splunk> SOLUTION GUIDE

SPLUNK SECURITY OPERATIONS SUITE

Modernize your security operations using Splunk Security Operations Suite

- Strengthen your cyber defense
- Reduce your exposure to risk
- Improve threat detection, investigation and response
- Increase the ROI of your security operations

Application Delivery

IT Operations

Security, Compliance & Fraud

Business Analytics

Internet of Things and Industrial Data

splunk>

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.

The Splunk Security Operations Suite brings together advanced security analytics, machine learning, automation and orchestration technologies to power your SOC — increasing the efficiency of your security tools and resources while reducing your exposure to risk.

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.

The suite includes market-leading SIEM, UEBA and SOAR solutions, which are all augmented with actionable use case content and built on top of a big data platform.

Security Information Event Monitoring (SIEM)

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

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

Splunk User Behavior Analytics (UBA) is a machine learning-powered solution 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 across software-as-a-service (SaaS) and on-premise sources to discover and determine the scope of user, network, endpoint, access and abnormal activities.

Splunk software can be used to detect insider and unknown threats using unsupervised 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.

Analysts can also automate repetitive tasks to maximize their SOC's efforts and focus their attention on real threats. Security professionals can use SOS to reduce dwell times with automated detection and investigation, and reduce response times with playbooks that execute 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