International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Next-Generation Security Operations: Leveraging Automation for Proactive Threat Mitigation

Kummari Sujan Kumar
Computer Science and Engineering
(Cyber Security)
Institute of Aeronautical Engineering
Dundigal, Hyderabad
21951a6253@iare.ac.in

Chanupalli Yugander
Computer Science and Engineering
(Cyber Security)
Institute of Aeronautical Engineering
Dundigal, Hyderabad
21951a6263@iare.ac.in

R Sai Ram Chowdary
Computer Science and Engineering
(Cyber Security)
Institute of Aeronautical Engineering
Dundigal, Hyderabad
21951a6245@iare.ac.in

Dr.Mahammad Rafi D
Associate Professor
Computer Science and Engineering
(Cyber Security)
Institute of Aeronautical Engineering
Dundigal, Hyderabad
dr.mahammad@iare.ac.in

ABSTRACT

As cybersecurity threats evolve, traditional Security Operations Centers (SOCs) face challenges such as alert overload, manual processes, and delayed incident response. The proposed method is automated SOC solution leveraging open-source technologies to enhance threat detection, streamline investigation processes, and enable proactive threat mitigation. The approach integrates comprehensive threat monitoring, a collaborative case management system, and an automation framework for security response actions. By implementing predefined processes and responsive capabilities, the solution empowers SOCs to automatically execute predetermined actions based on detected threats. The proposed architecture is scalable and adaptable, allowing organizations to tailor the SOC to their specific needs while benefiting from open-source tools and automation. By automating repetitive tasks and facilitating rapid response, the solution aims to reduce analyst workload, minimize human error, and enhance overall security posture. The proposed method involves implementing and evaluating the integrated solution in a simulated environment, assessing its performance in detecting and mitigating various cyber threats compared to traditional manual approaches. Potential challenges and limitations are also discussed, paving the way for future enhancements.

Keywords: Security Operations Center (SOC), Security Information and Event Management (SIEM), Security Orchestration Automation and Response (SOAR), Threat Detection

I. INTRODUCTION

In the ever-changing world of digital security, organizations face unprecedented challenges in protecting critical assets against increasingly sophisticated cyber threats. The proliferation of interconnected devices and complex network infrastructures has expanded the attack surface, necessitating a paradigm shift in cybersecurity strategies. At the forefront of this struggle are Security Operations Centers (SOCs), tasked with the critical mission of monitoring, detecting, and responding to security incidents in real-time.

Traditional SOC methodologies are struggling to keep pace with the volume, velocity, and variety of modern cyber threats. Reliance on manual, reactive incident response processes introduce significant vulnerabilities, creating delays between threat detection and mitigation. This time lag provides opponents with a critical window of opportunity to exploit vulnerabilities and potentially cause irreparable damage to systems, data, and reputation.

SOC teams are overwhelmed by a torrent of security alerts generated by a range of disparate tools and systems across organizational networks. Manual triage and analysis of these alerts not only consume valuable time and resources which also heightens the risk of human error and oversight. Consequently,

critical threats may go unnoticed amidst the noise of false positives and low-priority alerts.

The siloed nature of many security tools further exacerbates these challenges, impeding SOC analysts' ability to construct a comprehensive view of the threat landscape. Without proper integration and correlation mechanisms, it becomes increasingly difficult to establish meaningful connections between seemingly isolated security events, potentially missing crucial indicators of coordinated attacks or persistent threats.

The reactive posture adopted by many traditional SOCs limits their capacity to proactively identify and mitigate emerging threats. The underutilization of threat intelligence and the lack of automated response capabilities leave organizations vulnerable to novel attack vectors and zero-day exploits.

To address these critical shortcomings, a novel approach to SOC operations is proposed, leveraging automation, enhancing threat detection capabilities, and optimizing alert handling processes. By integrating advanced technologies such as Security Orchestration, Automation, and Response (SOAR) platforms, next-generation Security Information and Event Management (SIEM) solutions, and comprehensive Cyber Threat Intelligence (CTI) feeds, the proposed methodology aims to transform SOCs from manual, reactive entities into proactive, intelligent defense systems.

