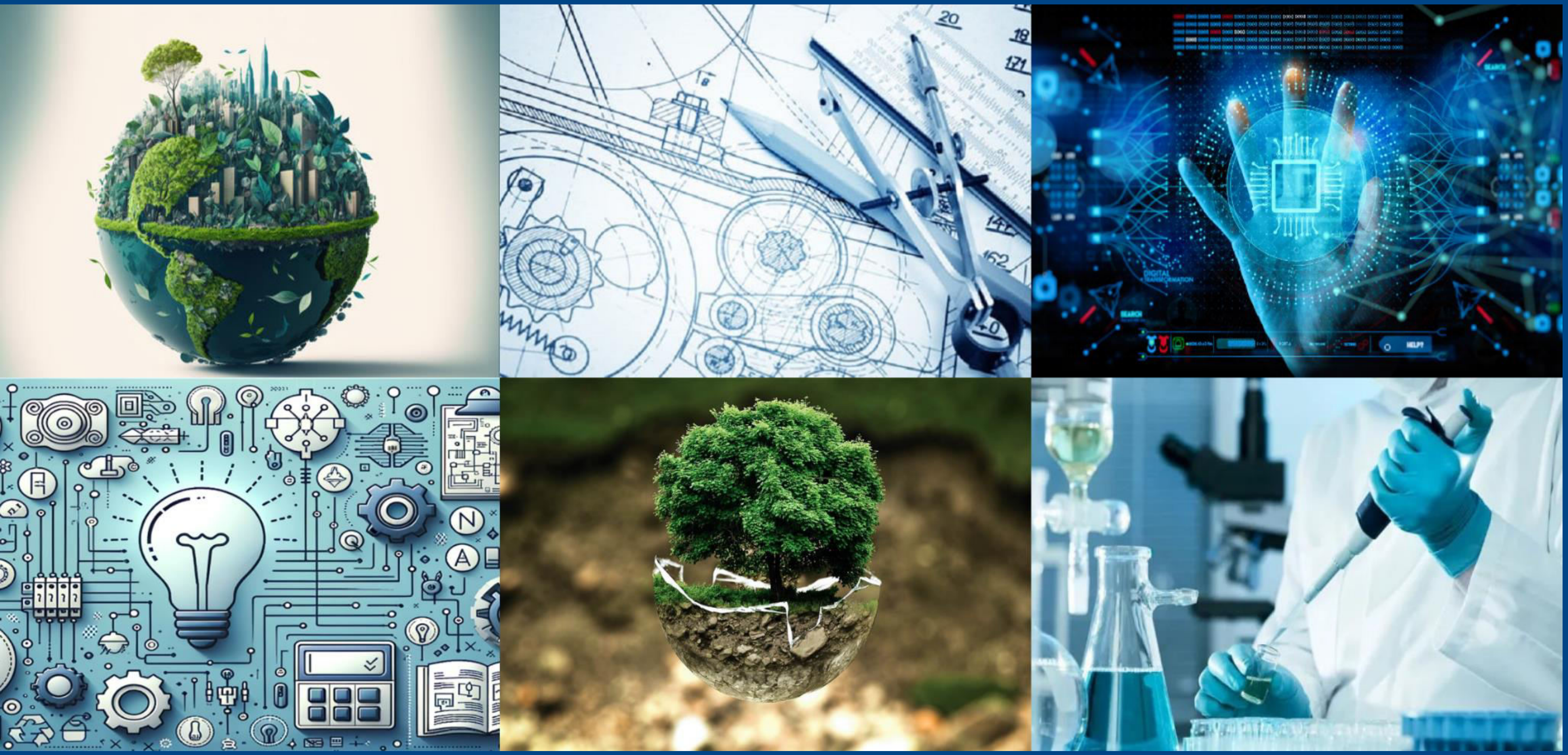
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 3, March 2025

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A Low Cost SIEM Implementation in Ubuntu

