

Security Information and Event Management (SIEM)

Detect what matters, investigate holistically, and respond rapidly.



Today's threat landscape presents significant challenges for security teams. Analyzing data noise, trying to gain visibility across hybrid, cloud, and on-prem environments, while being inundated with a vast amount of data from various security and IT sources can become overwhelming. It's difficult to prioritize major vulnerabilities before they escalate, while addressing minor security issues at the same time. Turning volumes of raw data into actionable insights is key.

Lack of context makes threat detection even harder. According to the SANS Institute 2025 SOC Survey, [the main challenge to a security operations center \(SOC\) is the immense lack of context related to security events](#). With the large number of alerts that analysts must take action on, it can be difficult to distinguish high-priority threats without it. Plus, an estimated average of 41% of alerts are ignored because analysts don't have the bandwidth.

Security teams are also burdened with managing up to 25+ different security tools for actions across detection, investigation, and response. As a result, analysts spend an average of three hours on alert investigations. Today's risks include detecting sophisticated AI-driven threat campaigns that operate at machine speed, as well as ensuring compliance with evolving regulations across geographies.

A modern security information and event management (SIEM) solution that delivers unified workflows, AI-powered analytics, and the ability to combat threats and mitigate risk at scale is the answer.

This shift requires a new operating model: the Agentic SOC — an integrated system bringing together data, analytics, tooling, and AI for the analyst to continuously adapt and conquer unprecedented challenges. An Agentic SOC sets a new baseline for what it means to be truly secure and catalyze innovation.

This essential guide explores what a SIEM solution is, what it does, and how to find the right SIEM for your organization.

What is a SIEM?

A SIEM solution is like a pilot's radar system. Security analysts steer the security operation center and need a radar to safely navigate what's around them, what's ahead of them and what might be hidden out of view. A SIEM solution is a security platform that helps SOC analysts see across enterprise IT so they can spot security threats hiding in the corners of the systems they protect. Without it, they're flying blind.

While security applications, network security and system software can catch and log isolated attacks and anomalous behavior, today's most serious threats are distributed and can't be caught with these tools alone. Hackers attack in unison across multiple systems and use advanced evasion techniques to avoid detection. Attackers also take advantage of stressful situations to exploit weaknesses — such as an immediate shift to remote work during a global pandemic. In that example, SOC teams were tasked with keeping systems secure, but without in-person access to the security tools and processes they'd come to rely on.

Situations like these are why a modern SIEM solution is more important than ever. Without the right SIEM, cyberattacks can fester and turn into catastrophic incidents that even the best SOC analysts can't see coming. And by the time they discover a vulnerability, like a ransomware attack, all that's left to do is damage control.

What does a SIEM do?

Gartner defines a SIEM solution as a tool that “aggregates the event data that is produced by monitoring, assessment, detection, and response solutions deployed across application, network, endpoint, and cloud environments.”

A SIEM solution helps SOC analysts work smarter. It ingests event logs and provides a single view of their data, with more insight and visibility into their security posture.

A modern SIEM can solve three major security challenges:

- Analyzing data noise
- Lack of contextualized threat detection
- Security and threat complexity

So how do organizations solve those challenges today without a SIEM solution? Historically, they’ve used “traditional” solutions, various point solutions or even built their own, which takes time, money and resources.

How traditional SIEMs fall short

Traditional SIEMs typically have dated architectures that use an SQL database with a fixed schema. These databases can become a single point of failure or suffer from scale and performance limitations.

Lack of unified visibility

The inability to seamlessly ingest, normalize, and analyze data from any source limits a traditional SIEM's detection, investigation, and response times. Additionally, the data ingestion can be a massively laborious process or very expensive.

Inability to reduce alert volumes

Traditional SIEMs cannot decrease the volumes of alerts analysts address. In fact, they often bring more alerts and false positives, causing an increased workload and noise that makes it more difficult to discern high-priority threats.

Inadequate out-of-the-box detections

Security analysts must have access to top-tier detections that can be integrated into the SOC to find and remediate threats faster.

