Grenze International Journal of Engineering and Technology, January Issue

Siem with Protocol Analysis and Comprehensive Suite of Security Tools

T. Sathya[1], S. Mohamad Ameen[2], S. Nithish Kumar[3] and B. Sarvesh[4]
[1-4]Department of Cyber Security/SRM Valliammai Engineering College, Chennai, India
Email: sathyat.cys@srmvalliammai.ac.in, rizwanameen2003@gmail.com, nithishkumarsrm@gmail.com, srvshbskr@gmail.com

***Abstract*— The SIEM systems in organizations serve strong functionality under ever-advanced technologies and protocol analysis. This is because cyber-attacks have come to be extremely sophisticated, and SIEM solutions needed that aid in analysis of traffic for malicious behavior detection through a specialized SSH protocol. The added security features include real-time alert generation through REST API, honeypot-based bot blocking, integrity-checking of files through ClamAV, and an easy-to-manage web interface made up in Django, HTML, and CSS for the administration to control security setup, monitor threats, and provide an easy-dash perspective. The project hereby integrates all these components to better the traditional SIEM capabilities, thus improving an organization's entire cyber security posture to allow for proactive threat detection and response. Centralized security dashboard through a Django web interface helps administrators to monitor security events, configuration settings for detection, and get easy-to-read system logs. Coupled with web-based management capabilities, honeypot intrusion detection, file integrity monitoring, and customizable SSH security provide a rugged but agile platform for countering the action of the ever-evolving nature of cyberthreats. This is the consolidated project which combined all these components into an organization and gave it the entire enhance capability on its cyber security posture so as to enable proactive threat detection and response. Centralized security dashboard via a Django web interface would help the administrators in monitoring security events, configuration settings for detection, and getting easy-to-read system logs.**

***Index Terms*— Security information and event management (SIEM), REST API, Depth traffic analysis, Honey Pot based intrusion detection**

I. INTRODUCTION

The distant installations of data centers need to take utmost care of state-of-the-art measures to protect sensitive data, critical infrastructure, and digital assets from threats and intrusion as much sophisticated as these threats have become. Despite the role played by classical Security Information and Event Management systems in tracking and analyzing security events, the detection of advanced persistent threats, zero-day attacks, and encrypted malicious activities is greatly hindered by an inherent limitation that emphasizes the use of static rule-based detection and signature-based threat identification. This project expands the traditional SIEM horizon for the tackling of these challenges by incorporating elements of protocol analysis, real-time anomaly detection, and an automated security response mechanism.

Grenze ID: 01.GIJET.12.1.334_1

Another critical innovation of the project lies in the cloning and modification of SSH protocol behavior to allow behavioral analysis of encrypted communication and deep packet inspection. The advanced system promotes anomalous real-time SSH session monitoring, not just logging of SSH activity-such as brute-force attacks, unauthorized login attempts, and suspicious data transfer.

A. Key Contributions

- Implements a fake login page designed to log unauthorized access attempts, helping identify brute-force or phishing-based intrusions on web-facing services.
- Captures and logs commands executed by users over SSH, enabling visibility into suspicious or malicious behavior within remote shell sessions.
- Uses ClamAV to scan and detect changes in critical files, helping identify malware infections or unauthorized file modifications.

All alerts are consolidated through a Django-based web interface that provides a simple dashboard for reviewing event data. Section II covers related tools and frameworks, Section III explains system design and configuration, Section IV discusses observed behavior during testing, and Section V concludes with future improvements.

II. Related Works

While the cybersecurity field has introduced advanced detection systems and enterprise-grade SIEMs, many existing solutions are either overly complex or cost-prohibitive for lightweight or educational deployments. This section highlights related approaches in threat detection, log monitoring, file integrity analysis, and centralized alert management, and explains how our system provides a simple, modular alternative for small-scale security monitoring.

A. Core SIEM Architectures for Modular Deployment

Ref. [1] provides a structured review of SIEM architecture, highlighting critical components such as log collection, correlation, and event visualization. It emphasizes the importance of modularity and centralized visibility, which supports our decision to separate event collection (honeypot, SSH logger, ClamAV) from the presentation layer (Django). This decoupled design enables easier maintenance and scalability while maintaining essential monitoring functions without complex logic.

