CyberOps: Cloud-Driven SOC with Automation

Saisharan R
B.Tech Computer Science and Business Systems
Chennai Institute of Technology
Chennai, India
saisharanr77m@gmail.com

Dhanush Rahul M
B.Tech Computer Science and Business Systems
Chennai Institute of Technology
Chennai, India
dhanushrahul0907@gmail.com

Mr. Selvaganesan C
Assistant *Professor, Department of Computer Science and Business System,*
Chennai Institute of Technology
Chennai, India
selvaganesanc@citchennai.net

***Abstract*— In today's interconnected virtual realm, the need for robust digital protection is critical for businesses handling sensitive financial transactions. This research details the architecture and deployment of a Security Operations Center (SOC) using Wazuh SIEM for properly detecting threats, responding effectively and also proactive prevention including automation and compliance enforcement for a FinTech company. It also includes email security and file analysis. The system integrates on-premise and explores cloud-based SIEM solutions to address scalability challenges. Attack simulations using Linux based systems as an attacking system and Windows 11 VM as a monitored target validate the system's effectiveness in detecting cyber threats. Additionally, malware analysis tools such as ANY.RUN and VirusTotal improve threat intelligence. The automation with playbooks streamline the incident response process. Compliance adherence to PCI-DSS and GDPR is reinforced through continuous policy audits. Due to limited infrastructure and efficiency needs, the project explores cloud migration for scalable SOC operations. Furthermore, to mitigate phishing threats, email security measures are implemented to protect financial transactions. This study demonstrates the practical implementation of a SOC tailored for FinTech security, highlighting the benefits of automated security enforcement, phishing protection, and cloud migration.**

Keywords*— *Cybersecurity, Security Operations Center (SOC), Wazuh SIEM, Threat Detection, Compliance, Cloud Security, FinTech Security, Automation, Phishing Protection.

I. INTRODUCTION

The central objective of the attackers is that the finance and money industry inherently becomes the prime target of cyberattacks since its business solutions are involved in online payment solutions, digital wallets, and transaction processing [15]. In security defense against threats like malware and phishing, which fundamentally seek unauthorized access, businesses need a robust Security Operations Center (SOC) with real-time threat detection and response [5]. This article examines the use of a SOC with Wazuh SIEM in addressing such security challenges.

The system that is being proposed creates a Security Operations Center (SOC) where Wazuh SIEM is combined with endpoint security and attack simulation, facilitating real-time detection and response of threats. With the incorporation of advanced threat intelligence tools such as ANY.RUN and VirusTotal, the system enhances security analysis through continuous scanning of the document and URL retrieved from mail. Automated security playbooks are employed to enhance incident response effectiveness in terms of blocking threats instantly and correctly without any intervention.

In addition to real-time threat detection, the solution is also secured to provide regulatory financial compliances such as PCI-DSS and GDPR in protecting sensitive financial data and restraining legal exposure. To further increase scalability and diversity, cloud migration is planned to facilitate simple security monitoring of flexible infrastructures. Furthermore, firm security measures against email are initiated to protect and block phishing emails on financial transfers, supplementing overall cyber-attack resilience.

II. LITERATURE SURVEY

Accurate logging and monitoring of all incidents with various security solutions specialists on

particular logs are a critical role in cybersecurity to maintain the required level of security and compliance enforcement [4] (Vielberth et al., 2020). There are a number of commercial and open-source SIEM solutions, each having unique characteristics. A cost-effective and scalable open-source solution incorporating diverse security solutions such as SIEM, Extended Detection and Response (XDR), regulatory compliance, file integrity monitoring, and incident response [5] (Wazuh, 2025). In contrast to traditional SIEMs, which tend to call for costly licenses and maintenance, the existing demand is an open and agile substitute to security for any organization of size and threats. The capability to be utilized on-premises and in the cloud provides security visibility across shifting infrastructures and is therefore an appropriate solution for hybrid and multi-cloud-enabled organizations [6] (Zhang et al., 2020).

As much as the SIEM products originated to be implemented for log accumulation and anomaly scanning, with most internet services enlarging and developing numerous new security technologies, responses to incidents now need to occur automatically and based on more advanced threat intelligence [11] (Splunk Inc., 2024). Our solution tackles all these issues with the incorporation of a standardized template that aims at eliminating human reaction time and response. Existing literature on SIEM systems addresses the necessity of dynamic security controls, which can evolve with the dynamically evolving cyber attacks [6] (Zhang et al., 2020). Modular structure and capability integration enable companies to tailor their security operations according to their threat environment [5] (Wazuh, 2025).

