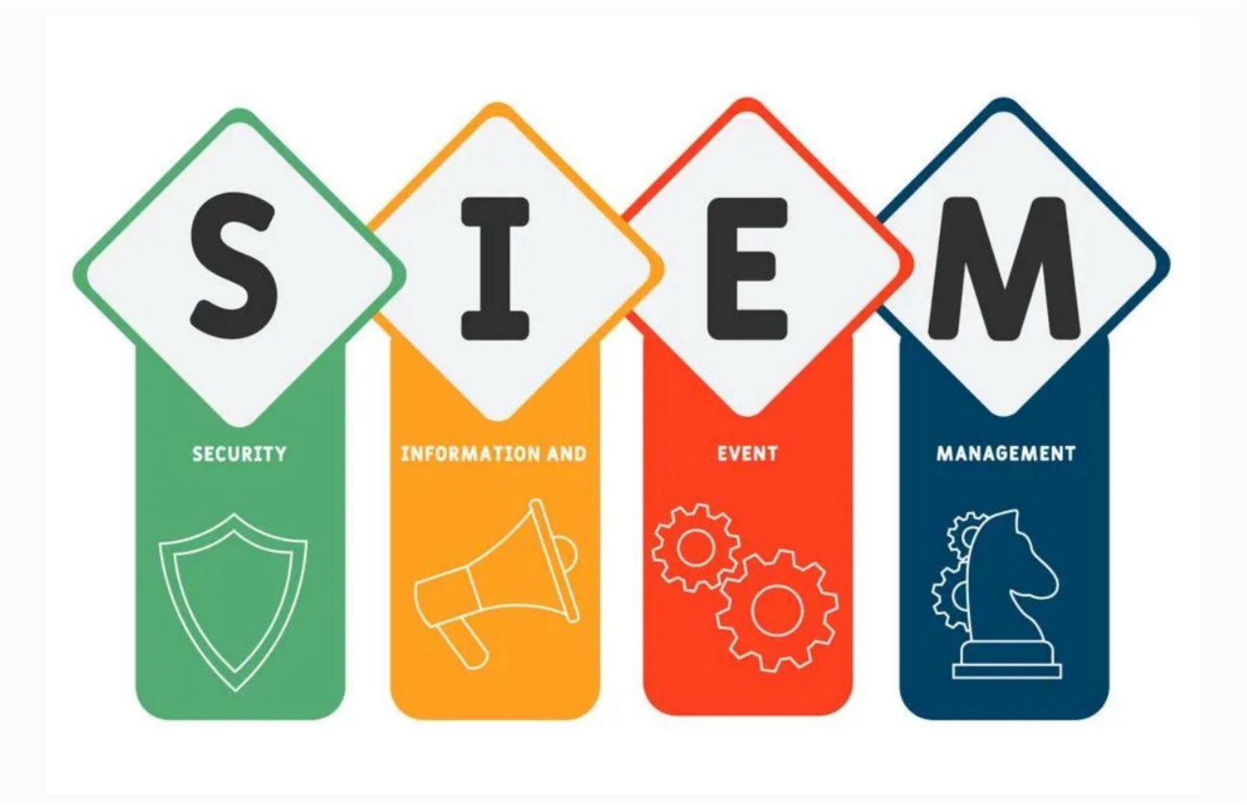
A Research Report on

SIEM ARCHITECTURE



Prepared by
Siva Krishna Siripurapu

Report on SIEM Architecture

Author: Sivakrishna Siripurapu

Date: 12-12-2024

Introduction:

Security Information and Event Management (SIEM) systems are essential tools for monitoring, analyzing, and responding to security threats in real time. They aggregate data from multiple sources, correlate events, and provide actionable insights to enhance an organization's security posture. This document explores the architecture of SIEM, detailing its components, workflow, and applications.

1. Objective:

Purpose:

- To understand the architecture of SIEM systems and their role in cybersecurity.
- To learn how SIEM systems aggregate and analyze security data in real time for early detection of threats.

Goals:

- Gain insights into the components and working of SIEM architecture.
- Learn about the different layers involved in SIEM and how they interact.
- Understand the role of SIEM in threat detection, monitoring, and incident response.

2. Scope:

Target Audience:

- Security analysts, IT professionals, organizations deploying SIEM systems, cybersecurity students.

