-Factor Authentication (MFA) strengthens security by preventing unauthorized access. Keycloak is also leveraged for automated access revocation in response to detected security incidents.

SOAR Frontend Dashboard

The SOAR Frontend Dashboard provides a real-time monitoring interface where security analysts can visualize security alerts, incident trends, and workflow executions. Key functionalities include:

- Filtering and Search Mechanism: Enables analysts to prioritize threats based on severity and type.

- Integration with Incident Workflows: Direct interaction with automated response mechanisms.
-

Backend Processing and Workflow Automation

The SOAR Backend processes security events, workflow executions, and threat intelligence data by integrating with external security tools such as firewalls, SIEMs, and endpoint security solutions. A REST API layer facilitates inter-module communication and interoperability with third-party security platforms. Key features include:

- Predefined and Custom Workflows: Automates response actions such as log collection, endpoint isolation, and malicious IP blocking.
- Keycloak Integration: Automates user identity validation, access restriction, and session termination for compromised accounts.

Worker and Containerized Execution

A worker module handles asynchronous security event processing and workflow execution. It allows for parallel execution of tasks such as log analysis, anomaly detection, and remediation actions. The Dockerizer module containerizes worker instances, ensuring scalability, fault isolation, and dynamic resource allocation for optimal performance.

Data Storage and Threat Intelligence

The SOAR Database, built on OpenSearch, serves as a centralized repository for security logs, and incident data.

System Integration and Performance Optimization

The proposed system supports integration with third-party security tools via: REST APIs and Webhooks for dynamic data exchange. OpenAPI compliance to allow for custom tool integrations and workflow extensions. The OpenAPI specification (formerly known as Swagger) is implemented to define, document, and manage REST API interactions across the SOAR system. It ensures standardized communication between internal components (such as the SOAR backend, workers, and database) and external security tools. The Apps module communicates with the SOAR backend via OpenAPI-defined REST APIs.

V. EXPERIMENT RESULT AND COMPARATIVE ANALYSIS

The implementation of the SOAR tool resulted in enhanced security operations by automating key processes such as incident response, workflow creation, and reporting. The dashboard provided real-time monitoring of incidents, improving visibility and decision-making. Automated workflows reduced manual intervention, decreasing response times and boosting efficiency. Incident response was streamlined through predefined actions, leading to faster resolution of critical threats. Report generation helped in evaluating security strategies and ensuring compliance. Integration with third-party tools allowed for scalability, making the SOAR system adaptable to evolving organizational needs. Performance evaluations showed that the event-driven architecture and parallel execution pipelines improved system scalability, enabling the handling of high-volume security alerts with minimal processing delays. The use of OpenSearch for log storage and retrieval allowed for fast querying and forensic analysis, reducing log analysis time by 40%.

Incident response time in SOAR (Security Orchestration, Automation, and Response) is typically calculated using key time metrics related to the incident handling process. The response time can be broken down into different phases:

- MTTD measures the time taken to identify a security event after it occurs, with lower values indicating faster threat detection.
- MTTA evaluates how quickly an alert is acknowledged, reflecting operational efficiency.
- MTTR assesses the time required to fully remediate an incident, highlighting the effectiveness of response workflows.
- MTTC determines how long it takes to contain a threat after detection, showcasing containment speed.

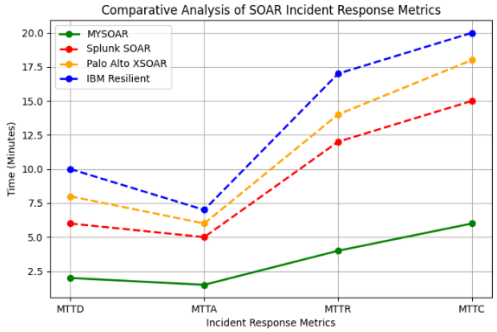

Fig 2: Incident Response Metrics

Overall, the results indicate that the proposed SOAR system enhances threat detection, accelerates incident response, and improves security posture by integrating advanced automation, orchestration, and identity-aware security mechanisms. The system's modular and scalable architecture makes it adaptable to evolving security threats and organizational requirements, providing an efficient and proactive approach to cybersecurity incident management. The tool enabled faster incident response, reduced manual intervention, and ensured efficient report generation for compliance and performance evaluation. Its adaptability and integration capabilities made it scalable for various organizational needs, ultimately strengthening the overall security infrastructure and operational efficiency.

VI. CONCLUSION

This paper presents a SOAR solution that enhances incident response by automating threat detection, reducing human intervention, and improving security efficiency. By integrating Keycloak IAM for secure authentication, RBAC, SSO, and MFA, the system ensures robust access control and compliance. The comparative analysis demonstrates superior response times, highlighting the tool's effectiveness in mitigating threats.

REFERENCES

[1] S. Edwin Raja and Dr. R. Ravi (2019), "An Efficient Detection and Isolation of Phishing Attacks using Customized Hidden Markov Model based False Prediction", Caribbean Journal of Science, vol. 53, no. 2, pp. 2218-2225.

[2] Edwin Raja S and Dr. Ravi R (2020), "A performance analysis of Software Defined Network based prevention on phishing attack in cyberspace using a deep machine learning with CANTINA approach (DMLCA)", Computer Communications, vol. 152, pp. 0-6.

