splunk>

FACT SHEET

Splunk® App for Enterprise Security

Security Intelligence and Continuous Monitoring for Known and Unknown Threats

The Challenges of Providing Security Intelligence

There is a widening asymmetry between the mindset and methodology of the attacker and the security professional and their detection tool set. Current tools have the security team monitoring a more mobile workforce and in constant cleanup mode reacting to infected hosts. Attackers have the time, expertise and resources to create attack scenarios that bypass detection by security point products and downstream security and event management (SIEM) systems hiding their activities in the terabytes of data generated through normal user activities. Though small in number, these highly targeted attacks can take place over years siphoning off the most sensitive and highly valued enterprise data. The same can be said of individuals bent on crimes of fraud, abuse or corruption. Both the persistent attacker and the 'criminal-on-the-inside' can be classified as unknown threats. These criminals have realized that many security teams can't see their attacks in the context of operations data due to organizational data silos, data collection issues, scalability challenges or a lack of analytics capabilities. Monitoring for known threats as reported by traditional security systems and unknown threats are now part of a revised security charter. How does the security team meet this new challenge? What enterprise solution can meet the goal of providing security intelligence aligned with business risk?

The Splunk App for Enterprise Security

The Splunk App for Enterprise Security has been created to take full advantage of all of the Splunk Enterprise platform's big-data, analytics and visualization capabilities. In addition, it provides key functionality supporting the search for and processing of 'known' and 'unknown threats.' Equally suitable for a small security team or an enterprise security operations center, the App is the primary data interface for the security professional faced with a growing list of challenges. The App's out of the box content includes:

Automated Correlation Searches–that use Splunk's analytics command language for cross data-type correlations that give the user an understanding of evolving threat scenarios in real-time

Technology Add-ons–that map specific data sources and the data fields to a common information model

Data Visualizations–organized into the traditional security domains of security posture, access control, endpoint protection and network protection

Reports and Security Metrics–supported throughout the App. Any search result can be a dashboard, a table, or raw data that can be exported as a PDF or CSV

Incident Review, Classification and Collaboration–supported as part of a comprehensive incident review capability that allows for bulk event reassignment, changes in status, and criticality classification. For any change to occur, comments are required for auditing purposes

User Identity Correlation–answers questions about a specific user's activity across multiple identities required for access to multiple applications

With time-indexed collection of any data without pre-normalization and the ability to monitor host file changes, the barriers to collecting and viewing application and operations data for security event context are removed. The Splunk platform can collect any structured or unstructured data from provisioning systems, GPS, RFID, DHCP servers, DNS systems, change management systems, physical access systems or other system data needed for security investigation. Splunk and the App for Enterprise Security are a single, flexible and scalable security intelligence solution that far exceeds traditional SIEM use cases.

Traditional SIEM use cases covered by the App are complemented by the ability to watch for abnormal patterns in normal data supporting fraud analysis, user behavior analysis and the discovery of advance persistent attackers and the malware they leave behind.

"We replaced a SIEM that we had before with Splunk and the Splunk App for Enterprise Security. The other SIEM's vision seemed right but it was extremely brittle and got more so over time."

Dan Frye, VP Security, Cedar Crestone

Enterprise Security Intelligence Defined:

The collection of data from all IT systems in the enterprise that could be security relevant and the application of the security team's knowledge and skill resulting in business value and benefit.

Splunk Enterprise Security Suite Overview

Security Posture

Get real-time SOC-style presentations of security events and incidents. See security events by location, host, source type, asset groupings, and geography. Key performance indicators (KPIs) provide real-time trending and monitoring of your security posture including vulnerabilities, unpatched systems, systems with malware and hosts allowing insecure authentication.

Splunk Enterprise Security App -- Security Posture Dashboard

Incident Review, Classification and Collaboration

Incident Review provides a view of a single event or a 'roll-up' of related system events and an incident management workflow for security teams allowing them to verify incidents, change their status and criticality and transfer among team members, all while supplying mandatory comments about the status changes. Status changes are audited, monitored and tracked for team metrics. Events can also be set to automatically trigger workflows in third-party incident management systems.

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 Windows, Linux and Solaris and the critical business applications that run in these environments.

Endpoint Protection

Increase the effectiveness of endpoint security products such as Symantec™ Endpoint Protection, IBM® Proventia Desktop or McAfee® Endpoint Protection. Prioritize and correlate threats to reduce false positives and see long term trending. Set policies for violations and discover and report on exceptions. The Endpoint Protection includes searches, reports and a library of alerts for malware, rare activities, resource utilization and availability.

Network Protection

Integrate event and logging data from network and security devices across the enterprise. Define network access time-based thresholds and discover anomalies across firewalls, routers, DHCP, wireless access points, load balancers, intrusion detection sensors and data loss prevention devices. Correlate events to follow network session activity across network technologies. The App's network protection capabilities include correlations, searches, reports and dashboards for monitoring, alerting and reporting on intrusion detection, vulnerability management, proxy data and more.

Asset Center

Understanding where assets are, who owns them and their criticality in the infrastructure helps prioritize security events and investigations. The App leverages Splunk's ability to 'look-up' data stored in an asset database, spreadsheets or CSV files and use information for additional context for security events in reports and dashboards.

Incident Review Audit

An important aspect of governance is the auditing of the security solution itself and the protection of event and log data against tampering and unauthorized access. The App for Enterprise Security provides reports on all Spunk user and system activities for a complete audit trail. The Splunk engine uses data signing to maintain chain-of-custody and detect any alterations to the original log and event data. The App provides a common information model (CIM) and data-maps to simplify cross data-type correlation for reporting.

Adding New Data Sources

Splunk collects and indexes all machine-generated data without the need for custom connectors or adapters, even for multi-line custom application logs. The App leverages Splunk's ability to index log data, configuration files, events and activities generated by any application, server, network or security device without complex connectors, collection schemas or expensive database deployments. Step-by-step documentation of the CIM makes adding a new data source simple.

Incident Response and Investigation

Built for speed, the security intelligence solution supports drill-down from graphical elements to raw data. When working with the raw data, built-in workflow actions (a feature unique to Splunk and the App) augment the security investigation process and allow the user to pivot on a single piece of common information across data-types to follow the trail of an investigation wherever it leads.

Additional Reading – Available on Splunk.com

- Splunk for Security Solutions Guide: Supporting a Big-data approach for security intelligence www.splunk.com/web_assets/pdfs/secure/Splunk_For_Security.pdf
- Splunk, Big Data, and the Future of Security Whitepaper www.splunk.com/page/securelink/signup/Splunk_Big_Data_and_the_Future_of_Security.pdf
- Tech Brief: Detecting Advanced Persistent Threats – Using Splunk for APT Visibility www.splunk.com/web_assets/pdfs/secure/Splunk_for_APT_Tech_Brief.pdf

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. You can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

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

Copyright © 2012 Splunk Inc. All rights reserved. Splunk Enterprise is protected by U.S. and international copyright and intellectual property laws. Splunk is a registered trademark or trademark of Splunk Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item # FS-Splunk-AppEntSec-101