Focus Areas:

- SIEM deployment models (on-premises vs cloud).
- Architecture components: Collectors, Aggregators, Correlation Engines, Data Storage, Dashboards.
- Integration with existing IT systems and network infrastructure.
- Use of SIEM in threat intelligence, compliance, and incident response.

3. Tools and Resources Used:

Software/Tools:

- SIEM platforms: Splunk, IBM QRadar, ArcSight, and LogRhythm.
- Security data collection tools (Syslog, SNMP, etc.).
- Threat intelligence tools (like Threat Feeder, OpenDXL).

Hardware Requirements:

- Servers for deploying SIEM software, storage for log data, network infrastructure for data collection.

References:

- Splunk Documentation: "How to Set Up and Manage Splunk."
- IBM QRadar Documentation: "QRadar SIEM Architecture Overview."
- NIST Special Publication 800-92: "Guide to Computer Security Log Management."
- O’Reilly: "Security Information and Event Management (SIEM)".

4. Components and Concepts:

Key Components:

- **Data Collection:** Captures logs and events from devices, network infrastructure, and security appliances (firewalls, routers, etc.).
- **Normalization:** Standardizes collected data into a common format for easy analysis.
- **Correlation Engine:** Correlates events across various sources to detect patterns indicating potential security threats.
- **Event Storage:** A central repository for storing raw logs and processed events for historical analysis.
- **Analysis and Reporting:** Dashboards and reports provide insights into security posture and alert status.

Key Concepts:

- **Event Correlation:** The process of linking related events to identify potential incidents.

- **Log Management:** Collecting, storing, and analyzing logs from various systems to detect threats and maintain compliance.
- **Threat Intelligence Integration:** Using external threat feeds to enhance the detection capabilities of SIEM systems.
- **Alert Management:** Raising alerts based on predefined rules or anomalous patterns.

SIEM Architecture Overview:

- **Data Sources**
    - Firewalls, IDS/IPS, network traffic, endpoints, servers.
    - Example: Logs from servers, network devices, and applications are sent to the SIEM system for analysis.
- **Log Collection Layer**
    - Collector's aggregate logs and events from various sources using protocols like Syslog, SNMP, or APIs.
- **Processing Layer**
    - Logs are processed for correlation and analysis using the SIEM's correlation engine and predefined rules.
- **Storage Layer**
    - The logs and events are stored in databases for real-time and historical analysis.
- **Analysis and Reporting Layer**
    - Dashboards provide a real-time view of alerts and incidents, with detailed reports for compliance and auditing.

