Security Operations Center (SOC) and SIEM Systems: Architecture and Log Analysis

Introduction

Modern organizations face increasing cybersecurity threats. To monitor, detect, and respond to these threats in real time, two critical components are employed:

- **SOC (Security Operations Center)** – A centralized facility where security professionals monitor, analyze, and respond to security incidents.
- **SIEM (Security Information and Event Management)** – A software solution that collects and analyzes security logs from various sources to identify anomalies or attacks.

Together, SOC and SIEM form the foundation of an organization's cybersecurity monitoring and response strategy.

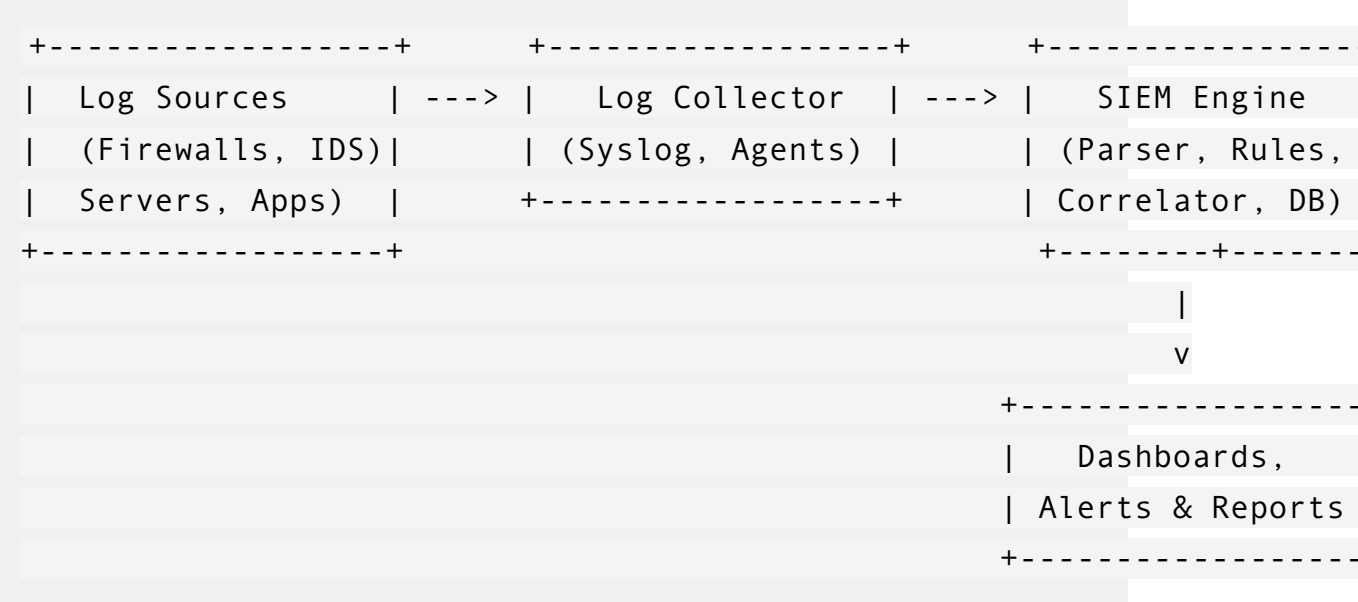
2. SIEM Systems: Architecture and Components

2.1 What is SIEM?

SIEM (Security Information and Event Management) is a platform that provides:

- **Real-time analysis of security alerts**
- **Correlation of log data from multiple systems**
- **Historical data storage for compliance and investigation**

2.2 SIEM Architecture



2.3 Components

- **Log Collectors**: Agents or services that gather logs from endpoints, applications, and network devices.
- **Normalization/Parsing**: Converts raw log formats into a consistent, structured format.
- **Correlation Engine**: Applies rules or machine learning to detect suspicious patterns across multiple sources.
- **Data Store**: Archives raw and processed logs for retention and forensic analysis.
- **Dashboards & Alerts**: Visualize security events and generate real-time alerts.

4. Log Analysis in SIEM

4.1 Parsing and Normalization

Logs from different sources are parsed using regular expressions or parsing rules. The normalized format includes fields like:

```
{
  "timestamp": "2025-07-21T01:00:00Z",
  "src_ip": "10.0.0.5",
```

```
  "dst_ip": "192.168.1.10",
  "event_type": "login_failure",
  "username": "admin"
}
```

4.2 Correlation Rules

Correlation links multiple log events into a meaningful alert:

- **Example 1**: 5 failed logins followed by a successful login from the same IP → brute-force attack.
- **Example 2**: User downloads >500 MB of data outside business hours → potential data exfiltration.

4.3 Use Cases

- **Insider Threat Detection**: Privileged users accessing restricted data.
- **Advanced Persistent Threats (APT)**: Long dwell-time, multi-stage attacks.
- **Malware Outbreaks**: Identifying lateral movement and command & control (C2) traffic.
- **Compliance Violations**: Logins from blacklisted IPs, disabled accounts used.

6. Challenges

- **False Positives**: Alert fatigue due to noisy rules.
- **Log Volume**: High ingestion costs and storage overhead.
- **Complex Configuration**: Rules and normalization can be time-consuming.
- **Encrypted Traffic**: Limits visibility without SSL interception.

Conclusion

The integration of a well-staffed SOC and a powerful SIEM system enables organizations to detect, investigate, and respond to cyber threats efficiently. By analyzing logs from across the IT landscape,

SIEM tools offer invaluable insights, and with automated response through SOAR or threat intelligence enrichment, organizations can stay ahead of adversaries in today’s dynamic threat environment.