Essential Guide

Security Information and Event Management (SIEM)

Detect what matters, investigate holistically and respond rapidly.

splunk> | data SOLUTIONS

Today's threat landscape poses significant challenges for security teams. Analyzing data noise, trying to gain visibility across hybrid, cloud and on-premises environments, while being inundated with vast amounts 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 2023 SOC Survey, the primary obstacle to a SOC's success 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 challenging 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. Risks today include detecting sophisticated AI-driven threat campaigns, as well as ensuring compliance with evolving regulations across geographies.

All of this makes it difficult for organizations to draw insights from and take action on their data — it's too time consuming and resource intensive. A security information event management (SIEM) solution that allows you to access data-driven insights, combat threats, mitigate risk at scale and includes ML-powered analytics you can act on is the answer.

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 (SOC) and need radar to safely navigate what's around them, what's ahead and what might be hidden out of view. A SIEM solution is a security platform that helps SOC analysts see across enterprise IT and 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 one 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 a 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.

Five essential SIEM capabilities

1. Scalable, real-time security monitoring and analytics

SOC success demands a platform that can transform raw data into actionable insights. The ability to ingest, normalize and analyze data from any enterprise source ensures analysts have the visibility to find threats before they cause costly damage to the organization. Whether deployed on-premise, in the cloud or hybrid, the SIEM must offer continuous monitoring and correlation across security tools at scale.

2. Curated detections

Out-of-the box detections that align to widely-used industry frameworks enable analysts to detect and identify threats within their networks. This provides the support they need to address sensitive threats, as well as context around varying tactics, techniques and procedures (TTPs) observed.

3. Alert prioritization

When it comes to alert triage, alert prioritization is a SOC analyst's best friend. It addresses the ongoing struggle of alert overload by ensuring analysts know which events need attention fast. The context around incident severity ensures that analysts are investigating what matters most instead of wasting time on false positives.

4. Visualizations and dashboards

Intuitive, visually-compelling dashboards that provide full environment visibility improve incident investigation and response to keep an organization's security posture up-to-date. They increase productivity and reduce mean time to response (MTTR) by providing a more comprehensive view of security incidents and severity levels.

5. Unify threat detection, investigation and response

Coordinated workflows across detection, investigation and response facilitate repeatable, automated SOC processes and battle overwhelming data volumes, alert storms and manual tasks.

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 visibility into the security posture improves decision-making and reduces risk. It ensures that threats are being detected, investigated and analyzed for faster response.

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.

Compliance

Insight across all IT/OT 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.

Enter Splunk

Splunk has paved the way in advancing SIEM and security analytics. Our innovations have helped thousands of customers outpace adversaries. As an industry-defining SIEM and security analytics solution provider, only Splunk has been named a leader by multiple analysts, earning the distinction of a **hat trick**.

Splunk Enterprise Security (ES) is the trusted choice for SOCs around the globe. Its powerful capabilities deliver comprehensive visibility, empower accurate detection with context and fuel operational efficiency. Powered by an extensible platform and assistive AI-driven capabilities, Splunk ES ensures analytics at scale for continuous security monitoring and cost-effective data optimization. With this foundation, you can detect what matters, investigate holistically and respond rapidly.

Realize comprehensive visibility

Security teams are in a tough spot, trying to gain visibility across hybrid cloud and on-premises, incorporating both 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 with assistive AI capabilities offers unmatched, comprehensive visibility by seamlessly ingesting, normalizing and analyzing data from any source at scale. It offers continuous monitoring and correlation across security tools regardless of deployment — on-premises, cloud or hybrid — to help maximize attack-surface coverage. Find threats with comprehensive search and use Splunk AI Assistant to translate searches into SPL to save time. Splunk's custom alert actions feature makes it simple to take fast action. These custom alerts can be set to varying levels of granularity based on a variety of conditions, such as data thresholds, trend-based conditions and behavioral pattern recognition like brute force attacks and fraud scenarios.

Splunk Enterprise Security ensures cost-effective data optimization by ingesting only 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.

