splunk>

FACT SHEET

Splunk® Enterprise Security

Analytics Driven Security and Continuous Monitoring for Modern Threats

Addressing the Challenges of a Dynamic Threat Landscape

The modern enterprise requires security technologies that can adapt to a dynamic threat landscape, evolving adversary tactics, advanced threats and changing business demands. To meet these new challenges, security teams need to have analytics capabilities, contextual incident response and be able to rapidly implement new threat detection techniques to reduce time-to-threat-response and make business-centric decisions.

Advanced threats are getting into organizations and infecting systems, often going undetected for long periods of time. During this time, threat actors are often escalating privileges, attacking other systems, moving laterally and potentially viewing and stealing confidential material. The evidence of the attack, as well as its activities, exists in machine data across the company, and security teams need to get insight from that data to properly detect, analyze and respond.

Security teams can detect, respond and disrupt these attacks by centralizing and leveraging all machine data. This includes traditional security data and non-security data such as business apps, web and email servers, and host data. Machine data can be supplemented with internal and external threat context such as threat intelligence feeds and other contextual information.

Splunk Enterprise Security

Splunk Enterprise Security (Splunk ES) is a premium security solution that provides insight into all data to enable security teams to quickly detect and respond to internal and external attacks, to simplify threat management while minimizing risk, and safeguard your business. Splunk ES enables your security teams to use all data to gain organization-wide visibility and security intelligence. Regardless of deployment model (on-premises, in a public or private cloud, software-as-a-service, or any combination of these), Splunk ES can be used for continuous monitoring, incident response, to run a security operations center, or to provide executives a window into business risk. Splunk ES provides organizations the ability to:

- Improve security operations through faster response times
- Improve security posture by getting end-to-end visibility across all machine data
- Increase detection capabilities using analytics-driven security
- Make more informed decisions by leveraging threat intelligence

Splunk Enterprise Security streamlines all aspects of security operations for organizations of all size and expertise. It provides insight from data generated by security technologies such as network, endpoint, access, malware, vulnerability and identity information, and correlates that data using pre-defined rules or via ad hoc searching. Splunk ES helps organizations address the following:

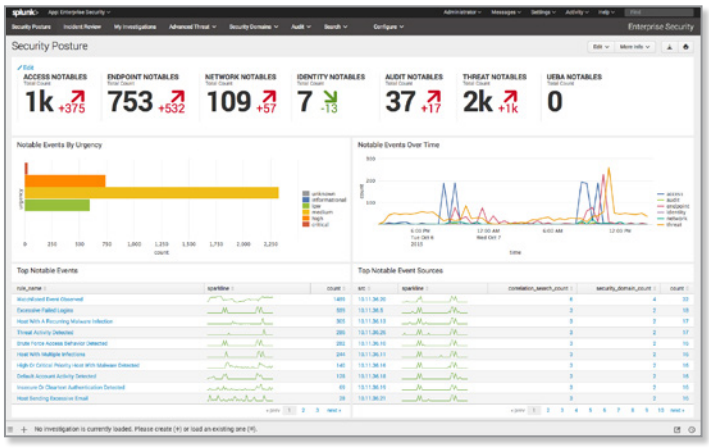
- **Continuous Monitoring**—Get a clear visual picture of the organization's security posture by using a comprehensive set of pre-defined dashboards, key security indicators (KSIs) and key performance indicators (KPIs), static and dynamic thresholds and trending indicators. Add, delete or modify these monitoring controls to easily customize views that are important to business and operations. Conduct deep investigations by drilling down to the raw event.
- **Prioritize and Act**—Optimize incident response workflows for individuals or teams by using centralized logs; alerts and incidents; pre-defined reports and correlations; incident response workflows; and correlations for a security-specific view.
- **Rapid Investigations**—Conduct rapid investigations using ad hoc search and static, dynamic and visual correlations to determine malicious activities. Investigate and pivot on any field from any data to rapidly develop threat context and track attacker steps to verify evidence, find additional information and collaborate with team members.
- **Handle Multi-Step Investigations**—Conduct breach and investigative analyses to trace the activities associated with compromised systems. Apply the kill-chain methodology to look at the attack lifecycle using ad hoc searches and all Splunk ES capabilities in combination with the investigator journal and investigation timeline.

Splunk Enterprise Security Features

Security Posture

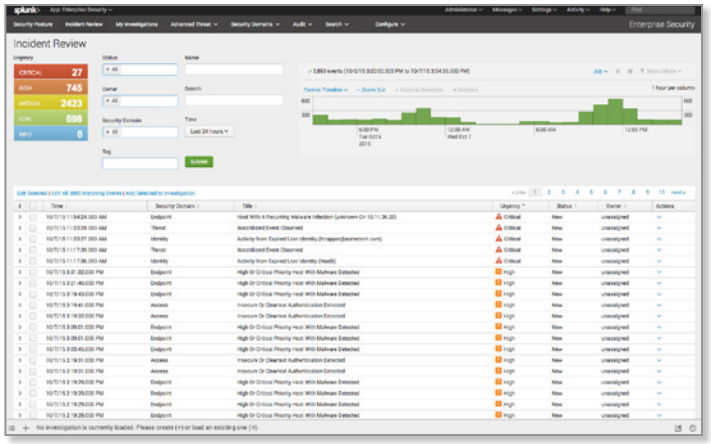
Get a library of security posture widgets to place on any dashboard or easily create your own. See security events by location, host, source type, asset groupings and geography. KPIs provide trending and monitoring of your security posture.