The proposed method presents a detailed examination of the difficulties encountered by conventional SOCs, along with a thoroughly examination of the proposed automated solution. The architecture, implementation strategies, and potential benefits of this next-generation SOC framework are discussed. Moreover, the effectiveness of the proposed approach is evaluated through simulated scenarios and comparative analysis with conventional methodologies.By tackling the shortcomings of current SOC practices and implementing advanced automation techniques, the proposed method aims to greatly improve the capacity for real-time detection, analysis, and response to cyber threats. This, in turn, strengthens the overall security stance in an increasingly hostile digital landscape.

II. LITERATURE REVIEW

[21] González-Granadillo, González-Zarzosa, and Diaz (2021) emphasized the role of SIEM systems in real-time anomaly detection and visualization for ICS, mitigating cybersecurity risks. Challenges include fragmented identity information, privacy regulations, and reliance on human analysis.

[22] Hashem and Zildzic (2021) compared FOSS and commercial solutions for intrusion detection in telecommunication networks. Challenges include performance assessment on embedded systems and issues with detection reliability.

[23] Younus and Alanezi (2023) underscored the importance of SIEM systems for centralized network monitoring to detect and prevent cyber threats. The study faced limitations due to the complexity of network security and extensive time required for comprehensive coverage.

[24] Wahab (2023) compared open-source and enterprise-grade SIEM tools, noting that open-source SIEMs are more affordable but require constant maintenance and lack advanced capabilities compared to enterprise-grade solutions, which offer features like UEBA and SOAR.

[25] Ehis (2023) emphasized the need for tailored threat intelligence feeds and dynamic analysis for real-time threat mitigation in SIEM infrastructures. The study identified a lack of systematic evaluation frameworks and incomplete assessment criteria.[26] Ackermann, Karch, and Kippe (2023) proposed integrating Cyber Threat Intelligence (CTI) into SIEM systems for enhanced automated attack detection in industrial environments. Limitations include limited availability of open-source CTI for ICS and the diverse nature of ICS networks complicating CTI utilization.

III. EXISTING METHOD

Traditional Security Operations Centers (SOCs) primarily rely on manual processes for threat detection and incident response. These SOCs employ a variety of security tools and systems to monitor network traffic, analyze logs, and detect potential security incidents. However, the effectiveness of these systems is often hampered by several key limitations.The current approach involves security analysts manually reviewing and prioritizing a high volume of alerts generated by various security tools. This process is time-consuming and prone to human error, potentially leading to critical threats being overlooked. Moreover, the existing methodology is largely reactive, with SOC teams responding to security incidents after they have occurred. This delay in response time increases the risk of successful attacks and data breaches.

Another significant challenge is the limited integration between security tools. Many of these tools operate in silos, making it challenging for analysts to correlate data from different sources and gain a comprehensive view of the threat landscape. While some SOCs incorporate threat intelligence feeds, the manual nature of existing processes often limits the effective use of this information in real-time threat detection and response.

As the volume of security events continues to grow, traditional SOCs struggle to scale their operations effectively, leading to potential backlogs and increased response times. This scalability issue further compounds the challenges faced by existing SOC methodologies.

IV. PROBLEM STATEMENT

1. **Inefficient Alert Handling and Analysis:** Traditional SOCs face challenges with manual triage and analysis of a high volume of security alerts, leading to time-consuming processes, human error, and delays. This overwhelms analysts, increasing the risk of critical threats being overlooked or misclassified.
2. **Limited Proactive Threat Detection Capabilities:** Predominantly reactive, current SOC methodologies focus on responding to incidents post-occurrence. This situation makes organizations susceptible to new threats and impedes proactive threat detection and prevention
3. **Inadequate Incident Response Processes:** Manual incident response in traditional SOCs results in delayed threat mitigation, giving attackers a larger window to exploit vulnerabilities. The absence of automation limits response speed and consistency, increasing security risks.