Another key area of cybersecurity concern is phishing detection and response. Sophisticated email security software is designed with spam filters and rudimentary anti-phishing functions, but they are insufficient for the critical business processes, and hence they find it difficult to deal with zero-day phishing and sophisticated social engineering methods [2] (Gupta et al., 2017). Current email security software does not have robust detection models that have machine learning-driven anomaly detection, behavior monitoring, and threat intelligence feeds. Consequently, organizations remain to be under severe attack as a result of phishing of financial transactions and identity theft [8] (Bilge & Dumitras, 2012). Such limitations can be surpassed by more secure email paradigms that entailed recognizing and acting upon phishing threats in real-time. When combined with SIEM offerings of real-time analysis and remediating, an end-to-end view of the attack vector is attained [13] (IBM, 2024).

Cybersecurity threat research identifies the growing sophistication of zero-day attacks and malware. The evidence shows that conventional antivirus tools are not adequate to handle emerging cyber threats, and hence active threat intelligence and behavior analysis-based detection systems are required [7] (Stiborek et al., 2021). Malware analysis techniques have been studied to a significant degree, highlighting the need to combine sandbox-based detection, static analysis, and dynamic analysis with SIEM solutions [1] (Aycock, 2017); [3] (Mell et al., 2005). Requirement for the definitive feature by making threat intelligence enrichment central and centralized along with providing automated response playbooks in the foundation security solution [5] (Wazuh, 2025).

Cloud security has also become a highly significant field of research due to the universal usage of cloud computing. Conventional security controls are generally short in dealing with cloud-specific threats, which have necessitated specific cloud security technologies. The MITRE ATT&CK framework has been extensively used in closing attack tactics and improving detection capacity [12] (Mitre, 2025). Apart from that, globally recognized SIEM solution providers like IBM QRadar and Splunk also contributed to security monitoring and cloud-incident response automation literature [13] (IBM, 2024); [11] (Splunk Inc., 2024).

This research is a continuation of previous work in utilizing a cloud-based SOC that combines Wazuh SIEM with automated incident response and anti-phishing defense capabilities. By investigating cloud migration, threat intelligence enrichment, and automation-enforced security, this research is an advancement of the frontier for scalable and proactive cybersecurity in financial institutions [16] (SANS Institute, 2024).

III. PROBLEM STATEMENT & SOLUTION

FinTech companies are confronted with various cyber threats that disrupt financial transactions and regulatory compliance, which are time-consuming and reputation-damaging. Ineffective real-time monitoring is one of the greatest challenges, leading to slow response to incidents and therefore leaving the organizations vulnerable to security loopholes. Not being able to automate threat detection and response only contributes to aggravating the situation, mostly due to the fact that manual intervention is extremely time-consuming and riddled with human errors. Furthermore, failure to conform to financial standards such as PCI-DSS and GDPR has huge financial consequences and loss of reputation. Further, one drawback is that SIEM software solutions in the premises are not very scalable, hence businesses must suffer difficulties in sustaining increasing security demands. Further, email phishing is still one of the most effective attacks, exploiting financial transactions and exposing sensitive information to cyberthieves.

To address such primary security threats, the referred system utilizes Wazuh SIEM for end-to-end log collection in totalling, real-time monitoring, and threat correlation in seeking additional security event knowledge. Cyberattacks simulated via cybertests or tests utilizing Kali Linux are performed to study detection and filtering threats by Wazuh. Such simulation through advanced malware analysis tools with a security-aware nature, such as ANY.RUN and VirusTotal, is utilized in providing in-depth awareness on security issues, e.g., detailed description of cyber threats. The solution also includes automated security playbooks, reducing human processes and enabling real-time response to threats. The solution also examines cloud migration, with agile and flexible security infrastructure that is able to transition to adjust to emerging threats. Advanced email security controls are imposed in a bid to scan for and prevent phishing attacks and annihilate threats in fraudulent financial activities.

IV. METHODOLOGY & IMPLEMENTATION:

The configuration of the system combines Wazuh SIEM as the core security solution with a Windows 11 system as the endpoint to be secured and a Linux system as the origin of the simulated attack, as illustrated in Fig. 4.1. As would be easily apparent from the architecture diagram, this configuration provides a sandbox environment to test and verify the security controls before deploying them enterprise-wide. Threat intelligence capabilities are supplemented by in-house tools such as ANY.RUN and VirusTotal to track malicious activity and suspicious activity and provide comprehensive analysis of potential security risks [1] [3]. Fig. 4.1 This integration of the tools with Wazuh SIEM provides an end-to-end security monitoring solution ensuring maximum detection accuracy with fewer false positives.

