Detect, Investigate and Act on All Threats Faster with Splunk Security Solutions

October 2, 2018

Splunk Ecosystem Puts the Operations Back in the Security Operations Center

SAN FRANCISCO & ORLANDO, Fla.--(BUSINESS WIRE)--**Splunk .conf18 -** Splunk Inc. (NASDAQ: SPLK), delivering actions and outcomes from any data, today announced new innovations across its security portfolio that will help make it easier and faster for security teams to detect, investigate and act on cyber threats to protect their organizations. Powered by new features such as security automation, orchestration and response (SOAR), the Use Case Library and Event Sequencing, Splunk® Security solutions help organizations take a more holistic approach to security operations from detection to automated machine-speed response.

“As security threats increase in both velocity and complexity, our customers have a more urgent need to take action on their data so they can respond to vulnerabilities at machine speed,” said Haiyan Song, senior vice president and general manager of security markets, Splunk. “The next generation of Splunk’s security portfolio provides a security operations platform, making Splunk’s vision of a security nerve center a reality. The combination of Splunk ES, Splunk UBA and Splunk Phantom enables our customers to protect their organizations more effectively than ever before.”

The global economy continues to rapidly digitize, creating oceans of security-relevant data and ever-growing digital footprints. In parallel, a rising volume of cyber criminals executing increasingly sophisticated, automated attacks are challenging Security Operation Centers (SOCs) to keep up with the new attack surface, which lives on premise and in the cloud. Splunk Security solutions allow customers to see the entire threat versus an individual incident.

The Combined Power of Splunk Enterprise Security (ES), Splunk User Behavior Analytics (UBA) and Splunk Phantom

Splunk’s expanded suite of security solutions announced at .conf18 helps security analysts monitor, visualize, detect, investigate and act on internal and external threats via Splunk’s industry-leading security information and events management (SIEM) platform. Following Splunk’s acquisition of Phantom earlier this year, customers can now also take action on their data via Phantom’s security SOAR technology.

Splunk unveiled a range of new features to its flagship SIEM platform, including new event sequencing, which groups correlation searches and risk modifiers to optimize threat detection and accelerate investigations, and a new Use Case Library, which gives Splunk ES customers ready-to-use, research-driven and actionable security content that is relevant to their security operations. The Splunk ES Use Case Library gives customers an automatic way to discover new use cases, such as adversary tactics, cloud security, abuse or ransomware, to determine how to take action on threats within their own environment.

“Insider threats and external cyberattacks continue to have a costly impact on businesses and consumers alike. To build resiliency, organizations are recognizing that they need an analytics-driven security platform that merges security information and event management (SIEM) and user behavior analytics (UBA) functionality,” said Robert Boyce, managing director, Accenture Security. “Organizations are continuing to digitize rapidly, and clients need to look at threats across their value chain, so they can focus on the right threats, at the right time. Accenture is helping our clients improve cyber resilience by providing deep industry-specific solutions that use Splunk’s Use Case Library in Splunk ES and advanced anomaly scoring in Splunk UBA.”

“If you want to stay secure from today’s cyber threats, data analytics must be at the heart of your security strategy,” said Steve McMaster, director, managed security services, Hurricane Labs. “New Splunk ES features such as Event Sequencing and Use Case Library will provide immediate value in our SOC, helping to find and remediate threats faster. We look forward to expanding our use of Splunk and working with our customers as they continue to embrace an analytics-driven approach to security.”

Splunk Phantom’s SOAR technology helps customers work smarter and respond faster, aiding SOCs to orchestrate tasks and automate complex workflows. With Splunk Phantom 4.0, customers gain access to a wide range of new features including clustering support, which helps customers scale their operations; a new indicator view, which gives analysts a threat-intelligence-centered way to perform investigations; and improved onboarding, which enables customers to take action with Splunk Phantom within minutes of deployment.

“Data is digital gold for every security team, but if you really want to lead with an analytics-driven approach to security, it’s essential that you can take action on the data you are ingesting,” said Sebastian Goodwin, senior director of cybersecurity, Nutanix. “Splunk Phantom has been a critical component of our SOC, enabling us to automate and orchestrate a response to security threats when we need to. New additions to Splunk Phantom, such as clustering support, will help us continue to scale our SOC and respond to threats - an absolute must as cyber criminals continue to get smarter and faster.”

Nearly half of all security breaches identify malicious insiders or criminal attacks as the root cause for data breaches[1]. Splunk UBA 4.2 further extends the power of Splunk ES, helping analysts leverage machine learning to find internal and external threats and anomalous user behavior. New features in Splunk UBA 4.2 include user feedback learning, which enhances Splunk UBA anomaly model scoring to improve severity and confidence in threat detection; improved data ingestion performance by up to 2x, which strengthens data quality; and new single-sign-on authentication support, which helps SOC teams maintain compliant access controls across their security nerve center.

Splunk Adaptive Operations Framework

Splunk also announced the launch of the Splunk Adaptive Operations Framework (AOF). An evolution of the Splunk Adaptive Response Initiative, enhanced with the flexible API-driven framework from Splunk Phantom, Splunk AOF is the industry’s largest community of innovative security vendors,

committed to improving cyber defense and security operations. With Splunk AOF, organizations can leverage Splunk in tandem with over 240 security technologies to ingest structured or unstructured data from any source, drive coordinated decisions supported by analytics and take action across a comprehensive range of technologies in the SOC.

Splunk ES 5.2 and Splunk UBA 4.2 will be generally available on October 16, 2018, while Splunk Phantom is available for free download today. For more information on Splunk security solutions, visit the Splunk website.

About Splunk Inc.

Splunk Inc. (NASDAQ: SPLK) helps organizations ask questions, get answers, take actions and achieve business outcomes from their data. Organizations use market-leading Splunk solutions with machine learning to monitor, investigate and act on all forms of business, IT, security, and Internet of Things data. Join millions of passionate users and try Splunk for free today.

[1] https://www.ponemon.org/blog/2017-cost-of-data-breach-study-united-states

Contacts

Splunk Inc.
Media Contact
Bill Bode, 415-706-1236
bbode@splunk.com
or
Investor Contact
Ken Tinsley, 415-848-8476
ktinsley@splunk.com