Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 03 | Mar-2026
ISSN (O) 3107-6696

Intelligent SOC Dashboard for Continuous Log Analysis and Incident Responses

[1]Priyadharshini K, [2]Nagarani M

[1]Student, Department of Computer Science with Cybersecurity, Dr. N.G.P Arts and Science College, Coimbatore, priyakathirvel357@gmail.com

[2]Professor, Department of Computer Science with Cybersecurity, Dr. N.G.P Arts and Science College, Coimbatore, nagarani.m@drngpasc.ac.in

---

Abstract - The rapid expansion of digital infrastructure has significantly increased the volume of security-related data generated by organizations. Every network device, server, firewall, and application continuously produces logs that record system activities, user behavior, and security events. Analyzing this enormous volume of log data manually is inefficient and increases the risk of missing critical cyber threats. Traditional security monitoring systems lack centralized visibility and intelligent automation, resulting in delayed detection and slow incident response. This paper proposes an Intelligent SOC Dashboard for Continuous Log Analysis and Incident Responses that integrates centralized log collection, real-time log processing, automated threat detection, and structured incident response into a unified platform. The system continuously monitors incoming logs, analyzes suspicious behavior patterns, and generates real-time alerts to support security teams in mitigating threats effectively. By providing an interactive and centralized dashboard interface, the proposed system enhances operational efficiency, improves threat visibility, and reduces response time, thereby strengthening the overall cybersecurity framework of organizations.

KEYWORDS: Security Operations Center (SOC), Continuous Log Analysis, Real-Time Monitoring, Incident Response, Threat Detection,Cybersecurity, Log Management, Security Analytics, Centralized Dashboard, Alert Generation.

1. INTRODUCTION

A Security Operations Center (SOC) is a centralized facility responsible for continuously monitoring and analyzing an organization's security posture. In modern computing environments, organizations rely heavily on interconnected systems, cloud services, enterprise applications, and network infrastructures. These systems generate a massive amount of log data that contains valuable security information. Logs record events such as login attempts, file access activities, configuration changes, firewall traffic, and network communication patterns. However, the increasing complexity and volume of these logs make manual monitoring extremely challenging. Without intelligent analysis mechanisms, security teams may overlook early indicators of compromise, resulting in severe data breaches and operational disruptions. Therefore, there is a strong need for an intelligent SOC dashboard capable of performing continuous log analysis and supporting rapid incident response. The proposed system aims to bridge this gap by providing automated monitoring, centralized visualization, and real-time alert generation.

2. LITERATURE SUVEY

Several studies have emphasized the importance of centralized log management and intelligent threat detection systems in modern cybersecurity practices. Research in Security Information and Event Management systems highlights the role of aggregating logs from multiple sources into a unified repository for efficient analysis. Industry reports published by organizations such as IBM and Cisco indicate that delayed detection of security incidents significantly increases financial and operational damage. Furthermore, advancements in log analytics using platforms like Elasticsearch have demonstrated improved indexing, search performance, and real-time monitoring capabilities. Behavior-based detection approaches have also been widely studied as an alternative to traditional signature-based detection systems, offering improved detection of unknown or evolving threats. These existing studies collectively demonstrate the necessity of intelligent and automated SOC systems capable of continuous monitoring and proactive incident management metrics, emphasizing that adaptive behavior based techniques can provide proactive protection while minimizing false positives[7].collectively, these studies underscore the shift from reactive, signature based approaches toward dynamic, behavior driven detection strategies, which are essential for strengthening endpoint security in modern computing environments.

Literature Survey On Intelligent SOC, LOG Analysis And Incident Response Systems

S.No	Author & Year	Title of the Paper / Work	Technique Used	Key Contribution / Findings	Limitation
1	R. Sommer & V. Paxson (2010)	Outside the Closed World: On Using Machine Learning for Network Intrusion Detection	Machine Learning-based IDS	Introduced ML techniques for intrusion detection	High false positive rate
2	M. Roesch (1999)	Snort: Lightweight Intrusion Detection for Networks	Signature-Based Detection	Real-time traffic monitoring and alerting	Cannot detect unknown threats
3	Elastic Research Team (2020)	Real-Time Log Analytics Using Elasticsearch	Log Indexing & Search Engine	High-speed log storage and search	Requires proper configuration
4	Splunk Research (2019)	Security Information and Event Management (SIEM) Practices	Centralized Log Correlation	Improved log visibility in SOC	High licensing cost
5	IBM Security (2022)	Cost of a Data Breach Report	Threat Intelligence & SOC Analysis	Emphasized importance of faster incident response	Industry survey-based
6	A. Valdes & K. Skinner (2001))	Adaptive Intrusion Detection System	Correlation-based Detection	Event correlation improves detection accuracy	Limited scalability
7	Gartner Research (2021)	SIEM Magic Quadrant	SOC Tool Evaluation	Compared modern SOC platforms	Commercial focus

3. BACKGROUND STUDY

The evolution of cyber threats has necessitated a transition from reactive security models to proactive and intelligent monitoring systems. Traditional monitoring solutions primarily rely on static rules or signature-based detection methods, which are insufficient to detect new and sophisticated attacks. In large organizations, multiple security tools operate independently, generating logs that remain scattered across different systems. This lack of integration results in fragmented visibility and slower decision-making processes. Centralized log analysis systems address this issue by collecting and correlating logs from diverse sources. Modern SOC architectures utilize high-performance search and analytics engines such as Elasticsearch to manage large-scale data efficiently. By combining centralized storage with continuous behavioral analysis, organizations can identify anomalies, detect suspicious patterns, and respond to threats more effectively.