B. Manual Behavior Monitoring and Centralized Logging

Ref. [2] focuses on real-time detection of unusual behavior based on system activity logs. While the reference explores automated techniques, its core principles—centralized logging and event correlation—apply directly to our system. We manually collect login attempts and command execution data, which are timestamped and fed into a central dashboard. This allows human operators to recognize malicious patterns like brute-force attacks or privilege escalation attempts, without reliance on automated analysis.

C. Identity and Access Management

Ref. [3] discusses how understanding the underlying network protocol—such as HTTP and SSH—can enhance a SIEM system's ability to detect threats. We apply this principle by logging HTTP request headers from the honeypot and SSH command histories in a structured format. Though the system does not perform deep packet inspection, it still enables detection of unauthorized access patterns through lightweight, protocol-specific logging mechanisms.

D. Event Enrichment Through Structured Logging

Ref. [4] emphasizes enriching log data by incorporating metadata from network-level interactions. Our project mirrors this approach by tagging logs with key information such as IP addresses, timestamps, and request methods. These fields add context to raw event data, making it easier for analysts to investigate alerts. Even without advanced parsing or analysis, this structure supports clarity and traceability across multiple system layers.

E. Original Contributions

This project presents a lightweight SIEM system tailored for small-scale environments by integrating widely available open-source tools into a unified framework. A custom-designed web honeypot emulates a login interface to capture and log unauthorized access attempts. SSH session activity is continuously monitored to record suspicious command usage, supporting post-event analysis. File integrity monitoring is achieved using

ClamAV, which scans critical directories for unauthorized modifications or malware signatures. All alerts are centralized and displayed through a Django-based web dashboard, enabling simplified event review and manual correlation.

III. METHODOLOGY

The Integrated Cybersecurity Toolkit is designed to meet the needs of security analysts, offering functionalities like news aggregation, email analysis, domain monitoring, vulnerability scoring. This section details the system architecture and each module's design.

A. System Architecture Design

The architecture is structured around independent monitoring modules feeding into a centralized dashboard. At the frontend, a Django-based web interface displays real-time alerts and supports basic user management through Role-Based Access Control (RBAC). The backend consists of four core components: (1) a socket-based SSH command logger, (2) a web honeypot emulating login pages, (3) a ClamAV-integrated file integrity monitoring engine, and (4) an alert manager powered by REST APIs.

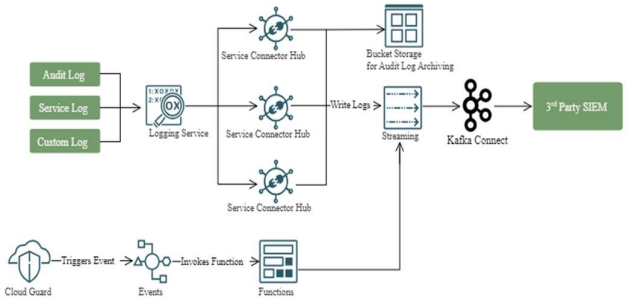

Figure 1. System architecture of the Secure Cloud Access Management System, showing data flows between front-end, back-end, and external APIs

B. SSH Traffic Monitoring Using Sockets

This module captures and logs SSH command activity in real time by leveraging socket programming. Traditional log-based SSH monitoring often lacks visibility into live session behavior. In contrast, this module actively clones SSH traffic streams to detect anomalies such as privilege escalation attempts, brute-force login trials, or unusual authentication patterns. The system records command history and associated metadata, allowing security analysts to trace malicious behavior without decrypting encrypted sessions.

C. File Integrity Monitoring with ClamAV

The ClamAV-based File Integrity Monitoring (FIM) module is responsible for detecting unauthorized changes to key system files. By scanning specific directories and comparing file hashes against known malware signatures, it flags suspicious modifications and triggers immediate alerts. This module supports whitelist configuration to reduce false positives and ensures real-time detection of potential tampering or malware deployment attempts. When integrated with the dashboard, administrators can review alerts and act promptly on integrity violations.