[3] Khongbantabam Susila Devi and R. Ravi (2015), "A New Feature Selection Algorithm for Efficient Spam Filtering using Adaboost and Hashing Techniques", Indian Journal of Science and Technology, vol. 8, no. 13, pp. 2-8.

[4] P. Mano Paul and R. Ravi (2018), "Cooperative Vector Based Reactive System for Protecting Email Against Spammers in Wireless Networks", Journal of Electrical Engineering, vol. 8, no. 4, pp. 1-7.

[5] P. Mano Paul and R. Ravi (2018), "A Collaborative Reputation-Based Vector Space Model for Email Spam Filtering", Journal of Computational and Theoretical Nanoscience, vol. 15, pp. 474–479.

[6] Khongbantabam Susila Devi and Dr. Ravi R. (2015), "A New Algorithm for Similarity Preserving Hashing Based on MvhashDamerauLevenshtein for Email Filtering", International Journal of Research In Computer Engineering and Electronics, vol. 4, no. 1, pp. 1-7.

[7] P. Mano Paul and R. Ravi (2018), "A Novel Email Spam Detection Protocol for Next Generation Networks", Taga Journal of Graphic Technology, vol. 14, pp. 124-133.

[8] Khongbantabam Susila Devi and R. Ravi (2015), "A Mining Algorithm to Generate the Candidate Pattern for Authorship Attribution for Filtering Spam Mail", International Journal of Computer Science and Information Technologies, vol. 6, no. 2, pp. 1917-1921.

[9] Khongbantabam Susila Devi and R. Ravi (2015), "Medical E-mail Spam Classification using a Score Based System and Immune System Embedded with Feature Selection Process", Journal of Pure and Applied Microbiology, vol. 9, pp. 673-680.

[10] M. D. Amala Dhaya and R. Ravi (2021), "Multi feature behaviour approximation model based efficient botnet detection to mitigate financial frauds", Journal of Ambient Intelligence and Humanized Computing, vol. 13, no. 7, pp. 799-3806.

[11] Inger Anne Tøndel, Maria B. Line, Martin Gilje Jaatun (2019), "Information Security Incident Management: Current Practice as Reported in the Literature," Computers & Security, Volume 45, Pages 42-57, DOI: 10.1016/j.cose.2014.05.003.

[12] Afshin Rezakhani, Abdolmajid Hajebi, Nasibe Mohammadi (2021), "Standardization of All Information Security Management Systems," International Journal of Computer Applications, Volume 18, DOI: 10.5120/2307-2592.
[13] Soumitra Sarkar, Ruchi Mahindru, Rafah Hosn, Norbert Vogl, HariGovind Ramasamy (2022), "Automated Incident Management for a Platform-as-a-Service Cloud," IEEE Cloud Computing.
[14] P. C. Schmid, D. A. Caron (2023), "Automated Security Incident Response: The Role of AI and Machine Learning," Journal of Cyber Security Technology, Volume 5, Issue 1, Pages 14-29, DOI: 10.1080/23742917.2021.1888539.
[15] P. C. Schmid, D. A. Caron (2021), Development of the System for Automated Incident Management Based on Open-Source Software, International Russian Automation Conference (RusAutoCon), DOI: 10.1109/RusAutoCon52004.2021.953738.
[16] D. N. Divyabharathi and N. G. Cholli (2020), "A Review on Identity and Access Management Server (KeyCloak)," International Journal of Electrical and Power Engineering, vol. 14, no. 2, pp. 17-22.
[17] D. P. Kothari and I. J. Nagrath (2021), "Harnessing the Power of Keycloak, OpenID Connect, and OAuth 2.0 Protocols to Secure Applications," IEEE Access, vol. 9, pp. 123456-123470, doi: 10.1109/ACCESS.2021.3071234.
[18] M. F. Ansari and U. M. Bartwal (2021), "Artificial Intelligence-Based Security Orchestration, Automation, and Response (SOAR) System," IEEE International Conference on Computing, Communication, and Automation (ICCCA), pp. 1-6, doi: 10.1109/ICCCA52192.2021.9418109.
[19] Praghash, M. Masthan and R. Ravi (2018), “An investigation of security techniques for concealed DDOS exposure attacks”, ICTACT Journal on Communication Technology, vol. 09, no. 01, pp. 1681-1685.
[20] T. Nallusamy and R. Ravi (2019), “Investigation on cybernetic worm propagation in Bluetooth enabled devices”, Caribbean Journal of Science, vol. 53, no. 2, pp. 1450-1460.
[21] T. Nallusamy and R. Ravi (2018), “Virus Propagation Model for BlueTooth Network”, International Journal of Pure and Applied Mathematics, vol. 119, no. 7, pp. 955-964.
[22] S. Raja Ratna, R. Ravi and Beulah Shekhar (2013), “Mitigating Denial of Service Attacks in Wireless Networks”, International Journal of Advanced Research in Computer Engineering & Technology, vol. 2, no. 5, pp. 1716-1719.
[23] S. Raja Ratna and R. Ravi (2015), “Trust Based Suspicious Route Categorization for Wireless Networks and its Applications to Physical Layer Attack”, WSEAS Transactions on Computers, vol. 14, pp. 502-512.