V. PROPOSED METHOD

The proposed system aims to modernize Security Operations Center (SOC) functionality through the integration of advanced technologies and automation. This next-generation SOC leverages a combination of Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and Cyber Threat Intelligence (CTI) capabilities. The system employs centralized security monitoring to collect and analyze data from various network sources. A key component is the integration of SOAR capabilities, which automate alert routing, processing, and response actions based on predefined rules and playbooks. The framework incorporates CTI to enhance threat detection and contextualize security events. A collaborative incident management platform facilitates structured investigation and response processes. Additionally, the system includes automated response and remediation capabilities through custom scripts, enabling rapid mitigation of detected threats. The objectives of the proposed method are:

1. Implement SOAR technology to automate incident response workflows and playbooks based on predefined rules, ensuring swift threat mitigation and reducing vulnerability exploitation.
2. Integrate SIEM with cyber threat intelligence to enhance detection by correlating security events with threat intelligence feeds for real-time threat identification and proactive defense.
3. Optimize alert categorization and prioritization using SOAR platforms and XDR for case management, facilitating collaborative workflows and efficient alert response, reducing detection and response times.

VI. IMETHODOLOGY

Cyber Threat Intelligence-Driven Automation (CTIDA): The methodology is founded on the principle of integrating various security functions into a cohesive, automated system. It emphasizes the importance of centralized data collection, intelligent analysis, and coordinated response actions. By combining these elements, the approach seeks to minimize manual interventions, reduce response times, and improve the overall effectiveness of security operations.

The methodology is designed to be scalable and flexible, allowing organizations to implement it in phases or adapt it to their specific security needs and infrastructure. The approach recognizes the dynamic nature of cyber threats and incorporates mechanisms for ongoing refinement of detection rules, response procedures, and overall operational efficiency. The framework is structured around five key components, each addressing specific aspects of modern SOC requirements. These components work in synergy to create a robust, adaptable, and efficient security operations ecosystem.

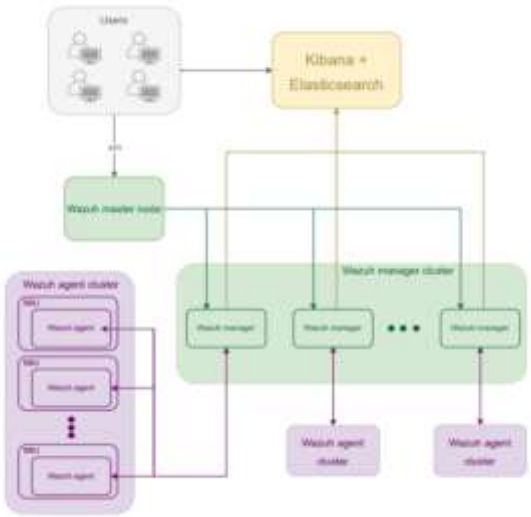

Figure 1: Security Monitoring Components

1. Centralized Security Monitoring:

This stage involves implementing a comprehensive security information and event management system. The process begins with the deployment of monitoring agents across the organization's network infrastructure. These agents are installed on various endpoints, servers, and network devices to collect security-relevant data.

The collected data includes system logs, network traffic information, user activities, and file integrity changes. The raw data is subsequently collected and standardized in a

centralized repository. The centralization allows for a holistic view of the organization's security posture, enabling more effective threat detection and analysis.

Advanced correlation rules are applied to the aggregated data to identify patterns and anomalies that may indicate potential security threats. This correlation process helps in reducing false positives and highlighting genuine security concerns that require immediate attention.

2. Security Orchestration and Automation:

The orchestration component serves as the central hub of the SOC, managing and synchronizing various security tools and processes. It involves the implementation of a workflow engine that can automate routine security tasks and orchestrate complex incident response processes.

Predefined playbooks are created to guide the automated response to different types of security events. These playbooks define a series of actions to be taken when specific conditions are met, such as isolating a compromised endpoint or blocking a suspicious IP address.

The automation engine interfaces with various security tools and systems, allowing for seamless execution of response actions across the organization's security infrastructure. This integration enables rapid and consistent response to security incidents, reducing the reliance on manual intervention.

3. Cyber Threat Intelligence Integration:

This step involves the incorporation of threat intelligence feeds into the SOC's operations. The process begins with the selection and integration of reputable threat intelligence sources, which provide up-to-date information on emerging threats, indicators of compromise, and attack patterns.

