Grenze International Journal of Engineering and Technology, January Issue

Threat Tracker using SIEM

Shyam K[1], Shervin Bruce S[2] and Dr. Javid Ali L[3]
[1-2]Student, St. Joseph's Institute of Technology Chennai, India shyamsam1818@gmail.com
[3]Professor St. Joseph's Institute of Technology Chennai, India
Email: javidinaug77@gmail.com

***Abstract*— This paper gives an overview of the role played by SIEM systems in the detection of abnormal behaviors and potential threats within a broad scope of IT environments. While SIEM systems are very important for productive security monitoring, there is equally the tendency to expose sensitive information contained in system logs. In this work, we propose an enhanced SIEM solution integrated with such features as data masking, fine-grained access control, and customizable dash- boards. These enhancements range from protecting sensitive data while enhancing anomaly detection automation to strengthening an organization's security posture.**

***Key Words*—SIEM, Data Masking, Access control, anomaly detection, Security Orchestration, Automation, and Response (SOAR).**

I. INTRODUCTION

Security Information and Event Management systems have become cornerstones in modern cybersecurity-things that hold together the events from an organization's IT infrastructure and provide analysis. These systems aggregate logs that emanate from operating systems, applications, and network devices to make the process of detection of abnormal behaviors and probable threats easier. Despite this, two main challenges face most SIEM systems: the volume of log data generated is increasing and sensitive information is usually exposed within such logs.

Log files often contain sensitive information about system configurations, user credentials, and proprietary data. For that reason, logs themselves are often a target of access without authorization. Many conventional methods of log evaluation may unwarily expose information of this nature and increase risks for data breaches. What is needed here is an enhanced approach-one that will not only improve the detection of security threats but safeguard sensitive data.

This paper discusses some approaches to the challenges identified by demonstrating advanced capabilities in the SIEM system using data masking for sensitive information, fine- grained access control that limits viewing of specific log data by person, and customizable dashboards that facilitate additional analysis. Third, the advanced SIEM system allows for better filtering and sorting the data, giving security teams the ability to prioritize resources. A case study is provided that explains how these enhancements reduce the risk of data exposure and build on existing capabilities for identification and response to incidents.

Section II describes related work about SIEM systems and their improvements for managing increasing log data including sensitive data disclosure limitations. Section III emphasizes how usability is improved based on intuitive interfaces, customized dashboards, and an efficient filtering mechanism. Section IV outlines challenges regarding massive log data and sensitive data disclosure and presents a secure and scalable solution.

Grenze ID: 01.GIJET.11.1.5

Section V describes, mathematically, statistical models and methods to conduct anomaly detection and pattern identification in the logs. Section VI describes how the data flows in the system: from collection to aggregation, detection, and response. Section VII and VIII reflect the result analysis and future enhancement.
The above sections concentrate on improving SIEM systems by addressing key challenges like handling large-scale log data and mitigating risks of sensitive data exposure.
They propose enhanced usability, scalable log analysis methods, and more secure workflows. The focus is on developing a robust SIEM approach that efficiently detects and responds to threats while offering flexibility for future improvements.

II. Related Works

A. Log Analysis and SIEM Integration for Enhanced System

Authors in paper[1],[4],[6],[9],[10] explored different ap- proaches toward system understanding and log analysis. The approaches used for understanding the system execution paths were log line analysis, state machine modeling, and work- flow analysis.
Again, purpose-driven logging was highlighted where logs are strategized with a focus on specific use cases and integrated into the SIEM systems to drive detection and response. Moreover, these research works underlined the necessity of data aggregation and normalization-that is, logs gathered from different sources needed to be brought together into a uniform format for deep analysis.
It also discussed how advanced SIEM system features are integrated with SOAR, threat intelligence feeds, among others, thus indicating how much SIEM technologies have evolved to fight current security threats.

B. Real-Time Threat Detection and Monitoring

Among the papers reviewed, authors of [5], [7] have focused on the evolution and advancement of SIEM systems. Real time monitoring and threat detection were emphasized. Much emphasis has been laid on log normalization and integration from different sources into an integrated system for accurate parsing and effective analysis.
Further, some of the discussion has shown that SIEM has been integrated with more advanced capabilities like SOAR: Security Orchestration, Automation, and Response, and with the inclusion of threat intelligence feeds to enhance further analysis.
A transition from traditional log-centric SIEM systems into the second generation of more sophisticated systems, integrated with behavioral and contextual analysis, was discussed. It thus shows further development in SIEM technology to help modern cybersecurity demands.

