PROJECT REPORT

Name Sudhir S Bhat

Title: **Security Information and Event Management (SIEM) Systems**

1. Introduction

In today's digital world, organizations rely heavily on IT systems to run daily operations. Every system-whether it is a server, firewall, application, or endpoint-generates logs that record activities such as logins, file access, errors, and network connections. Individually, these logs may not seem important, but collectively they tell the story of what is happening inside an organization's environment.

Security Information and Event Management (SIEM) systems are designed to collect, analyze, and correlate these logs to detect security threats in real time. This project focuses on understanding how SIEM systems work, how Security Operations Centers (SOC) use them, and how alerts are generated and handled—without performing any real attacks or exploitation.

2. Objective

The primary objective of this project is to gain a practical and conceptual understanding of SIEM systems from a SOC analyst perspective.

Specific objectives include

- Understanding **how logs are collected from multiple sources**
- Learning how **SIEM normalizes and correlates log data**
- Understanding **alert generation and severity classification**
- Simulating **SOC L1 analyst** responsibilities such as alert triage
- Learning how **SIEM supports incident detection and response**

This project is designed to **simulate real-world enterprise security** monitoring in a safe and ethical manner.

3. What is SIEM?

SIEM stands for Security Information and Event Management. It combines two core security concepts.

Security Information Management (SIM)

- Focuses on log collection, storage, and historical analysis.

Security Event Management (SEM)

- Focuses on real-time monitoring, correlation, and alerting.

A SIEM system acts as a **centralized security monitoring platform** that gives security teams visibility across the entire organization.

4. Why SIEM is Important in Cyber Security

Modern attacks are often stealthy and spread across multiple systems. A single log entry may not indicate an attack, but when correlated with other events, it may reveal malicious activity.

SIEM helps organizations by

- Detecting threats early
- Reducing incident response time
- Providing centralized visibility
- Supporting compliance and audits
- Enabling forensic investigations

Without SIEM, organizations would struggle to identify coordinated or slow-moving attacks.

5. Role of SIEM in a Security Operations Center (SOC)

In a SOC environment, SIEM is the primary tool used by analysts.

SOC analysts use SIEM to

- Monitor dashboards for alerts
- Investigate suspicious activities
- Validate alerts and reduce false positives
- Escalate confirmed incidents
- Document findings for incident response

For a SOC L1 analyst, SIEM is the starting point for almost every investigation.

6. SIEM Architecture Overview

A typical enterprise SIEM architecture includes.

6.1 Log Sources

- Firewalls
- Windows/Linux servers
- Web servers
- Databases
- Endpoints

6.2 Log Collection Mechanism

- Agents
- Syslog
- API integrations

6.3 SIEM Core Engine

- Log ingestion
- Parsing
- Indexing

6.4 Correlation & Analytics Engine

- Rule-based detection
- Behavioral analysis

6.5 SOC Dashboard

- Alerts
- Visualizations
- Reports

This layered architecture ensures logs are securely collected, processed, and analyzed.

7. Log Collection Process

Log collection is the foundation of SIEM. If logs are missing or incomplete, threats can go undetected.

Steps involved

- Logs are generated by systems and devices
- Logs are forwarded to SIEM using agents or syslog
- Logs are securely transmitted
- Logs are stored centrally for analysis

Common log types include

- Authentication logs
- Network traffic logs
- Application access logs
- System error logs

8. Log Parsing and Normalization

Raw logs come in different formats depending on the source. SIEM systems parse logs to extract useful fields such as.

- Timestamp
- Source IP
- Destination IP
- Username
- Event type

Normalization converts logs into a common structure, allowing correlation across different systems. This step is critical for accurate threat detection.

9. Correlation Rules

Correlation rules define what the SIEM considers suspicious behavior.

Examples

- Multiple failed login attempts from the same IP
- Successful login after multiple failures
- Access from a new geographic location
- Privilege escalation attempts

Correlation rules help reduce noise and focus attention on meaningful security events.

10. Alert Generation and Severity Levels

When a correlation rule is triggered, the SIEM generates an alert.

