NETWITNESS

EBook

Top Use Case of SIEM for Threat Detection Every Enterprise CISO Should Know

Table of Contents

Introduction

Enterprises generate enormous volumes of log data every day - from network devices, endpoints, cloud workloads, servers, identity systems, and SaaS applications. Collecting this data is necessary, but it is not sufficient. Security teams need to convert raw data into actionable intelligence to detect and respond to threats before they escalate.

Security Information and Event Management (SIEM) solutions serve as more than just log repositories. They aggregate, normalize, and enrich event data to uncover patterns, anomalies, and behaviors that indicate active threats. Properly implemented, SIEM enables organizations to detect attacks early, reduce dwell time, and prioritize responses to events that pose real business risk.

This e-book examines seven critical threat detection use cases where SIEM demonstrates its value: insider threats, cloud attacks, third-party access, lateral movement, compliance-driven monitoring, endpoint-to-network correlation, and integrated behavioral intelligence. Each chapter provides practical workflows, detection logic, and real-world examples that can guide security teams in strengthening their threat detection programs.

The final chapter highlights NetWitness SIEM, showcasing how a modern platform can centralize data, enrich it with intelligence, and streamline investigations. This resource is intended for IT security leads, cybersecurity teams, and decision-makers seeking to transform logs into intelligence with clarity, precision, and confidence.

Chapter 1: Detecting Insider Threats with SIEM

Why Insider Threats Are Critical

Insider threats remain one of the most challenging risks because the actors already have legitimate access. According to the 2023 Ponemon Institute, 60% of organizations reported a rise in insider threat incidents over the past year. These threats include employees, contractors, or even compromised accounts acting maliciously or negligently.

How SIEM Detects Insider Threats

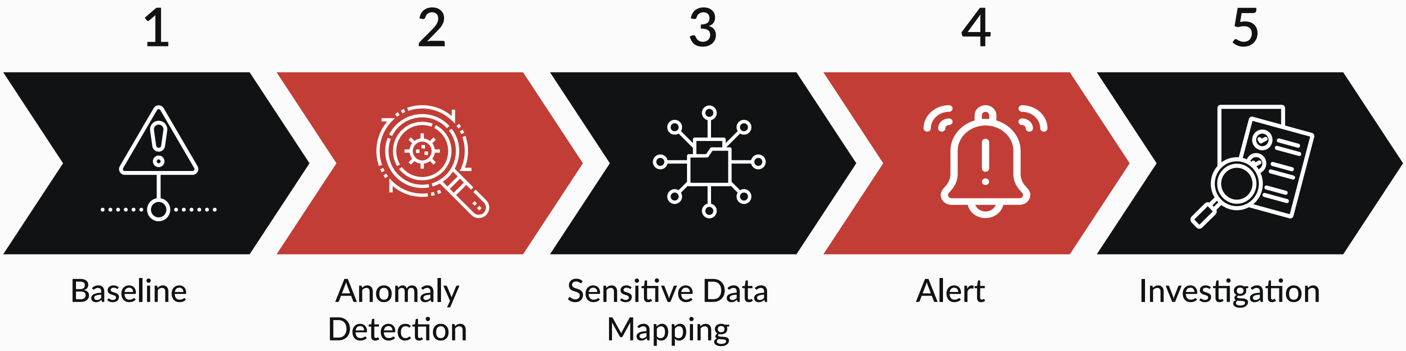
A SIEM identifies suspicious activity by correlating multiple streams of data: authentication logs, endpoint telemetry, file access, and cloud usage. It monitors patterns outside the user's normal behavior, including unusual file downloads, privilege escalation, and access to sensitive resources at odd hours.

Expanded Detection Workflow:

- **Establish a baseline:** Track normal login times, data access patterns, and endpoint usage per user.
- **Detect anomalies:** Trigger alerts when a user accesses files unusually, copies large data sets, or uses dormant privileges.
- **Map to critical assets:** Evaluate whether accessed resources are sensitive or high value.
- **Generate actionable alerts:** Provide full context for each event - who accesses what, when, and from where.
- **Enable investigation:** Include historical trends and connections to other events to quickly assess risk.

