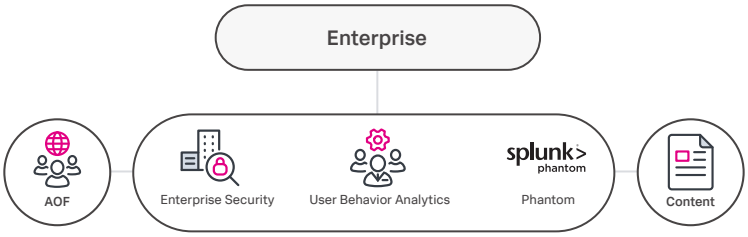
Splunk Security Operations

- Increase your threat detection, investigation and response capabilities
- Reduce your organization's exposure to risk
- Increase the return on your security operations investments



Security teams are hard at work identifying, analyzing and mitigating threats. But despite their best efforts, security incident backlogs continue to grow because there simply aren't enough skilled professionals to analyze the volume of incidents that most organizations face.

To make matters worse, the talent shortage is compounded by too many alerts being flagged by different tools within the security operations center (SOC). This leads to false alerts which slow down the response time to real threats — leading to more time spent on fixing problems that should have been caught earlier.

Splunk Security Operations Suite combines industry-leading Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and User and Entity Behavior Analytics (UEBA) solutions to modernize and optimize security operations, strengthen your cyber defenses and reduce your exposure to risk. The suite acts as your security nerve center, turning data into insights and insights into actions. It optimizes your security stack so that your team can function at peak performance. It's the only solution that utilizes a market-proven, scalable data-to-everything platform. The suite is continually augmented with actionable use case content to gain protection from the latest threats.

The suite addresses security challenges such as monitoring, investigation, automation and orchestration, advanced threats, insider threat detection, incident response, compliance and more. The suite comes with targeted content that helps solve ongoing and emerging threats quickly.

Security Information Event Monitoring (SIEM)

Splunk Enterprise Security (ES) is an analytics-driven SIEM offering. It provides real-time security monitoring, advanced threat detection, incident investigation and forensics, and more for efficient threat management.

User Entity Behavior Analytics (UEBA)/User Behavior Analytics (UBA)

Splunk User Behavior Analytics (UBA) is a machine learning-powered offering that finds unknown threats and anomalous behavior across users, endpoint devices and applications. It augments your existing security team and makes them more productive by finding threats that would otherwise be missed due to lack of people, resources and time.

Security Orchestration Automation and Response (SOAR)

Splunk Phantom is a security orchestration, automation and response (SOAR) platform. It integrates a customer's team, processes and tools together, enabling them to work smarter, respond faster, and improve their defenses.

Better Together

The Splunk Security Operation Suite uses purpose-built frameworks and workflows to speed up detection, investigation and incident response. It also uses pre-built dashboards, reports, investigation capabilities, use case categories, analytics, correlation searches and security indicators to simplify threat management and incident management.

The suite can also be used to correlate data across software-as-a-service (SaaS) and on-premises sources to discover and determine the scope of user, network, endpoint, access and abnormal activities.

The suite can be used to detect insider and unknown threats using unsupervised Machine Learning (ML) algorithms that most traditional security products miss. It can automate the correlation of anomalous behavior into high-fidelity threats using sophisticated kill-chain visualizations so security analysts can spend more time hunting with higher fidelity behavior-based alerts.

Identify the latest threats without operational downtime with dynamic content subscription updates that empower security teams to be proactive and stay up-to-date with the latest threat detection techniques.

Security team members can automate repetitive tasks to maximize their efforts and focus their attention on the highest priority threats. The Splunk Security Operations Suite works to reduce dwell times with automated detection and investigation, and reduce response times with playbooks that execute actions at machine speed.

Learn more about how Splunk's Security Operations Suite can help modernize your SOC today.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

2020-Splunk-SEC-Security-Operations-Suite-102-SG