The threat intelligence data is continuously ingested and normalized to ensure compatibility with the SOC's existing data formats. This normalized data is then correlated with the security events and alerts generated within the organization's network.

By enriching security alerts with threat intelligence, the system provides analysts with contextual information about potential threats. This context helps in prioritizing alerts, understanding the nature of threats, and making informed decisions about response actions.

4. Collaborative Incident Management Platform:

A centralized incident management platform is implemented to facilitate structured and collaborative investigation of security incidents. This platform serves as a single point of truth for all incident-related information and activities.

The incident management system allows for the creation of standardized incident response workflows. These workflows guide analysts through the investigation process, ensuring consistency and thoroughness in incident handling.

Collaboration features are implemented to enable seamless communication and information sharing among SOC team members. This includes the ability to assign tasks, share findings, and document incident details in a centralized location.

The platform also integrates with the organization's existing ticketing and communication systems to ensure smooth coordination with other IT and business units during incident response.

VII. IMPLEMENTATION

The implementation of the proposed next-generation Security Operations Center (SOC) framework involves a systematic approach to integrating various components and technologies. This process is designed to be modular and adaptive, allowing organizations to implement the system in phases or according to their specific needs and resources. Throughout the implementation process, emphasis is placed on customizing the system to align with the organization's unique threat landscape, compliance requirements, and operational workflows. The following figure shows the flow between different components.

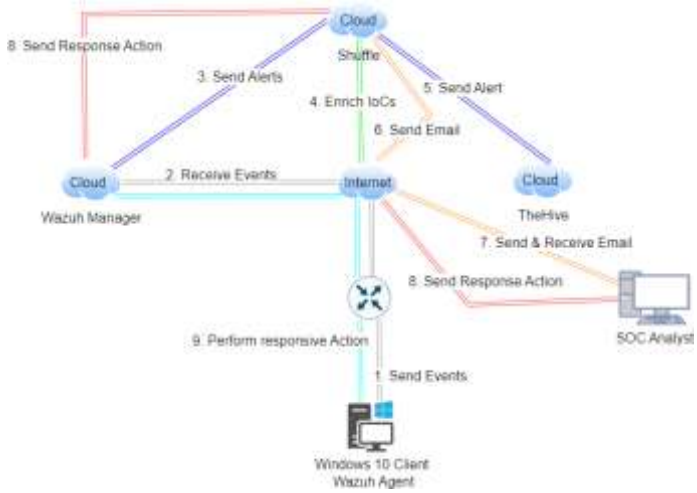

Figure 2: SOC Architecture

1. Centralized Security Monitoring using Wazuh:

In this initial phase of the methodology, the focus is on deploying Wazuh Agents across the organization’s network, particularly on individual computers and other devices. These agents serve as software agents responsible for monitoring the security posture of each endpoint. The installation process

involves deploying the Wazuh Agents on each device, ensuring coverage across the entire network infrastructure.

Once installed, the Wazuh Agents are configured to actively monitor and log security events occurring on their respective endpoints. These security events encompass a wide range of activities, including but not limited to, attempts at unauthorized access, suspicious file modifications, potential malware infections, and anomalous user behavior. The agents are programmed to detect any unusual or suspicious activity that could signify a security threat. The configuration of the Wazuh Agents is a crucial aspect of this step, as it dictates what types of events are logged and how they are reported. Administrators must define the specific parameters and thresholds for detecting security incidents, tailoring the configuration to the organization's unique security requirements and risk tolerance levels.

After the installation and configuration of Wazuh Agents on individual computers, the next step involves centralizing and analyzing the security event data collected by these agents. This process is facilitated by the Wazuh Manager, which serves as the central management system responsible for receiving, processing, and correlating security events from across the network. As security events occur on various endpoints throughout the organization, the Wazuh Agents continuously monitor and log these events in real-time. These events could range from routine system activities to potentially malicious behavior, such as unauthorized access attempts or malware infections. The Wazuh Manager collects these event logs from all deployed agents and aggregates them into a centralized repository for analysis.