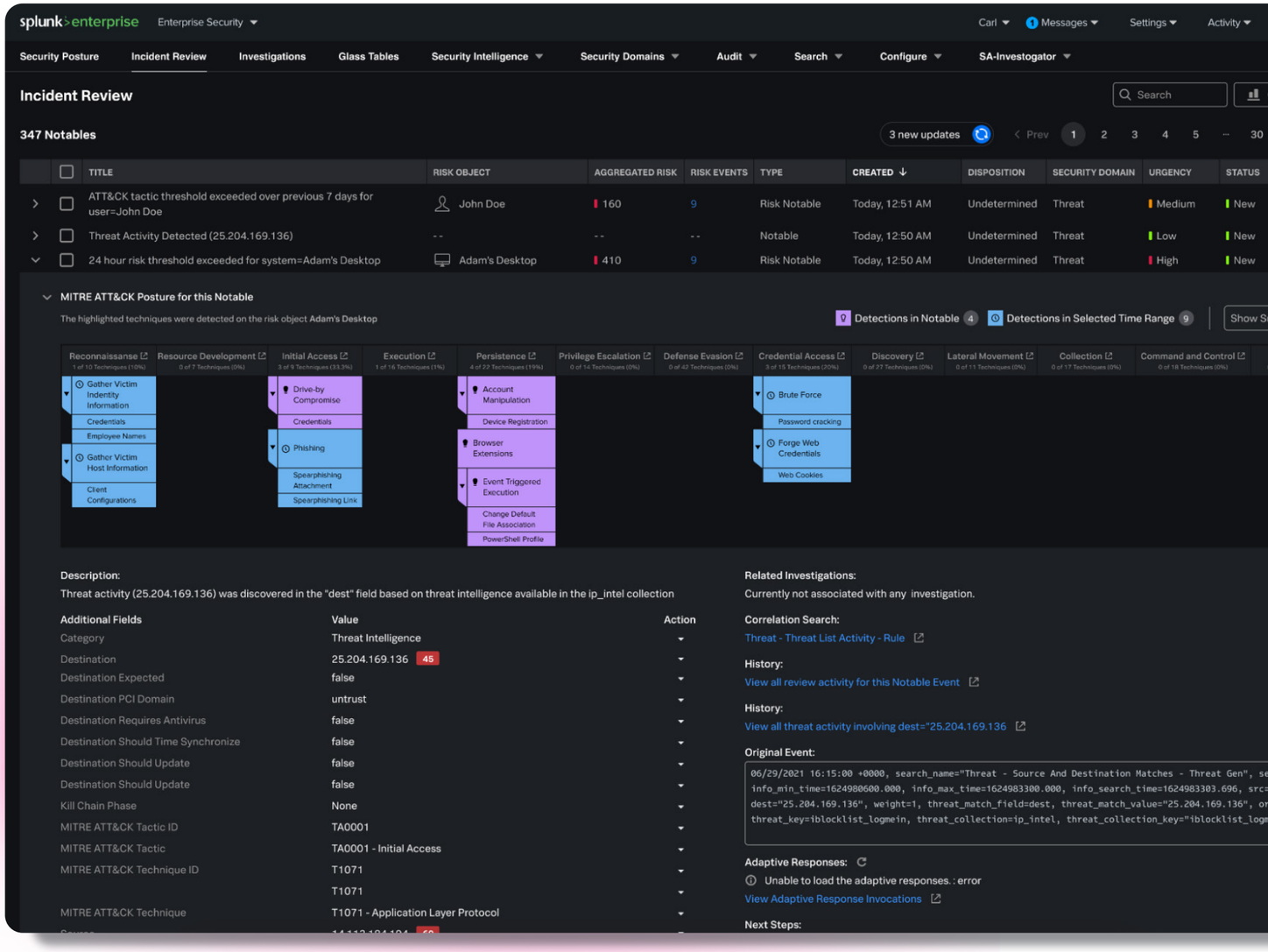
Empower accurate detection with context

Security leaders find themselves besieged by a pervasive lack of context when navigating the nebulous activity of threat detection.

Risk-based alerting (RBA) within Splunk Enterprise Security drastically reduces alert volumes by up to 90%. RBA uses the Splunk Enterprise Security correlation search framework to collect risk events into a single risk index. Events collected in the risk index create a single risk notable when they meet a specific criterion, so you can stay focused on imminent threats that traditional SIEM solutions might miss. This boosts productivity and ensures the threats you're detecting are high fidelity.

The Splunk Threat Research Team (STRT) delves deep into detection engineering, providing you with 1,500+ out-of-the-box detections so you can find and remediate threats faster. These detections align to industry frameworks like MITRE ATT&CK, NIST CSF 2.0 and Cyber Kill Chain®. Splunk also provides a machine learning toolkit (MLTK) to accelerate your ability to uncover threats with anomaly detection.

With Splunk Enterprise Security, you can enhance your security program with customizable dashboards, visualizations and reports. For example, you could operationalize the MITRE ATT&CK framework with a visualization matrix that highlights the tactics and techniques observed in risk events to save time when investigating. Or, you could discover the scope of an incident and respond accurately using the Threat Topology visualization. With the enhanced risk analysis dashboard, security analysts can monitor user entity risk events from detections across RBA and behavioral analytics.