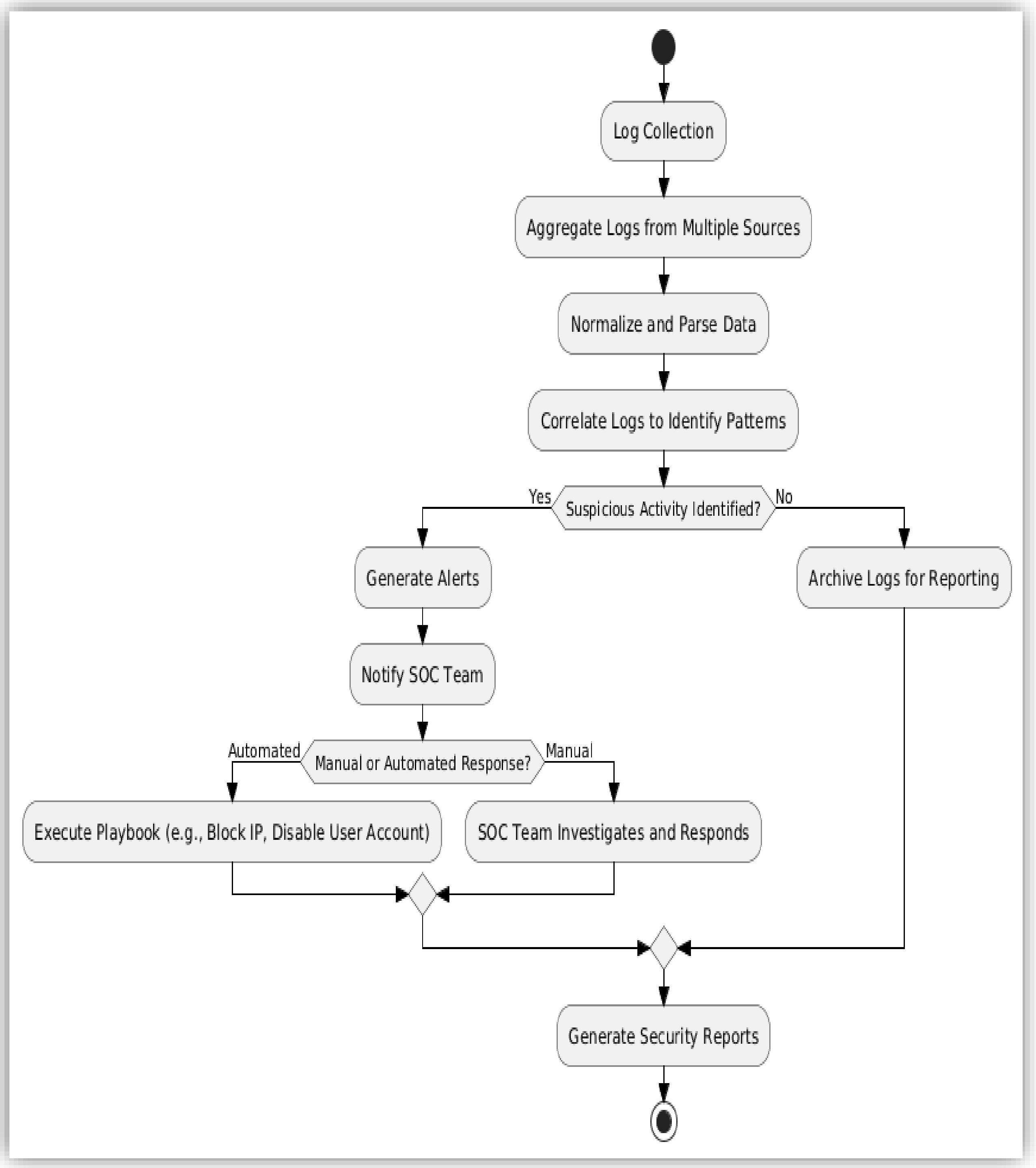

Log Collection
Aggregate Logs from Multiple Sources
Normalize and Parse Data
Correlate Logs to Identify Patterns
Yes
Suspicious Activity Identified?
No
Generate Alerts
Archive Logs for Reporting
Notify SOC Team
Automated
Manual or Automated Response?
Manual
Execute Playbook (e.g., Block IP, Disable User Account)
SOC Team Investigates and Responds
Generate Security Reports

Figure 1: SIEM Architecture Overview

5. Procedure/Implementation Steps:

1. **Preparation:**
   - Set up the SIEM platform (e.g., Splunk, QRadar).
   - Integrate log sources (e.g., firewalls, servers) with the SIEM system.
   - Define collection protocols (Syslog, SNMP, API integration).
2. **Execution:**
   - Configure log collection policies and data sources.
   - Set up correlation rules to detect potential threats.
   - Implement real-time monitoring and alerting systems.
3. **Validation:**
   - Test the system with simulated security events to ensure proper alert generation.
   - Validate the correlation engine's accuracy by reviewing false positives and refining rules.
4. **Challenges and Errors:**
   - False positives: SIEM systems may raise excessive alerts for benign events.
   - Data overload: Collecting vast amounts of logs and events can strain the SIEM system's resources.
   - Integration issues: Difficulty in integrating legacy systems with modern SIEM platforms.

6. Results and Analysis:

1. **Findings:**
   - SIEM systems provide real-time visibility into security events and enable faster incident detection.
   - Data normalization and correlation enhance the ability to detect advanced persistent threats (APTs).
   - Integration of threat intelligence feeds improves the detection of emerging threats.
2. **Insights:**
   - SIEM provides centralized monitoring and incident response capabilities.
   - Proper tuning of the correlation engine reduces false positives and improves efficiency.

- Regular updates to correlation rules and threat intelligence feeds keep the system relevant to emerging threats.

7. Discussion:

- **Strengths:**
  - Provides a centralized solution for security monitoring and analysis.
  - Detects sophisticated threats through real-time correlation and analysis.
  - Improves incident response times and enhances compliance reporting.
- **Limitations:**
  - High resource consumption in large-scale environments.
  - Complex integration with multiple heterogeneous systems.
  - Potential for false positives if correlation rules are not finely tuned.
- **Improvements:**
  - Enhance AI and machine learning capabilities for better anomaly detection.
  - Use cloud-based SIEM for scalable, cost-efficient deployments.
  - Implement automated response actions to reduce incident response times.