C. Anomaly Detection and Event Classification

Paper [2],[3] proposes an anomaly detection and event classification methodology using a Composite Sliding Win- dow. It involved identifying and filtering fluctuating events, thereby analyzing the first-order differential signal of the detected events. Such a method gave a new dimension to event classification in the log analysis domain.

D. Mitigating Brute Force Attacks with SIEM

The authors, in paper [8], have introduced the open-source SIEM platform Wazuh in a practical way with all its inte- grations of Active Response and Telegram notifications.
This work, therefore, has given a problem of brute force mitigation using Security Life Cycle Methodology and has shown that this methodology is quite effective for security enhancement and continuous monitoring of the system.

III. Ease of Use

The improved SIEM design will greatly enhance the ease at which users of all types can make use of this technology.

A. Intuitive Interface

It is designed in a way so that from an intuitive interface, one can view access events easily, set alerts, and do log reviews in real time.
Graphs and tables provide light summations of deep information, letting security teams grasp knowledge sans deep training in log analysis.

B. Custom Dashboards

Users can create custom dashboards that include the most helpful metrics and alerts for their needs so that this information can be obtained more easily, allowing them to act faster in response to incidents.

C. Automated Anomaly Detection

- Automation reduces the need for manual monitoring of correlated data points for login attempts and network
- Simplified maintenance and checks translate to easier routine tasks-such as managing temporary files and per- forming system checks-reducing the operational burden for IT and security teams.

D. Aggregated Analysis

Enhancements such as data masking, customized dash- boards, and automated anomaly detection are making SIEM even more usable and accessible. Attention to intuitive design, interface, and clear visualization of data allowed for threat detection and response without overwhelming the users. By overcoming data overload and exposure of sensitive information, this improved approach of SIEM provides a more effective user-oriented solution that strengthens both security posture and operational efficiency.

IV. Problem Statement

The nature of the work performed by a SIEM (Security Information and Event Management) system, which is used to classify collected log events, is one of the most important tasks in cyber security. It is crucial for detecting and responding to security threats. However, the classification and analysis of logs are often done manually, requiring significant domain knowledge and an understanding of various vulnerabilities, attack surfaces, and threat behaviors. This paper aims to achieve the following objectives:

- Study log events, identify anomalies in their activities, and analyze their associated attack surfaces using SIEM techniques.
- Develop an approach to classify groups of events, analyze suspicious activities, and identify potential threats, enabling the appropriate response actions.
- The findings of this research will be valuable to developers, administrators, SOC (Security Operations Center) analysts, and pen testers working with SIEM systems, as it will help them make informed decisions regarding log analysis and security threat management.

V. Log Analysis - Mathematical Methodology

A. Statistical Anomaly Detection

A common equation used in log analysis for anomaly detection is based on the Z-score, which measures how many standard deviations a data point is from the mean:

$$Z = \frac{X - \mu}{\sigma} \quad (1)$$

Where:

- Z is the Z-score
- X is the observed value
- μ (mu) is the mean of the log values
- σ (sigma) is the standard deviation of the log values

B. Sigma Notation for Aggregated Log Analysis

If aggregating counts of specific log events over time, the summation equation is:

$$\sum_{i=1}^{n} X_i \quad (2)$$

Where:

- Xi represents the count of a particular log event (e.g., failed login attempts) in each time period i
- n is the total number of time periods being analyzed

C. Logarithmic Analysis for Frequency Counts

In some log analyses, logs are analyzed on a logarithmic scale to handle large ranges of data:

$$Y = \log (X + 1) \quad (3)$$

Where:

- X is the frequency count of log events
- Y is the transformed value on a logarithmic scale, which can make patterns more discernible when dealing with highly variable data

Event Category	Vulnerability Category	Description
Network Intrusion	Injection Attacks	Malicious code injected through user input can lead to unauthorized network access
Compromise of Accounts	Authentication Violation	Weak authentication mechanisms can allow attackers to gain unauthorized access to accounts.
Malware Detection	Insufficient Security Settings	Inadequate security configurations on servers can allow malware to execute.
Violation of Security Policies	Dangerous Additional Components	Unpatched or vulnerable third-party components can expose sensitive data
Detection of Data Leaks	Leakage of Sensitive Data	Improper handling of user-uploaded content can lead to data breaches
Vulnerability Monitoring	Dangerous Additional Components	Third-party plugins or libraries with known vulnerabilities can compromise the application's security

