CS-086 · Vulnerability & Operations

# SIEM

Security Information and Event Management, the platform that collects and correlates logs to surface threats.

## Executive Summary

A SIEM, or Security Information and Event Management platform, collects logs and event data from across an environment, normalizes it, and correlates it to detect and alert on suspicious activity. It gives security teams a central place to see what is happening, investigate incidents, and retain evidence. The SIEM is the analytical backbone of most security operations.

## What It Is

A SIEM ingests data from a wide range of sources such as servers, endpoints, firewalls, identity systems, applications, and cloud services. It normalizes those varied log formats into a common structure, stores them centrally, and applies detection logic to spot patterns that indicate a threat. Historically the term combined two ideas: security information management, which focused on collecting and retaining logs for reporting and compliance, and security event management, which focused on real-time monitoring and correlation. Modern SIEMs do both, and many add analytics for user and entity behavior and integrate with automation. A SIEM is not a preventive control that blocks attacks; it is a detective and investigative platform that helps a team see and understand what is happening.

## Why It Matters

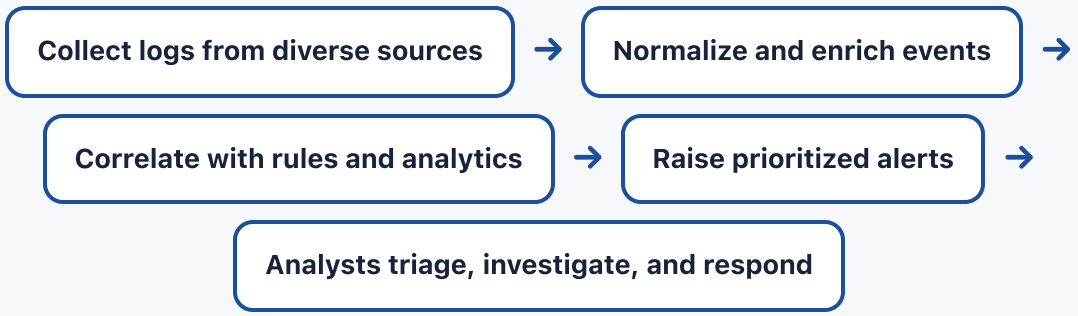
Attacks leave traces scattered across dozens of systems, and no analyst can watch every log by hand. A SIEM brings those traces together so a single alert can connect a failed login on one system to a suspicious file on another. It shortens the time to detect and investigate incidents, provides the searchable history responders need, and supplies the audit and retention evidence many regulations require. For the business, a well-run SIEM is often the difference between

catching an intrusion early and discovering it months later from a third party. For professionals, SIEM skills are among the most in-demand in security operations because the platform sits at the center of daily detection and response work.

## How It Works

Data flows into a SIEM through agents, log forwarders, and APIs. The platform parses and normalizes each event into common fields such as user, host, and action, then enriches it with context like asset criticality or threat intelligence. Correlation rules and analytics evaluate the stream to identify meaningful patterns, for example many failed logins followed by a success from an unusual location. When logic matches, the SIEM raises an alert, often assigning a severity, and presents it to analysts through dashboards and a queue. Analysts triage alerts, pivot through related events to investigate, and escalate real incidents. Tuning is continuous work: rules are refined to reduce false positives, new log sources are onboarded, and detections are added to keep pace with evolving threats. Many SIEMs connect to SOAR tools so common responses can be automated.

## Architecture Diagram




A SIEM ingests logs from many sources, normalizes and correlates them, then alerts analysts.

## Visual Workflow


## Common Attacks

- Attackers disabling or clearing logs to blind the SIEM
- Low-and-slow activity designed to stay under alerting thresholds
- Compromised credentials whose misuse only correlation across sources reveals
- Attacks against log sources that were never onboarded, so nothing is seen
- Alert flooding or noise used to hide the one event that matters

## Common Mistakes

- Collecting everything with no plan, driving up cost and noise
- Leaving critical log sources unmonitored so detections have blind spots
- Never tuning rules, so analysts drown in false positives and ignore alerts
- Treating the SIEM as compliance storage rather than a detection engine
- Failing to protect and back up logs so evidence can be tampered with or lost

## Best Practices

- Onboard log sources deliberately, prioritizing high-value detection data
- Map detections to a framework such as MITRE ATT&CK for coverage
- Continuously tune rules to cut false positives and alert fatigue
- Enrich events with asset context and threat intelligence
- Protect log integrity and set retention to meet legal and audit needs
- Integrate with SOAR and case management to speed response

## Quick Checklist

- [x] Critical log sources identified and onboarded
- [x] Detections mapped to a coverage framework like MITRE ATT&CK
- [x] Alert tuning process in place to manage false positives
- [x] Events enriched with asset and threat context
- [x] Log retention meets compliance and investigation needs
- [x] Log integrity protected and monitored for tampering

## Recommended Tools

**SIEM platform**
Collects, normalizes, correlates, and alerts on security event data

**Log forwarder or agent**
Ships logs from sources into the SIEM reliably

**SOAR platform**
Automates repeatable response actions triggered by SIEM alerts

**Threat intelligence feed**
Enriches events so detections reflect current adversary activity

## Industry Standards

**NIST SP 800-92**
Guide to computer security log management practices

**MITRE ATT&CK**
Knowledge base used to map detection coverage against adversary techniques

**PCI DSS**
Requires log collection, review, and retention that SIEM commonly supports

## Career Relevance

The SIEM is where SOC analysts spend much of their day, and building and tuning it is core to security engineer and detection engineer roles. Threat hunters query it to test hypotheses, and GRC and audit professionals rely on its logs and reports for evidence. SIEM fluency, from writing a detection to investigating an alert, is one of the most transferable skills in the security field that AI-Governance-Jobs.com serves.

## Interview Questions

- What does a SIEM do, and how is it different from a firewall or EDR?
- Walk me through how you would investigate a correlation alert in a SIEM.
- How do you reduce false positives without missing real threats?
- Which log sources would you prioritize onboarding, and why?
- How would you use MITRE ATT&CK to measure your SIEM detection coverage?

## Related Certifications

**CompTIA CySA+** | **CompTIA Security+** | **GIAC Certified Detection Analyst (GCDA)**

## Further Reading

- NIST SP 800-92: Guide to Log Management
- MITRE ATT&CK
- CISA: Logging Made Easy

## Key Takeaways

- A SIEM centralizes and correlates logs to detect and investigate threats.
- It is a detective and investigative platform, not a preventive block.
- Correlation across sources reveals attacks no single log would show.
- Continuous tuning is essential to fight false positives and alert fatigue.
- Mapping detections to MITRE ATT&CK helps prove real coverage.

## FAQ



## Related Careers

### RELATED ROLES

Soc Analyst | Security Engineer | Threat Hunter

### RELATED CERTIFICATIONS

CompTIA CySA+ | CompTIA Security+ | GIAC Certified Detection Analyst (GCDA)

### CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

### GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

### SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **SIEM**
3. Go deeper: The Security Operations Center (SOC)
4. Go deeper: Threat Hunting
5. Validate it: work toward **CompTIA CySA+**
6. Find the role: browse current openings

### RELATED SHEETS

CS-087 The Security Operations Center (SOC) | CS-088 Threat Hunting | CS-082 Vulnerability Scanning | CS-085 Risk Ratings | CS-001 Cybersecurity