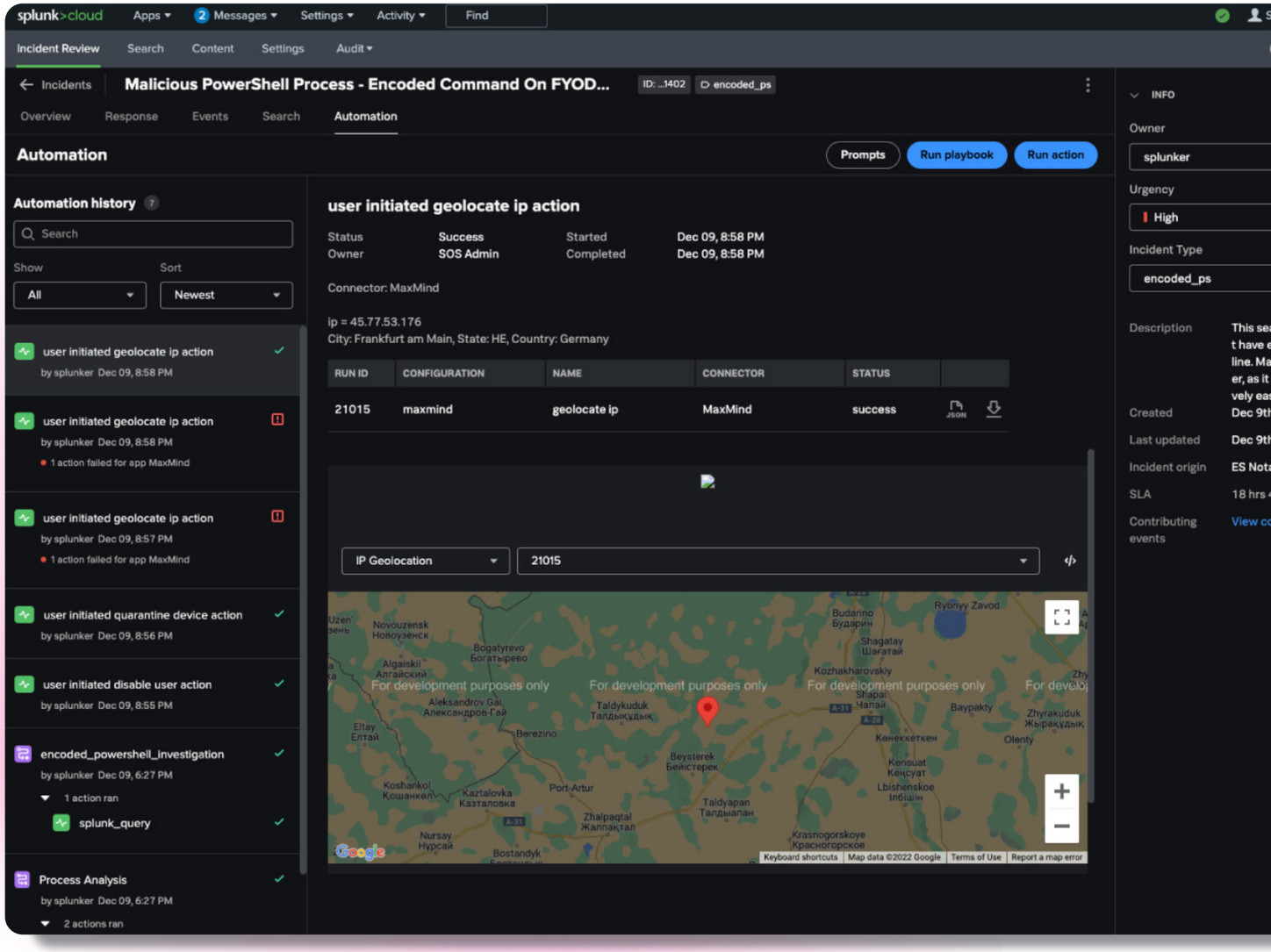
Fuel Operational Efficiency

Between overwhelming data and alert volumes, a multitude of tools and the burdens of regulatory compliance requirements, security teams have a lot to deal with while defending the organization from the full spectrum of risk, including AI-enabled threat campaigns.

Mission Control is an integral feature of Splunk Enterprise Security that unifies workflows across detection, investigation and response. Coupled with Splunk's leading SOAR solution, automated playbooks are infused with threat intelligence to streamline SOC processes and reduce manual effort and pivoting between disparate tools. With a unified platform for data aggregation, analysis and automation, operational efficiencies increase dramatically.

Plus, our vendor neutral approach lets you solve any number of use cases by building custom apps or leveraging our expansive community and partner ecosystem of 2,200+ partners and 2,800+ apps on Splunkbase. Collect, search, monitor and analyze data to meet increasingly complex compliance requirements. And with streamlined log management and specialized capabilities like the Splunk App for PCI Compliance, you can do it quickly.

Strengthen digital resilience and advance your SOC with unified threat detection, investigation and response. As the industry leader in security operations solutions, Splunk is at the heart of the modern SOC — providing the breadth of technologies, community and expertise for efficient and effective security at scale. Detect threats accurately, investigate holistically with security and IT context and automate response to proactively address risk with Splunk.



Get Started.

Are you ready to learn more about how an industry-defining SIEM can help modernize your SOC? Speak with a Splunk expert now.

splunk> | data SOLUTIONS

23-433250-Splunk-The Essential Guide to SIEM-EB-106