For compliance with regulatory needs, the system is PCI-DSS and GDPR compliant [17] with real-time monitoring and auto-compliance scanning to protect sensitive financial information. This aligns with best practice as outlined by the Cloud Security Alliance [17] for financial institutions within the online environment. Security playbooks are also utilized to automate incident response, reducing manual effort and response time in accordance with SANS Institute guidelines [16]. These playbooks are built on top of the MITRE ATT&CK framework [12] in an effort to categorize and eliminate threats through provided tactics, techniques, and procedures (TTPs). The email security controls are built into the solution to detect and prevent phishing attempts at financial transactions, which spans a major identified vulnerability listed on recent threat reports [15][2].

Wazuh SIEM server was deployed in on-premises configuration, gathering security logs of the Windows 11 endpoint as shown in Fig. 4.1. The configuration adheres to architectural recommendations outlined by Scarfone and Mell [10] for intrusion detection and prevention systems. A number of attack simulations were conducted using Kali Linux, including brute-force attacks in order to test authentication monitoring validity, phishing simulation for testing email security effectiveness, and malware execution in order to test endpoint detection features. Test cases were created by using the cyber kill chain model [9], including real-life scenarios on how the system detects and responds to cybersecurity attacks at different levels of an attack.

Security event analysis was performed by SIEM log correlation, which detected anomalies and discovered suspicious activity in real time. As shown in Figure 4.1, endpoint-to-SIEM server data transmission offers end-to-end visibility of security incidents in the environment. The alerts were also automated to notify security teams of likely attacks, and security playbooks allowed quick response to threats by reducing attack impact based on industry standards [16]. Email security was complemented by blocking phishing attacks and designing detection algorithms based on recommendations presented by Gupta et al. [2] and Bilge & Dumitras [8].

To guarantee regulatory compliance for PCI-DSS and GDPR, security configurations were kept under close observation of Wazuh policy monitoring, which detected and reported deviation as indicated in the compliance workflow section of Fig. 4.1. Compliance enforcement such as this ensured data integrity and privacy of sensitive financial information and therefore complied with a key compliance requirement of FinTech organizations operating in the regulated space [17]. The policy monitoring system was validated for compliance with regulatory agencies' prespecified compliance frameworks to ensure end-to-end security control coverage.

Fig. 4.1 illustrates how the various components of the system interact to create a unified security monitoring and response platform. The architecture demonstrates the data flow from security events generated at endpoints through the SIEM analysis engine and ultimately to the security operations team. This design enables both automated and manual response capabilities, providing flexibility in addressing different types of security incidents based on their severity and complexity.

Fig. 4.1 presents the manner in which different aspects of the system integrate to provide an integrated security response and monitoring platform. The design depicts data travel from the initiation of security incidents at the endpoint to SIEM analysis engine and eventually to the security operation group. The architecture is suited to accommodate automatic and manual response, and with such, the degree of handling multiple categories of security incidents differently by severity and level of complication remains flexible.

Other than on-premises deployment, the research also thought about hosting Wazuh SIEM on a cloud infrastructure. The research was grounded in the economic advantage of implementing cloud technology through the cost of savings, enhancing scalability to match increased security needs, and minimal maintenance processes over on-premises deployments. Cloud SIEM is scalable, and therefore a viable option for FinTech organizations willing to enhance their security processes.

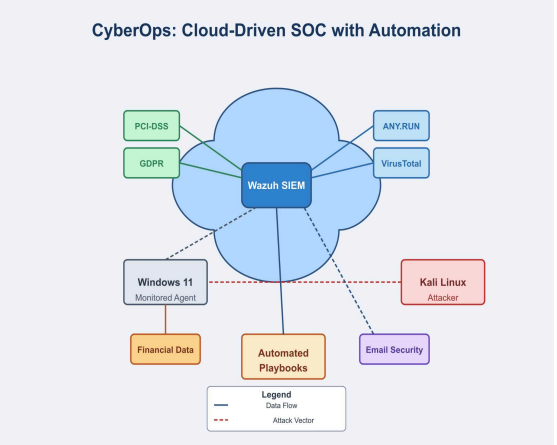

Figure 4.1 Project Architecture

V. EXPERIMENTAL RESULTS:

Cloud-based SOC performance with automation was confirmed through attack simulations and security monitoring testing. Wazuh SIEM was installed in an on-premises setup and retested to relocate it to the cloud. Brute-force and malware run attacks were launched from a Kali Linux attack platform against a Windows 11 machine under monitoring. The SIEM detected brute-force login attacks within seconds, thus confirming real-time threat detection. Malware execution scans, augmented by ANY.RUN and VirusTotal, also improved threat intelligence, with a good detection rate accurately flagging malicious files.

Incident response was transformed by automating it. Several minutes to almost half an hour response times were cut down to less than five minutes with security playbooks. Automated features offered rapid threat containment, for instance, real-time IP blacklisting and suspicious file quarantine. All of these were automated to minimize human intervention to get faster and more uniform threat containment.