Mrs. Gowridurga A[1], Rohit S V[2], Sandeep Kaushik R[3], Sreejay V[4]

Faculty of Department of Computer Science and Business System, R.M.D.Engineering College, Chennai, India[1]

Student of Department of Computer Science and Business System, R.M.D.Engineering College, Chennai, India[2]

Student of Department of Computer Science and Business System, R.M.D.Engineering College, Chennai, India [3]

Student of Department of Computer Science and Business System, R.M.D.Engineering College, Chennai, India[4]

ABSTRACT: Security Information and Event Management (SIEM) is a critical component of modern cybersecurity strategies, providing real-time analysis of security alerts generated by hardware and applications. This paper explores the implementation of a SIEM system on an Ubuntu-based environment, highlighting key components, configuration steps, and best practices.

We discuss the selection of open-source SIEM solutions such as Elastic Stack (ELK), Wazuh, and Security Onion, which provide log collection, correlation, and anomaly detection capabilities. The implementation process covers installation, log forwarding using agents like Filebeat or OSSEC, event correlation, dashboard setup, and alerting mechanisms. Additionally, we address system performance optimization, log storage management, and security hardening techniques to ensure efficient operation.Finally, we examine real-world use cases, including threat hunting, compliance monitoring, and incident response, demonstrating how an Ubuntu-based SIEM can enhance an organization's cybersecurity posture. The findings suggest that with proper configuration and tuning, an Ubuntu-based SIEM can provide cost-effective and robust security monitoring for enterprises and small businesses alike

I. INTRODUCTION

Security Data and Occasion Administration (SIEM) has gotten to be an basic component of present day cybersecurity foundation. As organizations confront progressively modern dangers, the usage of vigorous checking and examination devices on dependable stages is basic. This paper investigates the sending, setup, and optimization of SIEM arrangements on Ubuntu, one of the foremost broadly utilized Linux conveyances in undertaking situations. Ubuntu gives an perfect establishment for SIEM execution due to its soundness, security-focused plan, and broad community bolster. The open-source nature of both Ubuntu and numerous driving SIEM arrangements makes a cost-effective and customizable security checking system appropriate for organizations of all sizes. The SIEM market has evolved significantly in recent years, with a shift toward cloud-native architectures, advanced analytics, and automated response capabilities. Open-source SIEM solutions have gained traction alongside commercial offerings, providing viable alternatives for organizations with budget constraints or specialized requirements.This paper will look at the down to earth viewpoints of SIEM sending on Ubuntu frameworks, counting engineering contemplations, integration with existing security instruments, execution optimization, and best hones for risk detection and incident reaction. We are going moreover address challenges particular to Ubuntu situations and give direction for security experts looking for to improve their organization's security pose through successful SIEM usage.

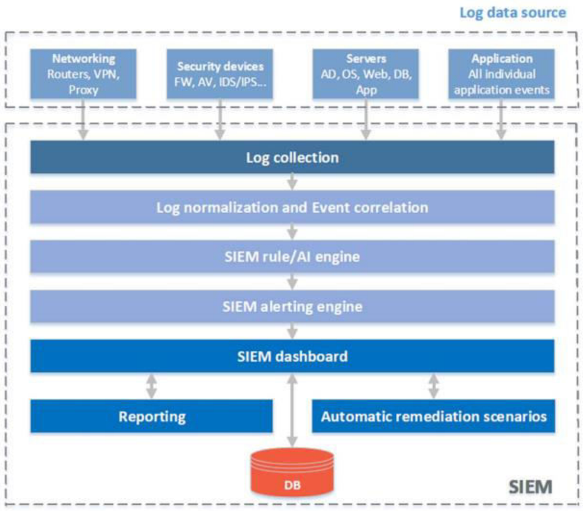

Log data source
Networking Routers, VPN, Proxy
Security devices FW, AV, IDS/IPS...
Servers AD, OS, Web, DB, App
Application All individual application events
Log collection
Log normalization and Event correlation
SIEM rule/AI engine
SIEM alerting engine
SIEM dashboard
Reporting
Automatic remediation scenarios
DB
SIEM