Limited deployment

Traditional SIEMs are often limited to on-premises or cloud deployments. Security practitioners must have the flexibility to use cloud, multi-cloud, on-premises, or hybrid environments.

Little or no unification of workflows

Analysts must act fast to address security incidents, but having multiple tools across detection, investigation, and response slows them down.

Closed ecosystem

Traditional SIEM solutions often lack the ability to integrate with other tools. Customers are forced to use what’s included in the existing SIEM or spend more on custom development and professional services.

Lack of embedded AI and automation

Traditional SIEMs lack AI-driven agents that can assist analysts throughout their workflow. Without embedded automation and agentic capabilities, analysts remain burdened by manual tasks and cannot operate at the speed required to counter modern threats.

Five essential SIEM capabilities for the AI era

1. High-fidelity data visibility across your environment

SOC leaders need complete visibility without runaway cost. A modern SIEM should cover cloud, on-premises, and hybrid environments using an open data fabric with strong data management, advanced pipelines, and flexible federation. Cost controls and tiering help scale coverage while keeping budgets predictable and investigations complete.

2. Purpose-built security analytics and detections

Reduce exposure by improving detection quality and coverage. Look for detections aligned to MITRE ATT&CK, strong correlation, and built-in detection engineering to close gaps quickly. Native behavioral analytics (UEBA) and integrated threat intelligence add context so analysts can make faster decisions with higher confidence.

3. Risk-based alerting and prioritization

Burnout and missed threats often start with poor prioritization. A modern SIEM should reduce noise by correlating signals and elevating high-fidelity findings using risk-based approaches. This improves true positive rates, focuses analysts on what matters most, and standardizes triage across the team.

4. Investigation and forensics experience

Improve mean-time-to-respond (MTTR) by speeding investigations and preserving context. A modern SIEM should provide fast search, flexible pivoting across sources, and investigation views that help analysts understand scope, relationships, and timelines quickly. Clear workflows and strong visualizations reduce handoffs and shorten the time to reach confident decisions.

5. Unified response workflows and automation

Consistency at scale requires unified response. Look for workflows that bring detection, investigation, response, and case management into one experience. Embedded automation, playbooks, and human-led AI assistance reduce manual steps, improve repeatability, and help teams execute response faster while keeping analysts in control.

Common use cases for SIEM

A modern SIEM helps teams search, monitor, and investigate events. It provides visibility across your entire environment for accurate threat detection and a more resilient organization. Security teams can achieve impactful results using workflows for:

Security monitoring

Real-time security monitoring ensures that threats are being detected, investigated, and analyzed for faster response. Ingest data from any source to gain end-to-end visibility across your environment and to make better, data-centric decisions to reduce risk. Enhance your attack surface coverage to include on-premises, hybrid, and multi-cloud environments.

Incident management

Determine root cause and easily search for evidence of an incident using fast, flexible search and reporting. This supports analysts throughout an investigation — from incident identification and detection through post-incident analysis. Asset and risk intelligence provides security analysts with the context of the system and user to quickly determine the who, what, and when during security investigations. This helps security teams save hours of effort and drive more complete and thorough investigations.

Compliance

Collect, search, monitor, and analyze data using a centralized solution to meet compliance requirements, and quickly identify your organizational gaps against regulations with automated compliance tasks and customized reports to ease the burden of audits. Insight across resources and security controls helps clear compliance and pass audits with minimal effort, regardless of mandate or regulatory framework. The SOC can meet increasingly complex compliance requirements using capabilities such as monitoring, reviewing, and retaining logs or generating ad-hoc reports to address auditor questions.

Splunk: a unified, AI-powered SecOps platform

As a next-generation SIEM and market leader for the 11th consecutive time in Gartner's Magic Quadrant, as well as the number one ranking vendor in Gartner's Critical Capabilities for OOTB, SIEM, Customizable SIEM, and TDIR. Per IDC's SIEM market share reports, Splunk helps organizations modernize security operations for today's threat landscape. Built to power the Agentic SOC, Splunk Enterprise Security brings together data, analytics, tooling, and AI to help analysts move faster with greater confidence across threat detection, investigation, and response.

