Introduction to SIEM

---

1. What is a SIEM?

Definition:
A SIEM (Security Information and Event Management) system collects, aggregates, normalizes, and analyzes security-related data from across an organization's IT infrastructure.

Purpose:

- **Centralized visibility into security events.**
- **Detect suspicious activity and potential threats.**
- **Support compliance and reporting requirements.**
- **Help security teams respond quickly to incidents.**

---

2. How SIEM Works (High-Level)

1. **Data Collection – Gathers logs and events from servers, applications, firewalls, endpoints, cloud services, etc.**
2. **Normalization – Converts all logs into a consistent format for easier analysis.**
3. **Correlation & Analytics – Applies rules, queries, or machine learning to detect patterns and anomalies.**
4. **Alerting & Reporting – Generates alerts and provides dashboards and compliance reports.**
5. **Retention – Stores log data for investigations, audits, and forensic analysis.**

---

3. Common Data Types Captured

Network Data

- **Firewall logs (allowed/blocked traffic)**
- **IDS/IPS alerts**
- **VPN and remote access logs**

System Data

- **OS logs (Windows Event Logs, Linux syslog)**
- **Authentication attempts (logins, failures, privilege escalations)**
- **Process creation/termination logs**

Application Data

- **Web server logs (HTTP requests, errors)**
- **Database queries**
- **Email server activity**

Identity & Access Data

- **Active Directory events (logins, group changes)**
- **Privileged account usage**
- **MFA events**

Cloud & SaaS Logs

- **AWS CloudTrail, Azure Activity Logs, GCP Audit Logs**
- **SaaS events (Office 365, Salesforce, etc.)**

Endpoint Data

- **Antivirus/EDR detections**
- **USB/device usage**
- **File access monitoring**

---

4. Why Organizations Use SIEM

- **Threat Detection – Spot abnormal behavior (e.g., repeated failed logins, unusual data transfers).**
- **Incident Response – Build event timelines for investigations.**
- **Compliance – Meet regulatory requirements (HIPAA, CJIS, PCI-DSS, etc.).**
- **Operational Visibility – Understand activity across the entire IT environment.**

---

5. A Simple Example

A SIEM receives:

- **10 failed login attempts from the same user in 2 minutes.**
- **A successful login from that user, but from an unusual country.**
- **Access to sensitive database records.**

The SIEM correlates these events and raises an alert for a possible account compromise.

---

6. The Next Generation of SIEM

- **AI & Machine Learning – Detect unusual behavior and trends beyond static rules.**
- **Behavior Analytics – Track normal user activity and identify deviations.**

Challenges:

- **High volume of alerts often requires manual intervention.**

---

7. Beyond SIEM: SOAR

SOAR – *Security Orchestration, Automation, and Response*

- **Automates routine tasks (e.g., finding and deleting phishing emails).**
- **Uses playbooks/rulebooks to respond automatically (e.g., quarantining a compromised computer).**

---

8. Real-World Example – My Environment

- **Devices monitored: ~162 (servers, workstations, firewalls, switches).**
- **Events captured daily: Over 15 million.**
- **Capabilities:**
    - **Rapid log search (keyword-based).**

    - **Pre-built (canned) reports for hardware and security insights.**
- **Licensing considerations:**
    - **Looked at Splunk – too expensive (licensed by daily GB of ingested data).**
    - **Chose an alternative with *device-based licensing*, allowing unlimited data per device.**