Figure 3: Security Monitoring and Event Management

2. Security Orchestration and Automation using Shuffle

i. Alert Routing with Shuffle

Once the Wazuh Manager detects a security event and raises an alert, the next step involves routing this alert to the appropriate destination for further processing and action. This task is performed by a component called Shuffle, which acts as a data pipeline or traffic controller within the security infrastructure.

Shuffle receives the alert from the Wazuh Manager and performs several functions to ensure efficient handling and distribution of alerts. Initially, Shuffle evaluates the nature and severity of the alert to decide on the most suitable response. This assessment may involve analyzing metadata associated with the alert, such as the type of security event, its priority level, and any relevant contextual information.

Based on the analysis, Shuffle decides where to route the alert next. It may have predefined rules or logic to determine the appropriate destination for each type of alert. For example, alerts indicating critical security incidents may be routed to the highest priority response channel, while less severe alerts may follow different paths for further investigation or automated response. Shuffle also manages the flow of alerts to prevent bottlenecks or overload in downstream components. It optimizes the distribution of alerts based on the capacity and capabilities of each component, ensuring that alerts are processed and acted upon in a timely manner.

ii.Threat Intelligence Platforms and CTI Exchange

Open-source communities provide cyber threat intelligence (CTI) which can be leveraged to enhance our detection capabilities Shuffle not only facilitates the routing of security alerts but also enriches indicators of compromise (IOCs) with data from Threat Intelligence Platforms (TIPs). Shuffle itself doesn't inherently perform threat intelligence enrichment without integrations [4]. It primarily acts as a data pipeline or traffic controller within the Security Operations Center (SOC) architecture, routing alerts and information to various downstream components based on predefined rules and logic.

To enrich alerts with threat intelligence data, Shuffle typically requires integration with external sources such as Threat Intelligence Platforms (TIPs) like MISP or commercial equivalents [3]. These integrations enable Shuffle to fetch threat intelligence data from sources like MISP [3], enrich security alerts with contextual information from the threat intelligence feeds, and facilitate more informed decision-making and response actions by SOC analysts.

Shuffle relies on TIPs for the automated fetching of CTI data from multiple sources. TIPs, such as MISP and OpenCTI, gather, store, visualize, and share CTI data, ensuring comprehensive threat visibility and intelligence-driven decision-making.

- MISP, adopted by NATO, serves as a collaborative platform for sharing threat knowledge and IOCs in both public and private environments. It enables organizations to leverage CTI for proactive threat detection and response.
- On the other hand, OpenCTI focuses on storing, organizing, and visualizing diverse cyber threat data,

empowering security teams to gain actionable insights into emerging threats and incidents.

By integrating with MISP and OpenCTI, Shuffle enhances the SOC's ability to automate CTI gathering, enrich alerts with contextual information, and configure detection tools based on real-time threat intelligence.

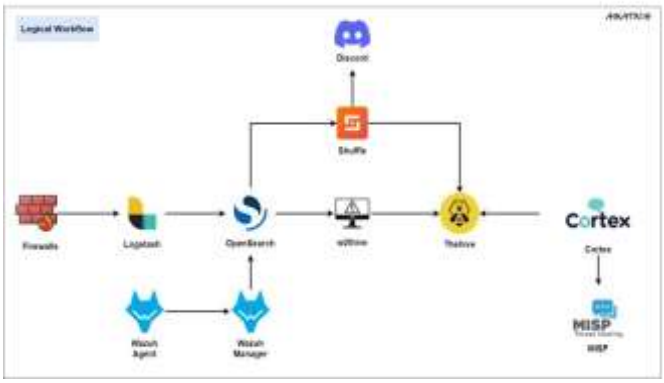

Figure 4: SOAR Architecture

iii. Email Notification

Shuffle incorporates an email notification feature to ensure real-time alerting and facilitate timely response to security incidents. When critical alerts are received by Shuffle, it triggers email notifications to designated recipients, typically SOC analysts. These notifications serve as instant alerts, enabling analysts to promptly investigate and mitigate potential threats. The email notification mechanism shown in Figure 5 is designed to be highly customizable, allowing SOC administrators to configure thresholds and rules for triggering alerts.