4. PROPOSED SYSTEM

The Intelligent SOC Dashboard is designed to operate as a centralized security monitoring and incident response platform. The system collects logs from various sources including firewalls, servers, applications, and network devices. These logs are transmitted to a centralized log collector module, where they are preprocessed and stored in a structured format. The stored logs are continuously analyzed by a processing engine that identifies suspicious patterns such as repeated failed login attempts, unusual IP activity, abnormal traffic spikes, and unauthorized access attempts. When the system detects anomalies, it generates real-time alerts and displays them on the dashboard interface. The dashboard provides a visual representation of security events, threat severity levels, and incident status updates. This integrated approach enables security analysts to monitor, investigate, and respond to threats efficiently within a single platform.

5. SYSTEM ARCHITECTURE

The system architecture of the Intelligent SOC Dashboard represents a structured flow of security data from generation to response. Initially, various log sources such as firewalls, servers, network devices, and applications continuously generate security logs that record system activities, user actions, and network events. These logs are transmitted to a centralized log collector, which aggregates and standardizes the data to ensure uniform formatting and smooth processing. The collected logs are then forwarded to the log processing and analysis engine, where real-time monitoring takes place. This engine examines the logs, applies predefined security rules, and identifies abnormal patterns such as repeated failed login attempts, unusual traffic spikes, or unauthorized access activities. After processing, the logs are stored in Elasticsearch, which enables fast indexing, efficient searching, and scalable storage of large volumes of security data. The SOC dashboard provides a visual interface that displays alerts, threat severity levels, and overall system status in an understandable format using charts and graphs. Finally, when a potential threat is detected, the alert and incident response module generates notifications and allows security teams to take immediate corrective actions, thereby reducing detection time and minimizing the impact of cyberattacks.

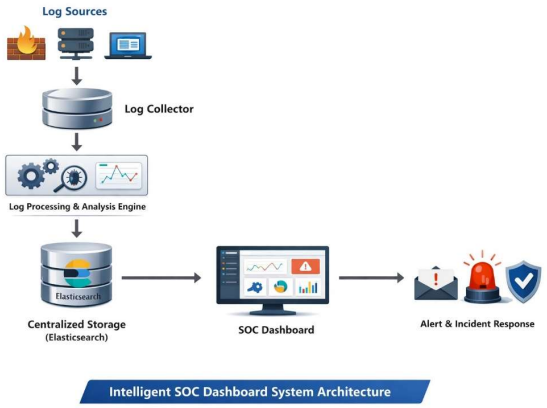

Fig 1:Intelligent SOC Dashboard System Architecture

6. CONTINUOUS LOG ANALYSIS WORKFLOW

The Continuous Log Analysis Flow represents the ongoing and automated process of monitoring, analyzing, and responding to security events within the SOC environment. The process begins with log generation, where various systems such as firewalls, servers, applications, and network devices continuously produce logs containing details about user activities, access attempts, traffic patterns, and system changes. These logs are then collected through a centralized log

collection mechanism that gathers and standardizes data from multiple sources to ensure consistency.

After collection, the logs are securely stored in a centralized repository, allowing both real-time and historical analysis. The real-time analysis stage continuously examines incoming logs using predefined rules and correlation techniques to identify abnormal behaviors, suspicious IP addresses, repeated login failures, or unusual system activities. When such anomalies are detected, the threat detection phase confirms potential security incidents by evaluating severity levels and impact. Once validated, the system automatically generates alerts and notifies the SOC team. Finally, the incident response stage enables security analysts to investigate the issue, take corrective actions such as blocking malicious traffic or isolating affected systems, and prevent further damage. This continuous cycle ensures 24/7 monitoring, faster detection, and effective mitigation of cyber threats.

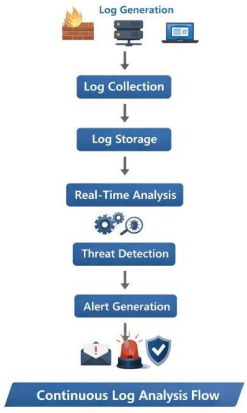

Fig 2: Continuous Log Analysis W orkflow

7. INCIDENT RESPONSE MECHANISM

The Incident Response Mechanism is designed to ensure that once a threat is detected, immediate and structured actions are taken to minimize its impact. After the system identifies suspicious activity through continuous log analysis, it not only generates an alert but also assigns a priority level such as low, medium, or high based on the severity and potential risk involved. This prioritization helps security teams focus first on critical threats that could cause significant damage. The SOC dashboard presents comprehensive details including the affected user account, system logs, attack pattern, frequency of occurrence, and historical context, allowing analysts to clearly understand the situation before taking action.