Fig. 1. Relation between event category and their vulnerabilities

VI. WORK FLOW

A. Getting the Data Together and Ready to Use

- Data Collection: Begin by aggregating data from all relevant sources, including security logs, network activity reports, antivirus scans, and user activity logs, which detail actions taken within the system.
- Emphasizing Access Logs: Focus specifically on access- related data, such as login attempts, permission changes,

B. Monitoring and Identifying Issues

- Network Monitoring: Continuously monitor network traffic to detect unusual patterns, such as unauthorized connections or signs of data exfiltration.
- Threat Detection: Correlate findings from antivirus scans with other data points, such as spikes in failed login attempts, to identify potential threats.
- Authorization Checks: Regularly monitor user logins, file access, and permission changes. Look for anomalies correlate them with other suspicious activities.

C. In-Depth Threat Analysis

- Pattern Recognition: Apply rule-based systems to detect patterns indicative of unauthorized access or misuse of permissions.
- Detailed Investigation: Investigate anomalies that could suggest attempts to elevate permissions or access sensitive data. Correlate these findings with other data sources, such as network activity or antivirus alerts, to gain a comprehensive understanding of potential threats.

D. User Interface and Reporting

- User-Friendly Interface: Develop an intuitive interface for monitoring access events, configuring alerts, and reviewing logs in real time.
- Clear Data Visualization: Use simple, clear charts and tables to present key trends, such as failed logins or permission changes, making it easier for users to interpret the data.

E. Reporting and Alerts

- Comprehensive Reporting: Generate reports summa- rizing key activities, identifying what's functioning correctly, what isn't, and highlighting any unusual access attempts.
- Critical Alerts: Implement alerts for significant events, such as a surge in failed logins, unauthorized access attempts, or substantial permission changes, ensuring timely responses to potential threats.

F. Maintenance and Routine Checks

- Managing Temporary Files: Regularly monitor and clean up temporary data to prevent system vi clutter.
- Routine System Checks: Conduct regular checks to ensure that all monitoring tools and logging systems are functioning correctly, maintaining the integrity of access tracking and threat detection.