Figure 1Process Flow

II. LITERATURE REVIEW

A critical assessment of the work has been done so far on Cloud Forensics to show how the current study related to what has already been done. Numerous companies are now a days migrating to cloud due to greater economic issues. But for small and medium sized companies the security of information is the primary concern. For these companies the best alternative is to use managed service which is also known as outsourced service in which they are provided with the full package of service including antivirus software to security consulting. And the alternative model that provides such outsourced security is known as Security as a service (SECaaS). Scientists and researchers together presented their latest ideas and findings on what the real world scenario is and what all efforts are made but it was found that despite of being so much research work in the field of cloud forensic there is only a fraction part of the total work that has contributed for the wealth of the society. However cloud came into existence in the mid of 90's yet it is not taken up by everyone fully. There have been lots of works before in this field and variety of methods for the forensic analysis of cloud yet there is a huge room for improvement that needs to be carried forward into the research.

[1] Podzins (2019) – "Why SIEM is Irreplaceable in a Secure IT Environment"
This paper explores the critical role of Security Information and Event Management (SIEM) in cybersecurity. It discusses SIEM's ability to analyze logs from various security solutions, providing a centralized system that can detect cyber threats, including zero-day attacks. The study highlights the advantages of SIEM, such as real-time threat detection and automated remediation, while also addressing its challenges, such as high costs and complex implementation. The paper emphasizes that SIEM solutions must be optimized and continuously improved to be effective, especially when integrated with a Security Operations Center (SOC).

[2]Anastasov & Davcev (2014) – "SIEM Implementation for Global and Distributed Environments"
This paper focuses on the challenges of implementing SIEM in large-scale, distributed environments. It introduces a hierarchical SIEM management model that utilizes multiple SIEM managers to improve log management and security event correlation. The proposed architecture is demonstrated using ArcSight ESM, showing how it can efficiently manage security logs across multiple regions. The study also provides examples of use cases to illustrate the practical application of this model, making SIEM more scalable and effective for global enterprises.

[3] Mokalled et al. (2019) – "The Applicability of a SIEM Solution: Requirements and Evaluation"
This paper presents a structured approach for selecting and evaluating SIEM solutions. It argues that choosing the right SIEM depends not only on technical capabilities but also on organizational requirements, compliance needs, and business objectives. The authors propose a framework for assessing SIEM solutions using both qualitative and

quantitative criteria. The paper aims to help enterprises adopt SIEM solutions that align with their IT environment, security goals, and operational constraints, ensuring effective threat detection and incident response.

[4]Serckumecka et al. (2019) – "Low-Cost Serverless SIEM in the Cloud"
This research investigates cost-effective alternatives to traditional SIEM solutions by leveraging cloud computing. The authors propose a serverless SIEM architecture that reduces operational costs while maintaining security and compliance. Key innovations include cloud-based event storage, indexing, and a serverless correlation engine that scales dynamically. By integrating cloud-native technologies such as Amazon Lambda, the study aims to provide an affordable and efficient SIEM solution for organizations with limited budgets.