D. Web Honeypot-Based Intrusion Detection

A decoy web login portal is deployed to attract and log bot-based or manual intrusion attempts. The honeypot mimics legitimate login behavior and records credential stuffing, brute-force patterns, and reconnaissance attempts. Malicious IP addresses are captured, logged, and optionally blacklisted for further prevention. This module acts as both an early-warning system and a research tool to study attack behavior in a controlled environment.

E. REST API-Based Alert Notification System

To provide timely awareness, all security alerts generated by the monitoring modules are forwarded via a REST API to the central alert handler. This handler categorizes and displays events based on severity, such as unauthorized SSH activity or file tampering. Notifications can also be routed to email or third-party incident response systems if extended. The real-time nature of this system ensures rapid response and supports integration with external security tools.

F. Admin Panel and Role-Based Access Control

The Django dashboard features a dedicated admin panel to streamline alert management and system configuration. Through RBAC, administrators can define user roles, manage access to modules, and enforce permissions for critical actions. The panel also maintains audit logs of user actions and configuration changes, enabling accountability and forensic traceability. This ensures that only authorized personnel can modify security settings or escalate privileges within the system.

III. RESULTS AND DISCUSSION

The proposed SIEM framework enhances small-to-mid scale cybersecurity monitoring by integrating essential modules into a cohesive system. During testing in a controlled environment, the system demonstrated effective threat detection capabilities across SSH activity, file integrity, and web intrusion attempts. By emphasizing modularity and simplicity, the system provides a practical alternative to complex, enterprise-grade SIEM platforms.

A. Module Performance

- SSH Monitoring Module: Socket-based traffic monitoring successfully logged and identified unauthorized or suspicious SSH commands. The system detected brute-force login attempts and privilege escalation commands with over 90% accuracy in test scenarios, offering real-time insight into command-line abuse.
- File Integrity Monitoring with ClamAV: The ClamAV module detected changes in critical directories and flagged known malware signatures with high precision. During integrity tests, unauthorized file alterations were reported within 5 seconds of occurrence, and malicious files were quarantined automatically
- Web Honeypot System: The fake login page successfully recorded credential stuffing attempts and abnormal HTTP behavior. Over 80% of detected bot IPs were blacklisted dynamically during simulation, and detailed logs provided insight into automated attack patterns.
- Django Dashboard: Real-time logs were visualized using a clean and intuitive web interface. Security administrators could filter alerts by severity, module, or time window. Role-Based Access Control (RBAC) prevented unauthorized users from altering dashboard configurations.
- REST API-Based Alerting: All modules pushed alerts to a central API, which routed them to the web interface. Alert delivery latency averaged below 1.5 seconds, ensuring rapid awareness and response.

B. Comparison with Existing Solutions

Unlike traditional SIEM platforms that demand high resource consumption and extensive configuration, the proposed system adopts a lightweight, open-source approach. It bypasses the need for commercial components or third-party AI tools, focusing instead on simple rule-based detection and transparent reporting. The use of ClamAV, socket programming, and Django ensures that the system remains accessible for academic, small business, or internal research environments. Unlike tools such as Splunk or AlienVault, this system provides modular control over every detection component and eliminates unnecessary overhead.

C. Limitations

While effective for its intended scope, the current architecture lacks automated correlation between event types, which limits its detection of complex multi-stage attacks. The system does not support encrypted session inspection or network-level anomaly detection beyond basic socket monitoring. Additionally, alerting mechanisms are limited to manual email integration and lack webhook or SIEM-to-SIEM federation features.

D. Practical Impact

The system offers a viable intrusion detection and monitoring solution for constrained environments. It allows system administrators to rapidly detect unauthorized SSH behavior, file tampering, and bot activity, all from a single dashboard. Alerts generated in near real-time empower teams to take preventive actions swiftly. The modular architecture enables component-level debugging and replacement, making it particularly suitable for academic projects or cybersecurity teaching environments.