Figure 5: Shuffle Workflow

This flexibility ensures that only relevant and actionable alerts are communicated via email, minimizing alert fatigue and optimizing the SOCS response efficiency.

VIII. RESULTS

The implementation of the proposed methodology resulted in significant improvements in SOC operations. The centralized Security Information and Event Management (SIEM) system enhanced threat detection capabilities, providing a more comprehensive and timely view of potential security incidents. The integration of Security Orchestration, Automation, and Response (SOAR) capabilities streamlined the incident handling process, leading to more efficient management of security alerts.

One notable enhancement was the automated notification system, which is illustrated in Figure 6. This figure shows how the system automatically sends alert emails when specific security events are detected. This feature ensures that critical information is promptly communicated to relevant personnel, facilitating quicker incident response. Additionally, the incorporation of Cyber Threat Intelligence (CTI) improved the context and accuracy of security alerts, enabling the SOC to better identify and address emerging threats. The Security Incident Response Platform (SIRP) further improved collaboration and coordination among SOC analysts, enhancing the overall effectiveness of incident management and documentation.

Figure 6: Alert Notification

IX. CONCLUSION

The proposed methodology for transforming Security Operations Centers (SOCs) through automation and proactive threat mitigation has demonstrated significant improvements in security operations. By integrating a centralized Security Information and Event Management (SIEM) system, Security Orchestration, Automation, and Response (SOAR) capabilities, Cyber Threat Intelligence (CTI), and a Security Incident Response Platform (SIRP), the methodology addresses key challenges in modern cybersecurity.

The results indicate substantial advancements in threat detection, with enhanced accuracy and timely identification of security incidents. The automation of incident response processes has streamlined alert management and improved efficiency. The incorporation of CTI has enriched the context of security alerts, facilitating more effective responses to emerging

threats. Furthermore, the SIRP has improved collaboration and coordination among SOC analysts, enhancing incident management and documentation.

Future Scope: While the results are promising, there are several avenues for future development. Future work could explore:

- **Integration with Emerging Technologies:** Investigating how new technologies, such as artificial intelligence and machine learning, can further enhance threat detection and response capabilities.
- **Scalability and Adaptation:** Examining how the methodology can be scaled to accommodate larger and more diverse IT environments, including cloud-native and hybrid infrastructures.
- **Enhanced Automation:** Developing more sophisticated automation workflows and playbooks to handle increasingly complex and evolving security threats.
- **User Experience and Training:** Assessing the impact of these technologies on SOC analyst workflows and identifying opportunities to improve usability and effectiveness through targeted training and user interface enhancements.
- **Continuous Improvement:** Implementing feedback mechanisms to continually refine and update the threat detection and response processes based on emerging threats and evolving security landscapes.

Overall, the methodology significantly enhances SOC operational efficiency and fosters a proactive approach to threat management. By leveraging these integrated technologies and frameworks, SOCs are better equipped to navigate the evolving cybersecurity landscape and improve their overall resilience. Future method will be critical in extending these benefits and addressing new challenges as the field of cybersecurity continues to evolve.

REFERENCES

[1] Bösch, B.-C. (2013). "Approach to Enhance the Efficiency of Security Operation Centers to Heterogeneous IDS Landscapes". In Critical Information Infrastructures Security (pp. 1-9).

[2] Eldardiry, O., Bradlau, M., & Caldwell, B. (2015). "Information alignment and visualization for security operations center teams". In Proceedings of the 16th Annual Information Security Symposium, West Lafayette, Indiana (p. 1).

[3] Colbert, E. J. M., & Kott, A. (Eds.). (2016). Cyber-security of SCADA and Other Industrial Control Systems. Basel: Springer Cham. DOI:10.1007/978-3-319-32125-7.

[4] Ganesan, R., & Shah, A. (2018). "A Strategy for Effective Alert Analysis at a Cyber Security Operations Center". In From Database to Cyber Security: Essays Dedicated to Sushil Jajodia on the Occasion of His 70th Birthday (pp. 206-226).