S.NO	TITLE	AUTHOR(S)	METHODOLOGY	PROS	CONS
1	SIEM Implementation for Global and Distributed Environments	Anastasov & Davcev (2014)	Proposed a Hierarchical Managers Model for SIEM using ArcSight ESM	Improves log management and threat detection efficiency	Requires significant customization and use-case development
2	Improving SIEM Alert Metadata Aggregation with a Novel Kill-Chain Based Classification Model	Bryant & Saiedian (2020)	Developed a kill-chain-based classification model to enhance SIEM alerting	Reduces false positives and improves correlation	Complex implementation and requires extensive tuning
3	The Applicability of a SIEM Solution: Requirements and Evaluation	Mokalled et al. (2019)	Proposed evaluation criteria for selecting a SIEM solution based on enterprise needs	Helps organizations choose a suitable SIEM	No universal SIEM fits all organizations; context-dependent
4	Low-Cost Serverless SIEM in the Cloud	Serckumecka et al. (2019)	Designed a cloud-based serverless SIEM using AWS Lambda	Cost-effective and scalable	Security concerns and vendor lock-in
5	An Approach to Developing the SIEM System for the Internet of Things (IoT)	Lavrova (2016)	Proposed a graph-based model for IoT security event analysis	Enhances SIEM adaptability for IoT environments	Traditional SIEMs struggle with IoT data volumes
6	Challenges and Directions in Security Information and Event Management (SIEM)	Cinque et al. (2018)	Explored SIEM integration challenges in mission-critical Air Traffic Control systems	Highlights key SIEM implementation issues	High complexity and difficulty in handling unstructured logs
7	The Ontological Approach for SIEM Data Repository Implementation	Kotenko et al. (2012)	Proposed an ontology-based SIEM data model	Improves event correlation and data representation	Computationally expensive and requires ontological expertise

III. IMPLEMENTATION METHODOLOGY OF PROPOSED SYSTEM

SIEM on Ubuntu:

The implementation of a Security Information and Event Management (SIEM) system on Ubuntu follows a structured approach that ensures seamless integration with the existing IT infrastructure while enabling efficient security monitoring. This methodology is divided into key phases: planning and requirements analysis, installation and initial setup, log collection and normalization, correlation and threat detection, alerting and incident response, performance optimization, and evaluation.

Setup of SIEM:
The appropriate SIEM solution is selected from options like ELK Stack, Wazuh, AlienVault OSSIM, or Graylog, considering factors such as scalability, performance, and compatibility. Once planning is complete, the installation and initial setup phase involves updating the Ubuntu system, creating a dedicated SIEM user, enabling time synchronization, and installing the chosen SIEM tool. For instance, installing the ELK Stack requires setting up Elasticsearch, Logstash, and Kibana, while Wazuh installation involves deploying the Wazuh Manager and enabling its services. Log collection and normalization are then configured, ensuring that log data is structured for analysis. Log forwarders such as Filebeat (for ELK) or Wazuh agents are installed on endpoints to transmit logs to the SIEM server, while log normalization is achieved using Logstash filters to parse logs into a standardized format.

Correlation and Threat Detection:
Once logs are collected, correlation and threat detection rules are implemented to identify potential security incidents. Custom rules, such as detecting brute-force SSH attacks by monitoring failed login attempts, are applied. Machine learning-based anomaly detection can be integrated to enhance the accuracy of threat identification. To respond effectively to security events, alerting and incident response mechanisms are set up. Email notifications are configured using ElastAlert for ELK, and automated incident response actions, such as blocking malicious IP addresses, are integrated with Security Orchestration, Automation, and Response (SOAR) tools. Performance optimization is then conducted to ensure efficiency, involving Elasticsearch tuning, log rotation to prevent excessive storage consumption, and fine-tuning correlation rules to reduce false positives.