Tracking anomalies alone isn't sufficient. Contextual enrichment - combining identity, asset criticality, and behavior trends - is what allows teams to focus on high-risk events.

Insider Threat Detection Process



Chapter 2: Detecting Cloud Infrastructure Attacks with SIEM

Understanding Cloud Complexity

Cloud environments expand the attack surface. Hybrid and multi-cloud deployments introduce numerous identity, API, and configuration vectors. In 2023, 45% of enterprises reported experiencing a cloud security incident. Security teams must detect risks spanning infrastructure, SaaS applications, serverless functions, and container workloads.

How SIEM Monitors the Cloud

Modern SIEM platforms ingest and normalize logs from cloud services like AWS CloudTrail, Azure AD, Google Workspace, and container orchestration platforms. Correlating these logs with identity and network telemetry helps detect anomalies, misconfigurations, and malicious activity.

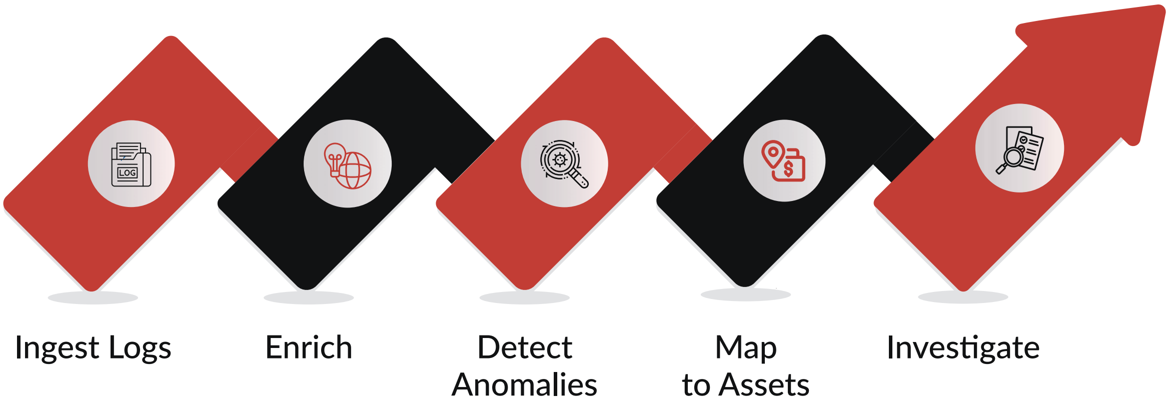
Expanded Detection Workflow:

- **Log ingestion:** Collect events from cloud platforms, firewalls, identity providers, and application logs.
- **Behavioral analysis:** Compare user and service account activity against historical patterns.
- **Detect suspicious activity:** For instance, a new IAM role creation granting broad privileges or a service account accessing sensitive storage from unusual regions.
- **Map to business assets:** Determine which critical applications or data sets could be affected.
- **Alert for investigation:** Provide contextual metadata to facilitate rapid response.

Did You Know?

Enterprises integrating cloud log analytics with identity correlation detect suspicious activity faster than traditional alerting approaches.

Cloud Threat Detection in Five Steps



Chapter 3: Monitoring Third-Party and Supply-Chain Access

The Supply-Chain Risk

External vendors and partners often have privileged access to internal systems. Attackers increasingly target these accounts to infiltrate organizations or move laterally without detection.

How SIEM Protects Against Supply-Chain Threats

A SIEM monitors external account activity across endpoints, cloud services, and network sessions. Alerts are triggered when third-party accounts behave outside normal patterns, such as accessing systems they do not usually touch or downloading sensitive files.

Expanded Detection Workflow:

- **Tag third-party accounts:** Identify and track vendor accounts, roles, and access levels.
- **Session monitoring:** Detect unusual login locations, times, or operations.
- **Lateral movement detection:** Observe if a third-party account accesses multiple systems sequentially.
- **Alert generation:** Provide enriched context for investigation, showing full activity chains.