Alerts are usually categorized as

- Low
- Medium
- High
- Critical

Severity depends on

- Asset importance
- Type of activity
- Potential impact
- Threat intelligence context

Proper severity classification helps SOC teams prioritize incidents effectively.

11. SOC Alert Triage

SOC L1 analysts are the first responders to SIEM alerts.

Typical triage steps:

1. Review alert details
2. Analyze related logs
3. Identify false positives
4. Validate suspicious activity
5. Escalate confirmed incidents

L1 analysts focus on speed, accuracy, and documentation rather than deep forensic analysis.

12. Integration with Incident Response

SIEM is closely integrated with incident response processes.

Once an alert is confirmed

- Tickets are created
- Incident response playbooks are followed
- Stakeholders are notified
- Evidence is preserved

SIEM provides the data needed to understand the scope and timeline of an incident.

13. Use Case Examples

Some common SIEM use cases include.

- Brute-force login detection
- Malware communication detection
- Insider threat monitoring
- Suspicious admin activity
- Data exfiltration detection

These use cases demonstrate how SIEM translates raw logs into actionable security insights.

14. Challenges Faced

During this project, several challenges were encountered.

- Understanding how different log sources relate to each other
- Distinguishing false positives from real threats

- Interpreting alert severity correctly
- Designing meaningful correlation logic

These challenges helped develop analytical thinking and a SOC-oriented mindset.

15. Outcomes

By completing this project

- I gained a strong understanding of SIEM fundamentals
- I learned how SOC analysts monitor and investigate alerts
- I understood the importance of log context and correlation

This project bridged the gap between theory and real-world SOC operations.

16. Lessons Learned

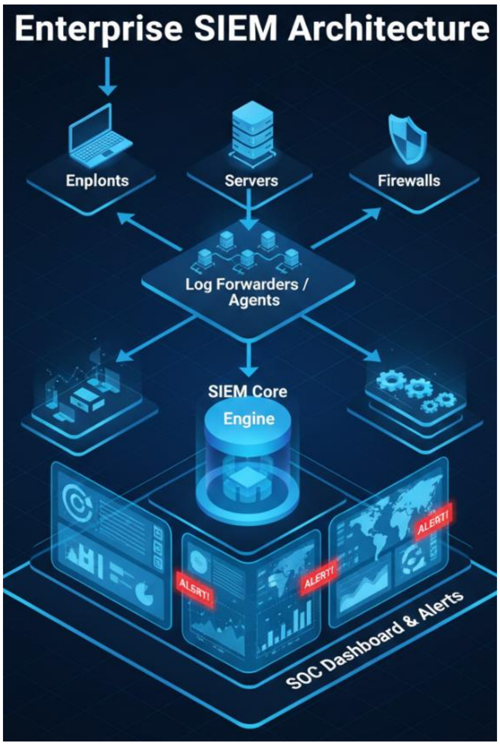
Key lessons learned include

- Visibility is essential for security
- Context matters more than individual alerts
- SIEM supports human decision-making, not replaces it
- Proper log management is critical for detection

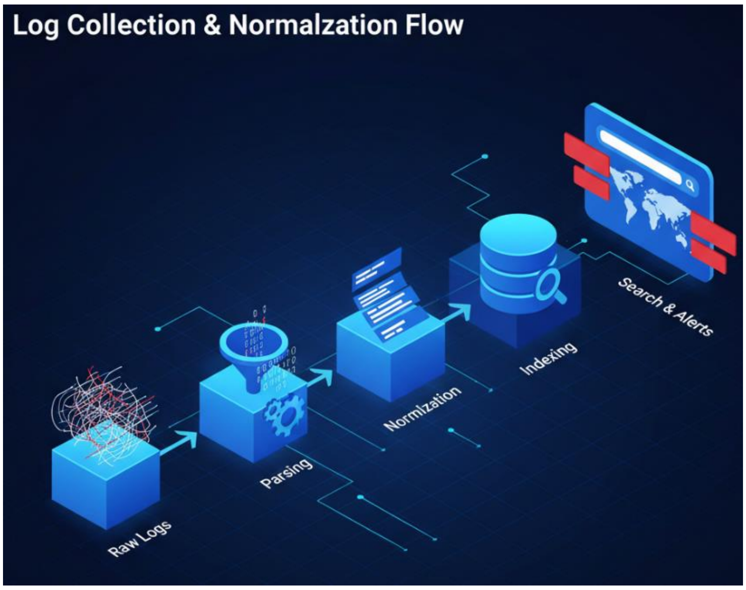
These lessons are directly applicable to entry-level SOC roles.