Powered by an extensible platform with embedded, human-led AI, Splunk ES Premier delivers comprehensive visibility across cloud, on-premises, and hybrid environments through advanced data management and federation. It unifies SIEM, SOAR, UEBA, threat intelligence, and detection engineering into a single experience, including native UEBA, Detection Studio, and integrated Cisco Talos threat intelligence, with coordinated workflows and embedded case management. The result is a unified, AI-powered SecOps platform that reduces friction, improves response consistency, and helps teams act decisively without constant context switching.

Realize comprehensive visibility (data)

Security teams are in a tough spot, trying to gain visibility across hybrid cloud and on-premises, incorporating both operational technology (OT) and IT environments, being flooded with overwhelming amounts of data from different security, IT, and other business sources. More than chasing down every security hiccup, reducing exposure and mitigating threats before they cause material damage must be the priority. In this digital whirlwind, security teams lack a single platform to transform raw data from any source into actionable insights.

Splunk's data-powered platform provides an open data fabric with advanced data management and federation, delivering comprehensive visibility across cloud, on-premises, and hybrid environments. It supports pre-built integrations, cost controls, robust data management, and advanced data pipelines, helping teams work with their data wherever it lives. Analysts can use fast, flexible search to investigate across sources, and use Splunk AI Assistant to translate searches into SPL to save time. Teams can operationalize data with flexible alerting configured at different levels of granularity, based on conditions such as data thresholds and trend-based signals.

Splunk Enterprise Security supports cost-effective data optimization by ingesting only the data critical to security use cases. Users have the flexibility to store and access their data, including at the edge, based on data tiering. This reduces forensics and compliance storage costs for added savings.



Empower accurate detection with context (analytics)

Security analysts often face a lack of context when navigating threats. With risk-based alerting (RBA), analysts can focus on high-fidelity alerts built from quality detections, increasing productivity and improving true positive rates. In many environments, this approach can reduce alert volume by 50% to 90%, with the remaining alerts easier to investigate because they are grounded in aggregated risk.

RBA uses the Splunk Enterprise Security correlation search framework to collect risk events into a single risk index. When risk events meet defined criteria, they generate a single risk notable, helping analysts stay focused on the threats that matter most, including attacker activity that traditional, rule-only SIEM approaches may miss.

Analysts can also apply an RBA detection strategy to create high-confidence, aggregated findings for investigation. This aggregate view, based on predetermined grouping techniques and calculations, brings related signals together so analysts can review the full story in one place and act faster.

With Splunk Enterprise Security, teams gain additional insight into risk through customizable dashboards, visualizations, and reports. For example, you can operationalize the MITRE ATT&CK framework with a visualization matrix that highlights observed tactics and techniques, or use the Threat Topology visualization to understand scope and relationships during an investigation. With enhanced risk analysis dashboards, analysts can monitor user and entity risk events across RBA and behavioral analytics to prioritize response with greater confidence.

Fuel operational efficiency (tooling + AI and automation)

Between overwhelming data and alert volumes, a multitude of tools, and expanding compliance requirements, security teams have a lot to manage while defending against the full spectrum of risk, including AI-enabled threat campaigns. Splunk Enterprise Security helps strengthen digital resilience by unifying threat detection, investigation, and response (TDIR) so teams can reduce manual effort, maintain context, and respond faster.

With TDIR, security teams get an end-to-end view of security posture within a single, unified platform. Mission Control helps unify workflows across detection, investigation, and response, while embedded case management supports consistent execution from initial triage through closure. Coupled with SOAR capabilities integrated into the workflow, automated playbooks can be infused with threat intelligence to streamline security operations center processes and reduce pivoting between tools. Automation rules can assign playbooks to specific detections so playbooks run automatically when findings are generated, improving consistency and helping teams scale response.

Analysts can detect, investigate, and respond from one modern interface, increasing operational efficiency with a unified solution for data aggregation, analysis, and automation. Embedded, human-led AI further accelerates common tasks by helping analysts summarize findings, generate SPL, and speed investigation steps while keeping every action transparent and under analyst control. Response plans in Splunk Enterprise Security also support collaboration and execution of repeatable incident response workflows for common security use cases.