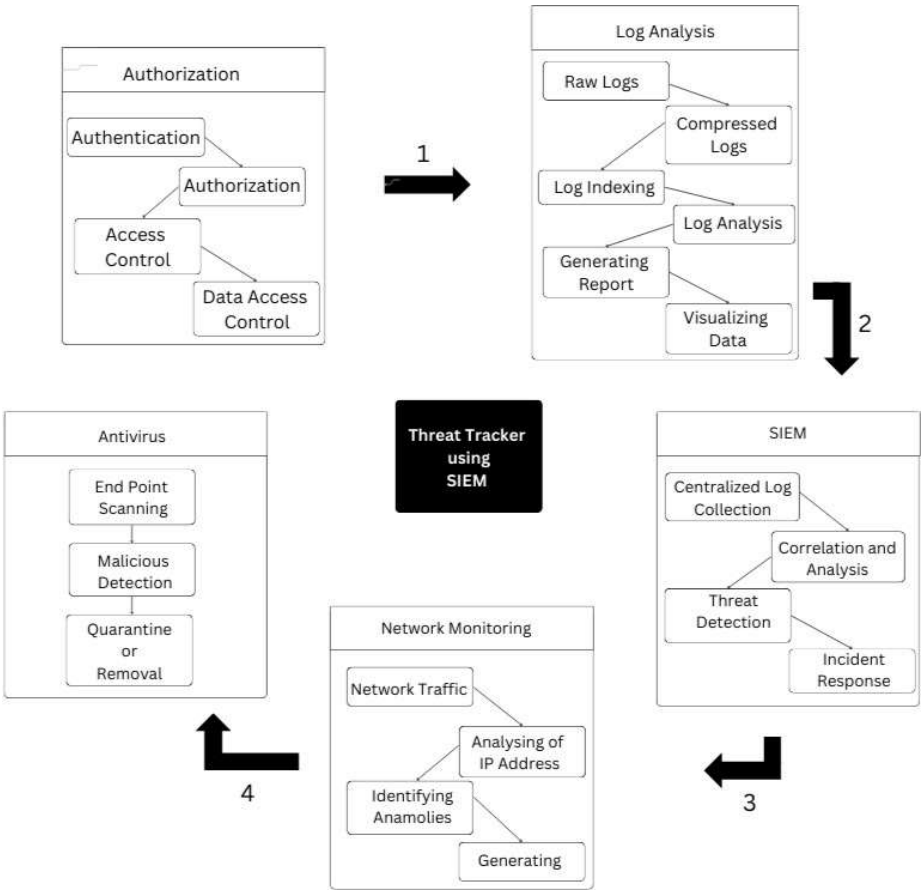

Fig. 2. Architecture Diagram

VII. Security Event Insights

The Security Event Insights Dashboard presents an overview of key security metrics important for monitoring and decision-making. As shown in Fig. 3, it visually displays data on the severity level of events—high, medium, and low—in a pie chart format, allowing the consumer at a glance to determine the most critical events that require immediate attention. The Events Over Time line chart depicts trends in the number of events occurring and helps teams make judgments about whether their security environment is static or in flux over some period of time.

The Top 10 Detections bar chart shows the frequency of certain detections, including Detection 1 and 2. This enables security teams to understand where attention should be focused by repeated threats. The event type bar graph categorizes incidents among a number of groups, such as login attempts, network traffic, and file access, which reflects the nature of the monitored activities. Another similar example can be seen in this Distribution of

Sources of Events pie chart, which shows the origins of security incidents, split fifty-fifty between two IP addresses and one user.

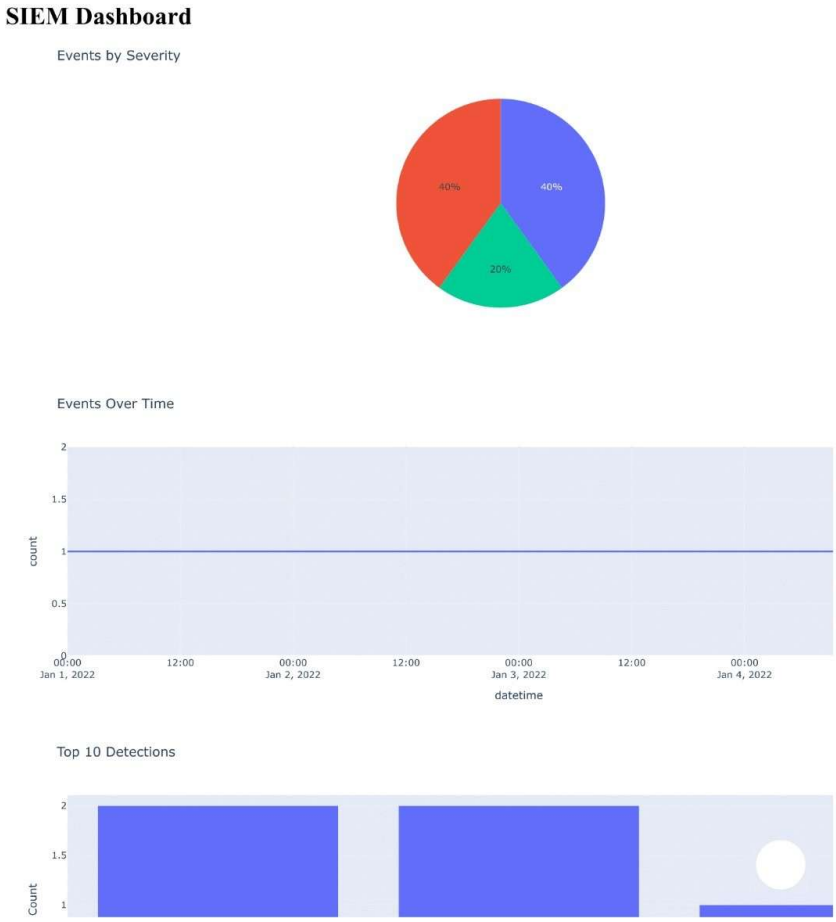

Fig. 3. Dashboard Insights

VIII. FUTURE ENHANCEMENT

A. More Complete Threat Intelligence Integration

The future of the SIEM system is to be integrated with other threat intelligence feeds that give real-time data about the latest cyber threats and vulnerabilities.

