splunk> turn data into doing™

SOLUTION GUIDE

Splunk® for Security

Leverage Analytics-Driven Security

- **Gain comprehensive security analytics** from security and non-security data sources
- **Streamline advanced threat investigations** using kill chain methodology
- **Rapid incident analysis** with fast time-to-answer and proactive threat hunting
- **Use machine learning-based advanced analytics** for rapid anomaly and threat detection and mitigate insider and external threats
- **Adaptive Response actions and Phantom playbooks** to improve operational efficiency with automated and human-assisted decisions

The sophistication of modern cyberattacks, the persistent nature of advanced threats, and the importance of managing business risk on a continual basis requires enterprises to reevaluate their entire security ecosystem. It's now critical that security analytics include a detailed analysis of information on users, attacks, context, time and location from identity, endpoints, servers, apps, web and email servers, and non-traditional systems.

The adoption of cloud, mobile workloads and hybrid deployments has magnified the need for visibility into cloud services and applications. This requires a dynamic infrastructure and application-wide view of activities to identify, investigate and respond to internal and external threats in real time.

Splunk's analytics-driven security solutions provide a comprehensive approach to cybersecurity, including advanced techniques like machine learning and behavioral analytics. These techniques help security teams quickly identify, investigate, and respond to threats based on a broader security context than is possible with legacy security products. Splunk solutions can be deployed on-premises, in the cloud or in a hybrid cloud deployment.

Splunk as Your Security Nerve Center

The Splunk Adaptive Operations Framework (AOF) helps improve cyber defense and security operations by leveraging an open ecosystem of security vendors who have built and developed integrations with leading Splunk security technologies.

Through these integrations, teams can better detect, investigate and respond at machine speed across their multi-vendor security environments - achieving a "security nerve center".

splunk>

Insider Threat Detection

Automatically detect insider threats using machine learning, behavior baselines, peer group analytics and behavior analytics.

Advanced Threat Detection

Use kill chain analysis to trace the different stages of an advanced threat, link the sequence of events and enable targeted remediation.

Fraud Detection and investigation

Detect, investigate and report on a range of fraud, theft and abuse activities in real time. Splunk complements existing anti-fraud tools by indexing event data to give an enterprise-wide view of fraud, or to create an aggregate fraud score for a single transaction.

SIEM

Use for enterprise SIEM use cases such as incident review, incident management support, analytics and behavior profiling, threat intelligence and ad hoc search. Large enterprises use Splunk for a full range of information security operations – including posture assessment, monitoring, alert and incident handling, CSIRT, breach analysis and response, and event correlation. Splunk can be used as a SIEM to operate security operations centers (SOC) of any size.

Rapid Incident Investigations

Collaboration enables SOC analysts and hunters across an organization to rapidly investigate incidents using ad hoc searches with existing correlation rules based on all security relevant data. In one centralized view, analysts and hunters can investigate the activities of potential threat actors within the SIEM workflow, speeding up the time for incident response. They can use past history to determine root cause and next steps.

Compliance Reporting

Create correlation rules and reports to identify threats to sensitive data or key employees and to automatically demonstrate compliance or identify areas of non-compliance in regards to technical controls such as: PCI, HIPAA, FISMA, GLBA, NERC, SOX, GDPR, ISO, COBIT, and the CIS Top 20.

Log Management

Consolidate, collect, store, index, search, correlate, visualize, analyze and report on any security relevant machine-generated data to identify and quickly resolve security issues. Ad hoc queries and reporting across historical data can be accomplished without third-party reporting software. Splunk software supports log data enrichment by providing flexible access to relational databases, field delimited data in comma-separated value (.CSV) files or to other enterprise data stores such as Hadoop or NoSQL.

Try Splunk Enterprise Security Now Experience the power of Splunk Enterprise Security – with no downloads, no hardware set-up and no configuration required. The Splunk Enterprise Security Online Sandbox is a 7-day evaluation environment with pre-populated data, provisioned in the cloud, enabling you to search, visualize and analyze data, and thoroughly investigate incidents across a wide range of security use cases. You can also follow a step-by-step tutorial that will guide you through the powerful visualizations and analysis enabled by Splunk software. Learn More.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

20-16281-Splunk for Security-112-SG