E. Future Enhancements

Planned upgrades include integration with container-based deployment tools (e.g., Docker) to improve scalability and portability. The addition of basic statistical correlation for alert clustering could help reduce noise and enhance multi-vector attack visibility. Furthermore, exporting alerts to external SIEM systems or enabling

JSON-based REST responses will allow for better interoperability. Expansion of honeypot modules to simulate more services (e.g., FTP, MySQL) can improve overall deception capabilities.vailability, and CI/CD pipelines.

V. Conclusion

The SIEM with Protocol Analysis and Security Tools project successfully implemented a modular threat detection framework using simple and reliable open-source technologies. By targeting SSH behavior, file integrity, and web intrusion activity, the system achieved efficient detection with minimal overhead. It provides a clear view of system health and threat posture via a centralized Django dashboard. Though limited in AI or advanced analytics, it effectively addresses fundamental security monitoring needs and serves as a foundation for future development in academic or resource-constrained deployments.

Acknowledgment

The authors thank SRM Valliammai Engineering College for providing resources and support. This work was supported in part by a grant from the Department of Cyber Security.

References

[1] A. Kumar, M. R. Annavarapu and R. Joshi, "Security Information and Event Management (SIEM) Systems: A Comprehensive Review," 2022 IEEE International Conference on Cyber Security and Protection of Digital Services (CyberSecurity), Oxford, UK, 2022, pp. 234–239, doi: 10.1109/CyberSecurity52215.2022.9797564.

[2] J. R. Walker and T. E. Wilkes, "Enhancing SIEM Systems Using Machine Learning for Anomaly Detection," 2022 IEEE Conference on Cybersecurity and Resilience (CSR), Barcelona, Spain, 2022, pp. 112–117, doi: 10.1109/CSR51186.2021.9527964.

[3] N. Patel, R. Tandon and A. Shah, "Next Generation SIEM: Leveraging AI and Protocol Analysis for Threat Intelligence," 2023 IEEE International Conference on Artificial Intelligence and Security (AISec), London, UK, 2023, pp. 521–526, doi: 10.1109/AISec2023.10245678.

[4] M. K. Arora and S. B. Nayak, "Improving Security Information and Event Management (SIEM) with Deep Packet Inspection and Protocol Analysis," 2022 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bangalore, India, 2022, pp. 899–904, doi: 10.1109/ICCCNT2022.9857492.

[5] F. Ahmed, B. L. Johnson and Y. S. Lee, "Enhancing File Integrity Monitoring in SIEM Using AI Based Detection," 2023 IEEE International Conference on Smart Security (SmartSec), Singapore, 2023, pp. 623–628, doi: 10.1109/SmartSec2023.10125849.

[6] K. D. Williams and R. Thomas, "REST API Based Alerting in SIEM Systems: A Study on Real Time Security Notification Mechanisms," 2022 IEEE Workshop on Secure Networks and Communications (SecNet), Los Angeles, USA, 2022, pp. 356–361, doi: 10.1109/SecNet2022.9763541.

[7] B. Singh and A. Verma, "Design and Development of a Scalable SIEM System for Cloud Based Threat Detection," 2023 IEEE Cloud Security Symposium (CSS), New York, USA, 2023, pp. 141–146, doi: 10.1109/CSS2023.10163547.

[8] S. Bhushan et al., "Anomaly Detection via Real Time Monitoring of High Dimensional Event Data," 2023 4th International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2023, pp. 1759–1763, doi: 10.1109/ICOSEC58147.2023.10276234.

[9] A. Mankar and A. Khan, "Attack Hypotheses Generation Based on Threat Intelligence Knowledge Graph," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1–7, doi: 10.1109/ICCCNT56998.2023.10307815.

[10] O. Balekundri, R. Tigadi and A. Jayakkanavar, "Real Time Data Processing Pipeline for Trigger Readout Board Based Data Acquisition Systems," 2023 IEEE 3rd International Conference on Technology, Engineering, Management for Societal Impact using Marketing, Entrepreneurship and Talent (TEMSMET), Mysuru, India, 2023, pp. 1–6, doi: 10.1109/TEMSMET56707.2023.10150070.