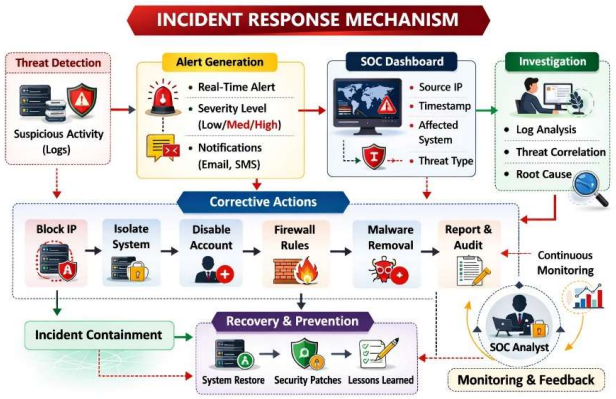

Fig 3: Incident Response Mechanism

8. PERFORMANCE EVALUATION AND SECURITY METRICS

Performance evaluation is an important aspect of the Intelligent SOC Dashboard because it determines how effectively the system detects and responds to security threats. Since the dashboard continuously processes large volumes of log data, it must maintain high speed, accuracy, and reliability. One of the primary performance indicators is Mean Time to Detect (MTTD), which measures how quickly the system identifies suspicious activity after it occurs. A lower MTTD means threats are detected early before causing serious damage. Another key metric is Mean Time to Respond (MTTR), which evaluates how quickly the system and security team can take corrective action once an alert is generated.

In addition to response time, the accuracy of alert generation is crucial. The system must minimize false positives, where normal activities are incorrectly flagged as threats, and false negatives, where real threats go undetected. High false positive rates can overwhelm analysts and reduce efficiency, while false negatives increase security risks. Log processing speed is another critical factor, as the system should handle thousands of logs per second without delay. Scalability testing ensures that the dashboard can support increasing log volumes as the organization grows. Reliability and uptime are also evaluated to confirm that the SOC system operates continuously without interruptions. By regularly analyzing these security metrics, organizations can fine-tune detection rules, optimize performance, and ensure that the SOC dashboard remains

efficient, accurate, and dependable in real-world cybersecurity environments.

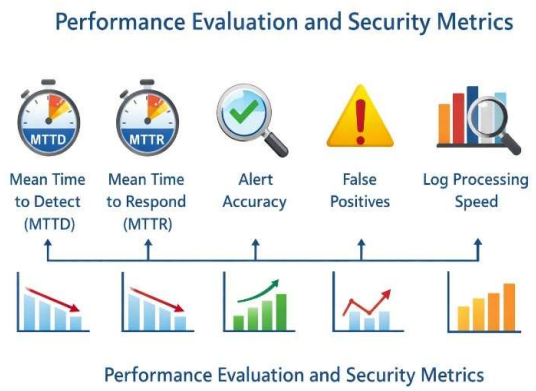

Fig 4: Performance Evaluation and Security Metrics

9. CONCLUSION

The increasing complexity of cyber threats demands intelligent and continuous security monitoring solutions. The Intelligent SOC Dashboard for Continuous Log Analysis and Incident Responses provides a centralized and automated framework for managing large volumes of security logs efficiently. By integrating real-time log analysis, centralized visualization, and structured incident response mechanisms, the proposed system enhances threat detection accuracy and reduces response time. The architecture ensures scalability, operational efficiency, and improved cybersecurity posture. Overall, the system serves as a practical and effective solution for modern organizations seeking to strengthen their Security Operations Center capabilities. Additionally, the system promotes proactive threat management through continuous monitoring and intelligent alert prioritization. It enhances security visibility while reducing manual workload for analysts. Overall, the proposed solution strengthens organizational resilience against evolving cyber threats.

10. REFERENCES

[1] R. Sommer and V. Paxson,"Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,"in *Proceedings of the IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.

[2] M. Roesch,"Snort: Lightweight Intrusion Detection for Networks,"in *Proceedings of the 13th USENIX Conference on System Administration (LISA)*, 1999, pp. 229–238.

[3] Elastic NV,"Elasticsearch: Real-Time Search and Analytics Engine,"Technical Documentation, 2020.

[4] National Institute of Standards and Technology (NIST), "Computer Security Incident Handling Guide," NIST Special Publication 800-61 Revision 2, 2018.

[5] MITRE Corporation,"MITRE ATT&CK®: A Knowledge Base for Adversary Tactics and Techniques,"2020.

[6] IBM Security,"Cost of a Data Breach Report," Annual Security Report, 2022.

[7] Cisco Systems,"Annual Cybersecurity Report," Cisco Security Research, 2021.

[8] Gartner Research,"Magic Quadrant for Security Information and Event Management,"Gartner Inc., 2021.