B. Improved Scalability

Due to the fact that the volume of log data is still growing, the scalability issue of the SIEM system needs much attention. Further enhancements might be directed at tuning the system for handling large volumes of data in order not to lose speed or accuracy.

C. Advanced Automation

Extend this further to more sophisticated incidence re- sponse measures that reduce security incident response times. Automation could involve incident response related to the isolation of affected systems, blocking suspicious IP addresses, or alerting relevant stakeholders based on predefined rules.

D. User Experience Refinements

Subsequent releases could fold in user feedback in order to iteratively refine the usability of the interface of the SIEM system, making it increasingly intuitive and personalized. This would include more flexible configurations of the dashboard and the ability to personalize reports and alerts to particular user roles within the organization.

E. Further Security Tool Integration

More integration with other security tools, like firewalls, intrusion detection/prevention systems, and endpoint security solutions, would continue to build out a more holistic ecosystem where the SIEM could, with future revisions, be more representative of a comprehensive approach to threat management.

IX. Conclusion

This paper has stressed the great significance of SIEM systems for enhancing cybersecurity by providing mighty monitoring, anomaly detection, and threat analysis. The pro- posed extensions meet some key challenges of traditional SIEM systems related to data masking, fine-grained access control, and customizable dashboards, which have been subject to overload and risk of leakage of sensitive information. All these improvements go on to enhance the effectiveness of threat detection and response, in turn protecting sensitive data and reducing data breaches. Scalability, advanced automation, and refinements in user experience will be of great help to the enhanced SIEM system in meeting modern cybersecurity landscape needs. These will, in turn, contribute to ensuring that organizations continue to maintain their security posture, while making it all accessible and manageable to users of all levels.

References

[1] S. Locke, H. Li, and T.-H. (P.) Chen, "LogAssist: Assisting Log Analysis Through Log Summarization," IEEE Trans. Software Eng., vol. 48, no. 9, pp. 2345–2361, Sep. 2023.

[2] M. Vielberth and G. Pernul, "A Security Information and Event Management Pattern," in Proc. SLPLoP'18, Valpara´ıso, Chile, Nov. 20-23, 2018, pp. 1–10.

[3] Z. Wang, Y. Wu, Y. Zhao, J. Wang, H. Liu, and Y. Wang, "A Composite- Window-Based Load Event Detection Method in Non-Intrusive Load Monitoring," in Proc. 2023 IEEE 7th Conf. Energy Internet and Energy System Integration, 2023.

[4] G. Hughes, "A Framework for SIEM Implementation," ISACA J., vol. 3, pp. 45–50, 2023.

[5] R. K. Sharma, D. K. Singh, A. Kumar, and A. P. Burnwal, "SecureLog: Open-Source Security Information and Event Management (SIEM) Solution for Enhanced Threat Detection and Incident Response," Int. J. Students' Res. Technol. Manage., vol. 11, no. 3, pp. 20–29, 2023.

[6] M. Sheeraz, M. A. Paracha, M. U. Haque, M. H. Durad Syed, M. M. Mohsin, S. S. Band, and A. Mosavi, "Effective Security Monitoring Using Efficient SIEM Architecture," Hum.-Centric Comput. Inf. Sci., vol. 13, no. 1, pp. 1–15, Apr. 2023.

[7] A. Yushko, R. Shevchuk, K. Łopacin´ski, M. Leszczynska, O. Yashchyk, and T. Yurchyshyn, "Shielding Web Application against Cyber-Attacks using SIEM," in Proc. 2023 13th Int. Conf. Advanced Computer Information Technologies (ACIT), IEEE, 2023.

[8] F. I. Farrel, I. Mardianto, and A. S. Qamar, "Implementation of Se- curity Information and Event Management (SIEM) Wazuh with Active Response and Telegram Notification for Mitigating Brute Force Attacks on the GT-I2TI Usakti Information System," Intelmatics, vol. 4, no. 1, pp. 1–7, Jan.–Jun. 2024.

[9] B. Debnath, M. Solaimani, M. A. Gulzar, N. Arora, C. Lumezanu, J. Xu, B. Zong, H. Zhang, G. Jiang, and L. Khan, "LogLens: A Real-time Log Analysis System," in Proc. 2018 IEEE 38th Int. Conf. Distributed Computing Systems, 2018.

[10] J. Caˆndido, M. Aniche, and A. van Deursen, "Log-based Software Monitoring: A Systematic Mapping Study," Published May 6, 2021.