Cloud migration tests demonstrated scalability advantages and reduced maintenance overheads. Cloud deployment demonstrated better alert processing time in addition to resource optimization of use compared to on-premises. Compliance-enforcing problems and delays in data exchanges existed and demonstrated where there would be optimization needed prior to exiting large-scale.

For regulatory compliance, the system was continuously checking security settings based on PCI-DSS and GDPR. Policy updates could detect misconfigurations, which were corrected within the time frame so that the system's capability to remain in compliance with regulatory requirements was not affected. Overall, the findings validate the effectiveness of a cloud SOC to detect threats in real time, respond to threats, and provide protection from cyber attacks and future improvement in upgrading alert systems and anti-phishing capabilities.

VI. DISCUSSION & FUTURE ENHANCEMENTS:

This paper describes the deployment of SOC by implementing Wazuh SIEM specifically for FinTech cybersecurity. By means of attack simulation, malware analysis, email protection, and automation, the research testifies to real-time detection and response capability. Fig. 4.1 displays the project architecture describing communication between the Wazuh SIEM server, monitored endpoints, and attack simulation solutions. The results identify the benefit of cloud-based SIEM, reiterating its scalability and cost-effectiveness potential for security monitoring.

While the system efficiently handles security threats, there are aspects that are still constrained: False positives in log monitoring need improvement in alert rules. AI-based phishing detection can be used in the implementation of email security. Multi-cloud SIEM integration would also add more security visibility between cloud providers.

VII. CONCLUSION:

This study presumes a cloud Security Operations Center (SOC) on Wazuh SIEM for robust FinTech cybersecurity. The system is very efficient in managing bulk security threats like phishing, malware attacks, and scalability capacity based on real-time attack detection, automated security breaches with playbooks, and regulation compliance enforcement. Simulation-based integration of attacks through malware test environments like ANY.RUN and VirusTotal gives threat intelligence to recognize and respond with maximum available efficiency to detect. Integration security functionality in email also gives an additional layer of security of financial transactions that level-set the risk by the mode of phishing attacks.

The results offer cloud SIEM benefits in terms of scalability, flexibility, and cost-effectiveness compared to on-premises legacy infrastructure. The system removes human labor and response time by providing real-time security monitoring and automated incident response to maximize the effectiveness of cyber defense processes.

Despite success, there is room for improvement, the research finds. False positives in log analysis must be removed by detection rules to make it tighter. Match email security controls with AI-driven phishing detection for that much tighter security against advanced threats. Match multi-cloud SIEM solutions to extend security visibility across multiple clouds and allow even more threats to be uncovered.

In summary, the present research contributes to the dynamic cybersecurity model with proof of a compliance-based, automated, and scalable model of SOC for FinTech firms. Sophisticated AI-based threat detection techniques and dynamic security rules can be investigated in future research to provide additional immunity against future cyberattacks.

REFERENCES:

[1] Aycock, J. (2017). Computer Viruses and Malware. Advances in Information Security, 22.

[2] Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28(12), 3629-3654.

[3] Mell, P., Kent, K., & Nusbaum, J. (2005). Guide to malware incident prevention and handling. NIST Special Publication, 800-83.

[4] Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. IEEE Access, 8, 227756-227779.

[5] Wazuh Inc. (2025). Wazuh Documentation, Version 4.7.

[6] Zhang, K., Wang, X., & Wang, J. (2020). A Survey of Security Operations Center: Threat Detection and Response. IEEE Access, 8, 181513-181533.

[7] Stiborek, J., Bartos, V., & Řehák, M. (2021). Malware Detection and Analysis in Security Operations Centers: Challenges and Approaches. IEEE Access, 9, 1762-1780.

[8] Bilge, L., & Dumitras, T. (2012). Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World. ACM Conference on Computer and Communications Security (CCS), 833-844.

[9] Yadav, T., & Rao, A. M. (2015). Technical aspects of cyber kill chain. International Symposium on Security in Computing and Communication (SSCC), 438-452.

[10] Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication, 800-94.

[11] Splunk Inc. (2024). Splunk SIEM Documentation.

[12] Mitre Corporation. (2025). MITRE ATT&CK Framework.

[13] IBM. (2024). IBM QRadar SIEM: Security Intelligence and Analytics. IBM Security Whitepaper.

[14] Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication, 800-82

[15] European Union Agency for Cybersecurity (ENISA). (2023). Threat Landscape Report 2023.

[16] SANS Institute. (2024). Incident Response Playbook: Best Practices for Threat Hunting.

[17] Cloud Security Alliance (CSA). (2024). Cloud Security Guidance for Financial Institutions.

[18] Amazon Web Services (AWS). (2024). AWS Security Best Practices.

[19] Microsoft. (2024). Azure Security Center Documentation.

[20] FireEye (Mandiant). (2024). Threat Intelligence Report 2024.