8. Conclusion:

SIEM architecture is fundamental in detecting and managing cybersecurity threats by providing real-time monitoring, event correlation, and detailed reporting. Its ability to integrate with various security tools and systems makes it a powerful solution for threat detection, incident response, and compliance. By continually refining correlation rules, integrating threat intelligence, and adapting to emerging threats, SIEM systems remain an essential component of an organization’s cybersecurity strategy.

9. Recommendation:

- Implement SIEM systems for centralized monitoring and incident management.
- Regularly update correlation rules and threat intelligence feeds.
- Train security teams to efficiently use SIEM platforms for effective threat analysis and response.

10. References:

Splunk Documentation: "Splunk Architecture Overview." https://www.splunk.com/
IBM QRadar Documentation: "QRadar SIEM Implementation Guide." https://www.ibm.com/security/qradar
O’Reilly: "SIEM: A Complete Guide for Security Management." https://www.oreilly.com/
NIST SP 800-92: "Guide to Computer Security Log Management." https://csrc.nist.gov/publications/detail/sp/800-92/final
"SIEM Architectures: A Practical Guide" – Wiley, 2020.

11. Appendices:

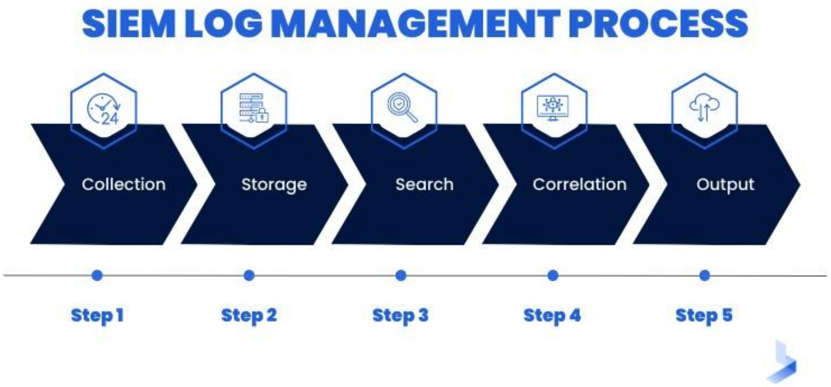
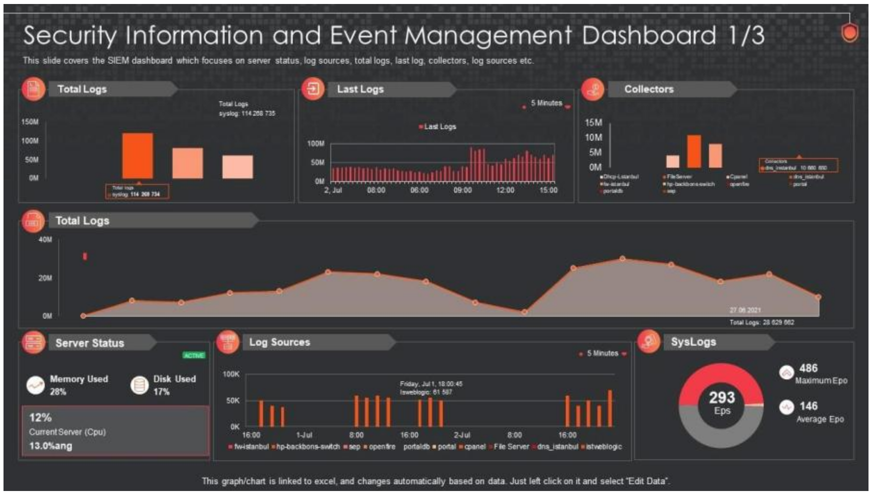


Figure 2: SIEM Integration with Log Sources


Security Information and Event Management Dashboard 1/3

This slide covers the SIEM dashboard which focuses on server status, log sources, total logs, last log, collectors, log sources etc.

This graph/chart is linked to excel, and changes automatically based on data. Just left click on it and select "Edit Data".

Figure 3: Example SIEM Dashboard