SIEM evaluation checklist

High-fidelity data visibility across your environment

SOC leaders need complete visibility without runaway cost. A modern SIEM should cover cloud, on-premises, and hybrid environments using an open data fabric with strong data management, advanced pipelines, and flexible federation. Cost controls and tiering help scale coverage while keeping budgets predictable and investigations complete. This data foundation is essential for an Agentic SOC, because AI-driven agents are only as effective as the quality, accessibility, and context of the data they can operate on.

What to look for:

- Broad, maintained integrations across security, IT, cloud, and identity sources
- Normalization and enrichment that improves search and correlation quality
- Federation options to query data where it resides when centralizing is impractical
- Data routing, filtering, masking, and tiering to control ingest and storage costs
- Support for hybrid deployments and long-term retention needs

Conclusion: If your data foundation is incomplete or too expensive to scale, everything downstream in the SOC suffers.

Purpose-built security analytics and detections

Reduce exposure by improving detection quality and coverage. Look for detections aligned to MITRE ATT&CK, strong correlation, and built-in detection engineering to close gaps quickly. Native behavioral analytics (UEBA) and integrated threat intelligence add context so analysts can make faster decisions with higher confidence.

What to look for:

- Curated detection content mapped to frameworks like MITRE ATT&CK
- A full detection lifecycle (author, test, tune, deploy, monitor)
- Correlation and risk scoring to reduce false positives and increase fidelity
- Native UEBA to identify abnormal user, device, and app behavior
- Threat intelligence ingestion and enrichment embedded in detection workflows

Conclusion: Strong analytics are measured by fewer, higher-confidence findings and faster coverage against new attacker behaviors.

Risk-based alerting and prioritization

Burnout and missed threats often start with poor prioritization. A modern SIEM should reduce noise by correlating signals and elevating high-fidelity findings using risk-based approaches. This improves true positive rates, focuses analysts on what matters most, and standardizes triage across the team.

What to look for:

- A risk model that aggregates related signals into prioritized findings
- Consistent scoring that incorporates user, asset, and threat context
- Clear explainability for why something is prioritized
- Tuning workflows that make it easy to reduce noise over time
- Metrics and reporting for alert reduction and investigation efficiency

Conclusion: Prioritization is how a SOC scales, because it protects analyst time for the threats that truly matter.

Investigation and forensics experience

Improve MTTR by speeding investigations and preserving context. A modern SIEM should provide fast search, flexible pivoting across sources, and investigation views that help analysts understand scope, relationships, and timelines quickly. Clear workflows and strong visualizations reduce handoffs and shorten time to confident decisions.

What to look for:

- Fast search and pivoting across multiple data sources and time ranges
- Investigation views that maintain context from alert to root cause
- Entity-centric investigation (users, hosts, IPs, identities, cloud resources)
- Visualizations for timelines, relationships, and scope
- Reporting that supports audits, post-incident reviews, and executive visibility

Conclusion: The best SIEM investigations reduce guesswork and get analysts to root cause faster, with fewer tool switches.

Unified response workflows and automation

Consistency at scale requires unified response. Look for workflows that bring detection, investigation, response, and case management into one experience. Embedded automation, playbooks, and human-led AI assistance reduce manual steps, improve repeatability, and help teams execute response faster while keeping analysts in control.

What to look for:

- Embedded case management and collaboration (assignments, evidence, notes)
- SOAR playbooks integrated into incident workflows, not bolted on
- Automation triggers tied to detections and risk thresholds
- Integrations with key security tools for containment and remediation actions
- Human-led AI assistants that are transparent, auditable, and controllable

Conclusion: Unified response turns detection into outcomes by making fast, consistent action repeatable across the SOC.



Get started.

Are you ready to learn more about how a market-leading SIEM can help modernize your SOC? Discover how [Splunk Enterprise Security](#) can help.



Splunk, Splunk>, Data-to-Everything, and Turn Data Into Doing are trademarks or registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2026 Splunk LLC. All rights reserved.

26_CMP_essential_Essential-guide-to-SIEM_v6