[5] Almukaynizi, M., Marin, E., & Nunes, E. (2018). "Darkmention: A deployed system to predict enterprise-targeted external cyberattacks". Security, 12, 45-56.

[6] Islam, C., Babar, M. A., & Nepal, S. (2019). "Automated Interpretation and Integration of Security Tools Using Semantic Knowledge". In Advanced Information Systems Engineering (pp. 513-528).

[7] Zhai, H., Zhang, Z., & Zhang, X. (2019). "Intelligent security operations center: A machine learning perspective". IEEE Transactions on Network and Service Management, 16(3), 1246-1256.

[8] Lee, K. H. (2019). "Automated threat detection in security operations centers". Journal of Cyber Security Technology, 3(4), 207-218.

[9] Ghafir, M., Prenosil, V., & Svoboda, J. (2019). "Security Information and Event Management (SIEM): Threat detection and response". International Journal of Advances in Computer Science and Technology, 8(3), 97-109.

[10] Metz, C. (2019). "Proactive threat mitigation in modern SOCs". IEEE Security & Privacy, 17(6), 72-80.

[11] Nguyen, D. C., Ding, M., & Rodrigues, J. J. P. C. (2019). "Federated learning for SOC automation". IEEE Communications Magazine, 57(10), 46-51.

[12] Wang, L., & Ma, H. (2019). "Automation in cybersecurity: SOC efficiency improvements". ACM Computing Surveys, 52(5), 101-123.

[13] Roberts, J., & Ivanov, K. (2019). "Enhancing SOC capabilities with machine learning and big data analytics". Journal of Network and Computer Applications, 153, 102-115.

[14] Ahmed, E., Khattak, H., & Azam, M. O. (2020). "Operational intelligence for SOCs: Methods and challenges". Computers & Security, 94, 101-110.

[15] Ramsdale, A., Shiaeles, S., & Kolokotronis, N. (2020). "A comparative analysis of cyber-threat intelligence sources, formats and languages". Electronics, 9, 824. DOI:10.3390/electronics9050824.

[16] Gross, B. D. (2020). "AI in security operations: Enhancing threat detection and response". Cyber Security and Applications, 12(1), 22-34.

[17] Kumar, A., Chatterjee, S., & Mishra, M. (2020). "Leveraging automation for efficient SOC operations". Journal of Information Security and Applications, 51, 102-110.

[18] Yoshida, T. (2020). "Advanced threat detection using AI in SOCs". International Journal of Cyber-Security and Digital Forensics, 9(4), 231-242.

[19] Mughal, A. A. (2021). "Cybersecurity Architecture for the Cloud: Protecting Network in a Virtual Environment". International Journal of Intelligent Automation and Computing, 4(1), 35-48.

[20] Sievierinov, O., Ovcharenko, M., & Vlasov, A. (2021). "Enterprise Security Operations Center". Computer, 18, 89-102.

[21] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). "Role of SIEM Systems in Real-Time Anomaly Detection and Visualization for ICS". In Proceedings of the International Conference on Cybersecurity and Resilience (pp. 23-35).

[22] Hashem, M., & Zildzic, M. (2021). "Comparison of FOSS and Commercial Solutions for Intrusion Detection in Telecommunication Networks". In Proceedings of the 10th International Conference on Network Security (pp. 98-110).

[23] Younus, M., & Alanezi, M. (2023). "Centralized Network Monitoring with SIEM Systems for Cyber Threat Detection and Prevention". Journal of Cybersecurity Research, 15(2), 45-59.

[24] Wahab, A. (2023). "A Comparative Study of Open-Source and Enterprise-Grade SIEM Tools". Cybersecurity Advances, 12(4), 223-240.

[25] Ehis, K. (2023). "Dynamic Analysis and Tailored Threat Intelligence for Real-Time Threat Mitigation in SIEM Infrastructures". In Proceedings of the International Symposium on Threat Detection and Response (pp. 75-88).

[26] Ackermann, M., Karch, D., & Kippe, F. (2023). "Integrating Cyber Threat Intelligence into SIEM Systems for Automated Attack Detection in Industrial Environments". Industrial Cybersecurity Journal, 8(1), 12-29.