Top 5 Use Cases for Splunk Enterprise Security

splunk> a CISCO company | PRESIDIO

It's not easy to detect and respond to security events quickly. A security analyst can spend minutes (if not days) on an alert. Now, multiply that by thousands of security alerts, and you're left with too many tickets, and too few analysts. Starting to see the problem?

We need to help security teams speed up their response times while reducing the number of alerts they get. We can start by improving visibility into their environment, so they can detect and respond to threats faster. Better yet, an automated response to alert triage can turn minutes into seconds and hours into minutes.

This gives hard-to-detect, insidious threats like malware fewer places to hide and propagate, and reduces the amount of damage they can cause — meaning stressed out security analysts become that much happier.

Bottom line? Analysts need fewer alerts, and require a smarter, unified way to work. That means accelerating investigations with AI-powered agents and unlocking full visibility across cloud, on-prem, and hybrid environments. With the right solution, security teams can reduce alert volume by up to 80%, supercharge analyst productivity, and respond to events with confidence.

That's where a market-leading security information and event management (SIEM) solution like Splunk Enterprise Security (ES) can help. Splunk ES is the premiere AI-powered SecOps platform — unifying SIEM; security orchestration, automation, and response (SOAR); user entity and behavior analytics (UEBA); threat intelligence; and detection engineering with embedded AI across the threat detection, investigation, and response (TDIR) workflow.

The result? Faster outcomes, reduced risk, and increased resilience for the agentic AI era. In this quick guide, we'll walk through five of the top use cases customers rely on Splunk and Presidio to solve. From eliminating alert fatigue to unifying visibility and scaling automation, these examples showcase how security teams can hit the ground running, wherever they are in their security journey.

1. Cut through alert fatigue with risk-based alerting and agentic AI

Most security operations centers (SOCs) are buried in alerts consisting of false positives, duplicate signals, and endless noise that obscure very real threats. Analysts are often forced to pivot across tools and chase dead ends until burnout sets in.

Splunk ES eliminates the manual toil that slows analysts down with risk-based alerting — this works by attributing risk to users and entities, subsequently triggering an alert once certain risk and behavioral thresholds are exceeded, cutting false positives by 80%.

This helps SOCs optimize threat detection by reducing the volume of alerts — thereby increasing true positives — while helping surface more sophisticated threats like low and slow attacks that most correlation searches traditionally miss. This also frees up time and resources to home in on actual (often complex) threats and align operations to industry-standard cybersecurity frameworks.

Layer in agentic AI, and suddenly the noise becomes much more manageable. Agentic AI marks the next stage in security automation, where AI doesn't just assist analysts, but also acts on their behalf. Analysts regain focus, investigations accelerate, and teams scale effectively without hiring armies of responders. By embedding AI into modern SOAR solutions, organizations can automate repetitive tasks, enrich alerts in real time, and accelerate the entire TDIR workflow.

All in all, AI-driven automation analyzes massive volumes of telemetry in seconds, prioritizes alerts by risk score, recommends steps to remediation, and orchestrates workflows across multiple tools — dramatically reducing mean time to detect (MTTD) and respond (MTTR).

Among organizations that have adopted AI, 59% say it has moderately or significantly boosted their SOC efficiency.

Source: Splunk, State of Security, 2025

2. Unlock full-fidelity visibility of your data

The shift to cloud has brought flexibility, but it's also created sprawling, siloed data environments. Security teams face an impossible tradeoff: duplicate storage at skyrocketing costs or live with dangerous blind spots across AWS, Azure, GCP, SaaS, and on-prem. Splunk ES eliminates these gaps and allows security teams to route, tier, and access data flexibly, while correlating telemetry across hybrid and multicloud deployments in one unified platform. This means complete visibility, lower total cost of ownership (TCO), and the agility to adapt as the business changes — whether it's M&A, new applications, or evolving infrastructure. Splunk future-proofs your SOC, delivering the confidence that every signal is visible, contextualized, and actionable.

Organizations that use a unified security platform report faster incident response (59%), less time maintaining tools (53%), and better threat coverage (49%).

Source: Splunk, State of Security, 2025

3. Accelerate investigations with AI-driven workflows

Investigations often stall under the weight of disconnected tools and manual workflows. Analysts waste time piecing together evidence, writing queries from scratch, and drafting reports while attackers continue to move through the system. Splunk ES transforms the process with AI embedded directly into the TDIR workflow.

Analysts can use plain language to generate complex search processing language (SPL) searches, automatically summarize findings, and even receive recommendations for next steps. At the same time, integrated case management keeps notes, files, and threat intel in one place — so context is never lost and handoffs are seamless. What once took days now takes minutes. Analysts ramp faster, documentation becomes consistent, and the SOC gains clarity and speed exactly when it's needed most.

In the future, AI will become an integral part of the security analyst experience. AI can enable self-healing systems to detect and mitigate malicious behavior in real time. Imagine what that technology could do once it's embedded in the SOC.

Tamara Chacon
Security Strategist, Splunk SURGe

4. Get SOC-wide automation and contextual enrichment

In many SOCs, automation is powerful but limited — confined to senior responders who can manage complex SOAR deployments. Everyone else is left with manual toil, creating bottlenecks and burnout. Splunk Enterprise Security Premier changes that by embedding SOAR natively into ES, putting automation in the hands of every analyst.

With AI playbook authoring, anyone can describe a workflow in natural language and have Splunk translate it into a tested, executable playbook. And with autonomous response agents, the platform can contain threats instantly while keeping humans in the loop. This democratizes automation across the SOC, standardizing response, accelerating containment, and empowering each and every analyst to contribute. The result: consistent, fast response at scale, with less manual grind and a stronger security posture.

Automated security tools can take phishing emails, run them against threat feeds, use these results to create a score, and use that score to either quarantine, block, or report the email. They can work faster than any human.

Kirsty Paine
Field CTO and Strategic Advisor, EMEA, Splunk

5. Close detection gaps for faster mean time to detect

Threat actors never stop evolving, and all too often, detection coverage can't keep pace. Most SOCs don't have a clear picture of which tactics they can defend against, leaving blind spots where threats loom large. Splunk Enterprise Security provides the visibility and precision needed to stay ahead.

Detection studio delivers a full detection engineering lifecycle, enabling SOCs to test, deploy, and monitor high-fidelity detections with confidence. Real-time MITRE ATT&CK mapping shows exactly where coverage is strong and where it needs reinforcement, while curated content from the Splunk Threat Research Team (STRT) and Cisco Talos ensures detections stay up-to-date against emerging tactics, techniques, and procedures (TTPs). This looks like a SOC that proactively closes gaps, bolsters coverage, and reduces the risk of unseen attacks, rather than reacts to adversaries a little too late.

Detection engineering is ranked in the top three skills for a future-ready SOC by 74% of respondents, yet 41% report a detection engineering skills gap.

Source: Splunk, State of Security, 2025

Ready to drop your breaches with a cloud-based, analytics-driven SIEM solution?

Learn how Splunk and Presidio help organizations from strategy to deployment.

Contact our team at SplunkSolutions@Presidio.com to learn more.

splunk> a cisco company | PRESIDIO®

Learn more: www.splunk.com/asksales

www.Presidio.com