Incident Review and Classification



View a single event or get a 'roll-up' of related system events and an incident management workflow for security teams. Security teams can easily verify incidents, change their status and criticality, and transfer among team members, all while supplying mandatory comments about status changes. Status changes are audited, monitored and tracked for team metrics.

Investigator Journal and Investigation Timeline



Streamline multi-step analyses and investigations by focusing on tracking attack activities while the system tracks your searches and activities throughout the investigation. Add relevant events, activities and notes to the investigation timeline to visualize, and therefore more clearly understand, the attack details, as well as the sequential relationship between various events to quickly determine the appropriate next steps.

Access Protection

Simplify access control monitoring, exception analysis and audit processes for applications, operating systems and identity management systems across the enterprise. Satisfy compliance and forensics requirements to track highly privileged users and system access attempts on any business-critical application.

Endpoint Protection

Increase the effectiveness of endpoint security products such as Symantec™ Endpoint Protection, IBM® Proventia Desktop or McAfee® Endpoint Protection. Prioritize threats and view long term trends. Endpoint Protection includes searches, reports and a library of alerts for malware, rare activities, resource utilization and availability.

Network Protection

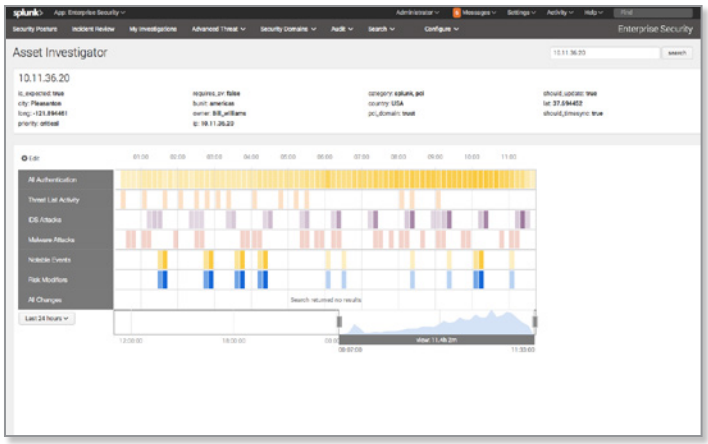
Monitor and detect events from network and security devices across the enterprise. Discover anomalies across firewalls, routers, DHCP, wireless access points, load balancers, intrusion detection sensors and data loss prevention devices. Capabilities include correlations, searches, reports and dashboards for monitoring, alerting and reporting on network-based events. Statistical analysis is employed on proxy data to understand HTTP-based behavioral outliers.

Asset Center/Identity Center

Understanding where assets are, who owns them, their criticality and who should be accessing critical information on systems helps prioritize security events and investigations. Leverage Splunk's ability to perform 'lookups' of data stored in an asset database, active directory, spreadsheets or CSV files and use information as context for security events in reports and dashboards.

Asset Investigator

Visually correlate events over time for any given IP address. This helps the analyst gain insight into time relationships across events.



Advanced Threat Investigation

A variety of advanced detection and investigative controls provide analysts the ability to use Splunk ES for investigative purposes or to detect abnormal activity (often associated with compromised systems). This includes DNS new domain analysis, HTTP category and user agent analysis; traffic size analysis; URL length analysis; and threat intelligence artifacts.

Protocol Intelligence

Get information from the wire that either is either in lieu of or complementary to data from the endpoint or network, or could otherwise not be obtained. Provides protocol information supported by the Splunk App for Stream including SSL, DNS and email activity.

Threat Intelligence Framework

Enhance incident investigation, breach investigation, and scoping by leveraging threat feeds from a broad set of sources including open source feeds in the form of flat files via an API service; a subscription-based feed in the form of TCP streaming; feeds from law enforcement or local environment in the form of manual download; and shared threat feeds in the form of STIX or OpenIOC documents via the TAXII protocol. Feeds can be weighted based on relative value, and automatically collected, aggregated and de-duplicated.

Identity and Asset Framework

Immediately understand the identity and privilege level of users and assets based on automatic mapping of data stored in an asset database, active directory, spreadsheets or CSV files and use information as context for security events in reports and dashboards.

Risk-Based Analysis

Align security posture with business needs by assigning a risk score to any event, asset, behavior, or user based on their relative importance or value to the business to prioritize security events and investigations. Easily track their security status to understand and actively manage overall business risk.

Spunk ES leverages Splunk Enterprise capabilities that include:

- **Index Any Data Source.** The ability to bring in any data without custom connectors or vendor support enables analysts to quickly access, search and analyze the data they need to complete their investigation.
- **Scalability.** The ability to index hundreds of terabytes of data per day. Splunk does not apply a schema at the time data is indexed, so searches across terabytes of data can be performed quickly.
- **Flexible Dashboards.** Dashboards can be easily created or customized for a quick graphical view of any data or correlation that is important to the organization. Organize multiple dashboards on a single screen for a customized view of the organization's overall security posture.
- **Ad Hoc Searches.** Ad hoc searches enable security teams to quickly understand what attacks are occurring in their environment to determine the best course of action.

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 15-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.

250 Brannan St., San Francisco, CA 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 splunkbase.splunk.com

splunk> listen to your data

www.splunk.com

Item # FS-Splunk-AppEntSec-122