17. Diagram

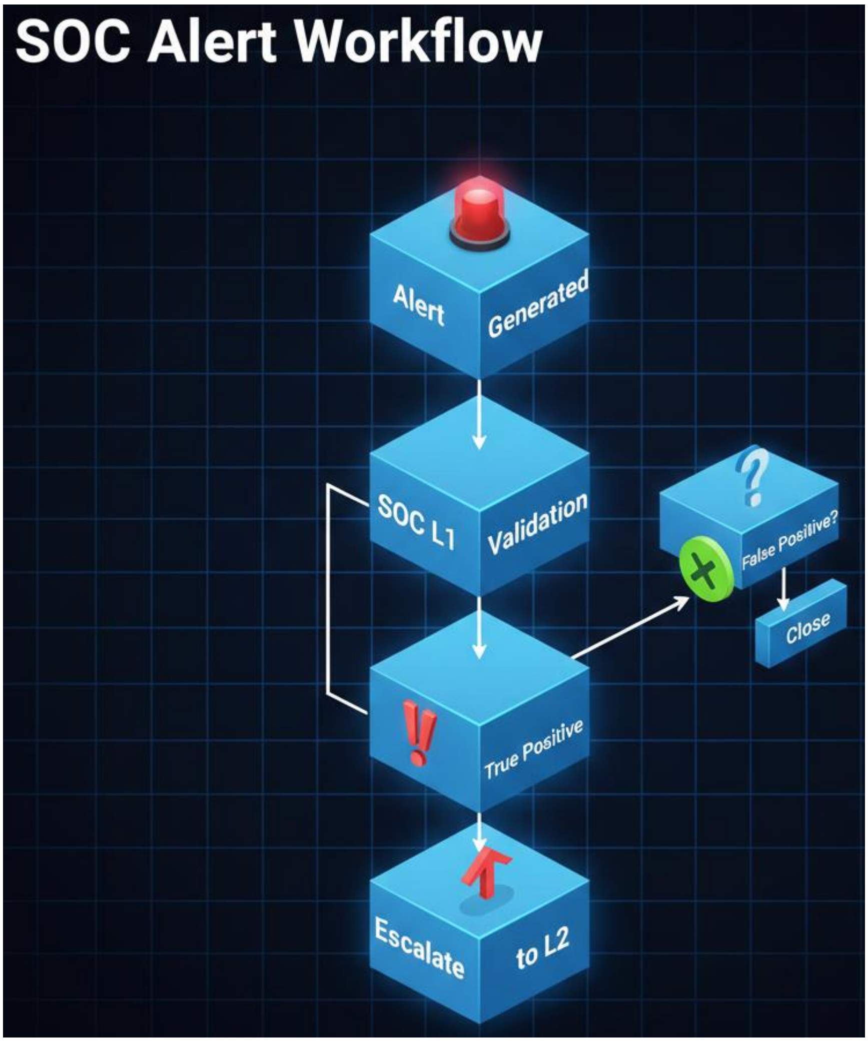
1. Enterprise SIEM Architecture



2. Log Collection & Normalization Flow



3. SOC Alert Workflow



18. Conclusion

Security Information and Event Management systems play a vital role in modern cyber defense. By centralizing logs, correlating events, and generating alerts, SIEM enables organizations to detect and respond to threats efficiently. This project provided hands-on conceptual exposure to SIEM systems and SOC workflows, preparing me for real-world cyber security operations.