Treat vendor activity with the same scrutiny as internal users. Even a single anomalous action could indicate compromise or credential misuse.

Chapter 4: Detecting Lateral Movement and Persistent Threats

Understanding Hidden Threats

After initial access, attackers move laterally to escalate privileges, persist, and exfiltrate data. This stage often goes undetected because the activity appears legitimate unless correlated across endpoints and networks.

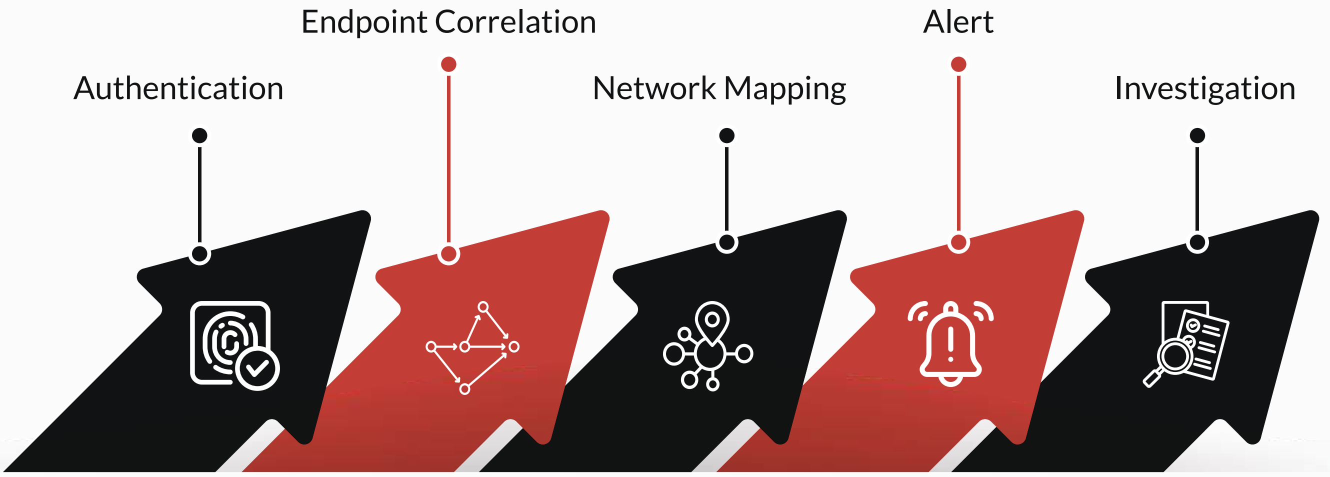
How SIEM Detects Lateral Movement

SIEMs collect and correlate logs from endpoints, networks, and identity systems to identify suspicious patterns, such as multiple credentials uses, unusual session initiation, or anomalous process activity.

Expanded Detection Workflow:

- **Internal authentication monitoring:** Track repeated logins across hosts or systems.
- **Endpoint telemetry correlation:** Identify abnormal process behavior and connections.
- **Network mapping:** Detect unusual traffic patterns, data staging, or unauthorized transfers.
- **Alert generation:** Create high-fidelity alerts combining identity, endpoint, and network data.

Lateral Movement Detection Workflow



Chapter 5: Compliance-Driven Threat Detection Use Cases

Beyond Meeting Requirements

Regulatory frameworks such as PCI-DSS, HIPAA, and SOX generate logs that, when integrated into SIEM workflows, serve as early threat detection signals. Organizations leveraging compliance logs for real-time detection reduce breach costs by up to 24% (Ponemon, 2023).

How SIEM Enhances Compliance Detection

SIEMs ingest audit-relevant logs, correlate events across assets and identities, and flag anomalies. Real-time monitoring prevents unauthorized activity and enables proactive intervention.

Expanded Detection Workflow:

- **Collect compliance logs:** Include privileged access, configuration changes, and system audits.
- **Rule-based monitoring:** Detect violations of access policies or procedural requirements.
- **Contextual correlation:** Combine identity, asset sensitivity, and historical activity.
- **Alert escalation:** Provide detailed evidence for rapid investigation and remediation.

