PRESIDIO®

SOLUTION BRIEF

Splunk

Splunk Enterprise Security Cloud Quick Start

THE CHALLENGE

Deploying a SIEM is only the first step. The real challenge is turning the platform into an operational capability that can prioritize threats, reduce alert noise, and provide meaningful security insights. Without a structured approach, organizations often spend months configuring foundational capabilities before realizing measurable security value.

THE SOLUTION

The Splunk Enterprise Security Cloud Quick Start rapidly transforms a newly deployed Splunk Cloud environment into a production-ready security operations platform by onboarding and validating up to 5–10 high-value security data sources, implementing Risk-Based Alerting, and enabling 5–10 production-ready threat detections. The result is faster time-to-value, improved visibility across users, systems, and security events, reduced alert fatigue through risk-based prioritization, and actionable security insights that help teams detect and investigate threats more effectively.

THE APPROACH

Presidio uses a proven, phased approach that includes discovery, platform configuration, priority data onboarding, security detection enablement, and knowledge transfer. This structured methodology accelerates operational readiness while establishing a scalable foundation for ongoing security monitoring and threat detection.

KEY BENEFITS

- Accelerates time-to-value by rapidly transforming a newly deployed Splunk environment into a production-ready security operations platform.
- Improves threat visibility across users, systems, and security events through the onboarding and validation of prioritized security data sources.
- Reduces alert fatigue through Risk-Based Alerting (RBA), helping analysts focus on high-priority threats and investigations.
- Enables faster threat detection and investigation prioritization through security detections aligned with the Splunk Risk Framework.
- Integrates and validates 5–10 high-value security data sources, establishing a strong foundation for effective security monitoring.
- Deploys 5–10 production-ready correlation searches to help identify suspicious and potentially malicious activity.

WHY PRESIDIO

Presidio is here to guide your digital journey and help you navigate the fast-changing tech landscape. As the bridge between where you've been (foundational IT and where you're going (ultra-modern AI and cloud services), we measure success in your terms. We strive to build lifetime relationships with those that give us their business, and we do so by being fearless, fast, flexible, and compassionate. It's our mission to earn your trust and deliver innovative, high-quality results at the speed your business needs to succeed.

ACCELERATE SECURITY OPERATIONS

The Splunk ES Cloud Quick Start rapidly transforms a newly deployed Splunk Cloud environment into a production-ready security operations platform. By combining structured implementation, prioritized data onboarding, Risk-Based Alerting, and threat detection enablement, the service improves threat visibility, reduces alert fatigue, prioritizes investigations, and accelerates time-to-value.

Contact Presidio today:
www.presidio.com/contact-us