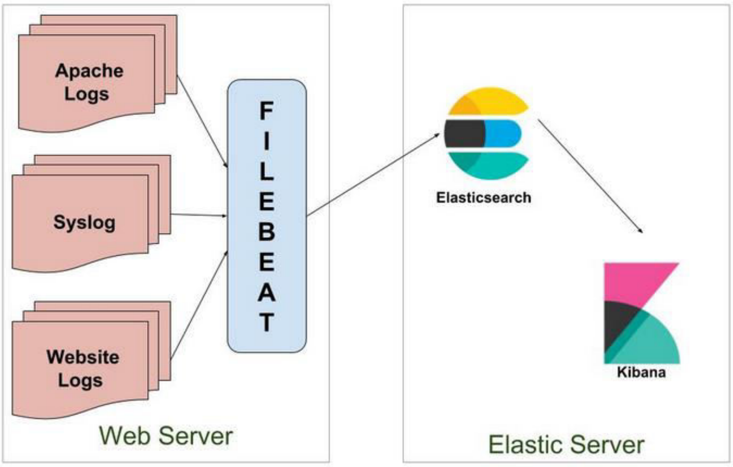


Figure 2 Log collection

Evaluation and Improvement:
Structured logs have been successfully implemented, and it is time to proceed to the correlation & threat detection step. This step is about analyzing security events to potentially identify security threats and incidents. The correlation rules are the best way to detect behavior patterns that can be potentially suspicious. For example, this can be multiple failed login attempts, privilege escalation, unauthorized access to critical systems, and so on. The following example can illustrate this point. An SSH brute-force may be detected by tracking multiple failed login attempts on the same IP address within a short period.

Machine learning-based anomaly detection can also be incorporated to improve the accuracy of threat detection. Anomalies detection algorithms analyze historical log data and detect deviations from normal activity patterns, so they can detect unknown threats, zero-day attacks and sophisticated cyberthreats that can evade traditional rule-based detection.

Once security threats are identified the alerting and incident response phase ensures that security teams are notified in real-time and appropriate countermeasures are deployed. Email alerts can be configured using ElastAlert for ELK or

Wazuh's built-in alerting mechanisms.At the end evaluation and continuous improvement include defining key performance indicators, such as false-positive rates and Mean Time to Detect (MTTD), performing penetration testing using tools like Metasploit, and continuously refining correlation rules based on emerging threats.

IV. CONCLUSION AND FUTURE WORK

With the implementation of Elastic Cloud, we have established a centralized platform for security operations, enabling streamlined management and real-time monitoring of data. This setup allows security analysts to remotely access the Elastic SIEM (Security Information and Event Management) system, ensuring continuous oversight and swift response to potential security incidents from any location. The Elastic Stack suite, comprising Logstash, Elasticsearch, and Kibana, serves as the backbone of this system. Logstash facilitates the ingestion and processing of log data, Elasticsearch provides efficient storage and rapid search capabilities, and Kibana offers robust visualization and analytical tools. Additionally, Elastic Agent plays a crucial role in bridging the SIEM with Windows-based systems, ensuring seamless log data transmission via Sysmon and Winlogbeat.

To enhance proactive threat detection, a range of detection rules and real-time alerts have been configured to identify unauthorized access attempts, anomalous behaviors, and other security threats. By integrating VirusTotal, the system further strengthens its threat intelligence capabilities through automated malware scanning and analysis, improving overall security posture. Furthermore, Arkime has been incorporated to bolster security from a network traffic analysis perspective, providing deeper insights into potential threats within network communications. The addition of a Honeypot system enhances defensive strategies by attracting malicious actors, capturing their attack methods, and gathering critical intelligence on event triggers and adversary behaviors.

In summary, the integration of Elastic SIEM with complementary security tools has significantly improved the organization's ability to detect, monitor, and respond to security threats in real time. By leveraging automation, threat intelligence, and network monitoring capabilities, this comprehensive solution enhances overall security efficiency and resilience against evolving cyber threats

REFERENCES

[1] Podzins ,"Why SIEM is Irreplaceable in a Secure IT Environment",IEEE,2019
[2]Serckumecka et al. "Low-Cost Serverless SIEM in the Cloud", 38th Symposium on Reliable Distributed Systems (SRDS),2019
[3 Mokalled et al. "The Applicability of a SIEM Solution: Requirements and Evaluation",2019
[4] Anastasov & Davcev "SIEM Implementation for Global and Distributed Environments" ,2014
[5] An Approach to Developing the SIEM System for the Internet of Things (IoT)-Lavrova 2016
[6]Challenges and Directions in Security Information and Event Management (SIEM)-Cinque et al. 2018
[7] The Ontological Approach for SIEM Data Repository Implementation Kotenko et al. (2012)

INNO SPACE
SJIF Scientific Journal Impact Factor

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com