Compliance logs are not just for auditors; they can be a powerful source of threat detection intelligence when correlated with real-time events.

Chapter 6: Endpoint-to-Network Correlation for Threat Detection

Why Correlation Matters

Attackers rarely limit activity to either endpoints or the network. Detection requires correlating events across both domains. Organizations combining endpoint and network telemetry reduce detection times by nearly 50% (Gartner, 2023).

How SIEM Enables Correlation

SIEM platforms collect endpoint events, network flows, and identity activity to detect anomalies like unusual processes initiating external connections. Correlation improves alert accuracy and reduces analyst fatigue.

Expanded Detection Workflow:

- **Endpoint monitoring:** Capture process activity, file access, and registry changes.
- **Network monitoring:** Collect flow data, firewall logs, and packet metadata.
- **Correlation:** Detect anomalies that span both domains.
- **Alerting:** Provide a full activity chain from process initiation to network connection.

Did You Know?

Endpoint-network correlation enables analysts to trace the entire attack sequence in one investigation, reducing dwell time significantly.

Chapter 7: Advanced Threat Detection with NetWitness SIEM

The Growing Complexity of Enterprise Threats

Modern cyberattacks are stealthy, distributed, and increasingly automated. They exploit blind spots between security tools and thrive in environments where data is siloed. Traditional SIEMs often struggle to connect fragmented logs into a coherent story, which delays detection and overwhelms analysts with noise.

This is where NetWitness SIEM redefines what effective threat detection looks like. It doesn't just collect data, it understands it - providing visibility, correlation, and context that transforms scattered events into actionable intelligence.

How NetWitness SIEM Enhances Threat Detection

1. Unified Data Visibility

By consolidating data from endpoints, networks, cloud platforms, and identity systems, NetWitness provides a full picture of enterprise activity.

- Collects and normalizes logs in real-time from diverse sources.
- Eliminates silos by mapping relationships between users, hosts, and applications.
- Helps analysts identify suspicious behavior faster through contextualized views.

2. Contextual and Correlated Alerts

Instead of flooding teams with false positives, NetWitness focuses on high-fidelity alerts enriched with context.

- Correlates events across domains to detect hidden attack patterns.
- Prioritizes alerts based on business impact and severity.
- Uses behavioral analytics and threat intelligence to minimize alert fatigue.

3. Streamlined Investigation Workflow

The investigation-centric interface makes it easy to reconstruct an incident from the first alert to full remediation.

- Presents a unified timeline connecting user sessions, devices, and network activity.
- Allows pivoting directly between related entities for faster root cause analysis.
- Cuts down manual effort and improve response accuracy.

4. Adaptive and Scalable Design

As environments evolve, NetWitness scales seamlessly.

- Integrates new data sources quickly without complex reconfiguration.
- Adapts to on-prem, cloud, and hybrid infrastructures.
- Supports continuous monitoring across distributed architectures.

NetWitness Detection Framework

Stage	Purpose	What NetWitness Does
Data Ingestion	Gather logs and telemetry	Ingests from endpoints, networks, cloud, and identity systems
Normalization	Make data readable and usable	Parses and standardizes events in real-time
Correlation	Connect related events	Maps relationships across systems to detect attack patterns
Alerting	Prioritize threats	Generates high-fidelity alerts with business context
Investigation & Response	Resolve faster	Gives analysts the full picture for root cause analysis

Why It Matters

With NetWitness SIEM, detection becomes proactive rather than reactive. It transforms overwhelming data volumes into meaningful insights, helping analysts not only see attacks but understand them in context, which is what truly drives faster containment and stronger resilience.

About Netwitness

Founded in 1997, NetWitness is a leader in threat detection & cyber security monitoring. The NetWitness platform combines visibility, analytics, and automation into a single solution allowing customers to prioritize, respond, reconstruct, survey, investigate and confirm information about the threats in their environment and take the appropriate response—quickly and precisely.