July 24, 2012

Splunk® Showcases Security Intelligence Solutions at Black Hat 2012

Booth Demonstrations of Latest Applications for Monitoring Threats, Improving Security Posture, Fighting Cyber Attacks, and more

LAS VEGAS, July 24, 2012 /PRNewswire/ -- Black Hat 2012 -- Splunk Inc. (NASDAQ: SPLK), the leading provider of software for real-time operational intelligence, today unveiled the line-up of product demonstrations at Black Hat 2012 — several of which are being shown in public for the first time. Splunk and its team of security experts will be on hand to run live product demonstrations and answer questions at the expo on July 25 — 26 starting at 8 a.m. daily.

(Logo: http://photos.prnewswire.com/prnh/20120620/SF27490LOGO)

"Splunk is proud to be part of one of the premier security events in the world where we will share the latest solutions that are relevant for the security threats organizations face today," said Mark Seward, senior director, security and compliance, Splunk. "The nature of security threats has changed. Cyber attacks have become increasingly more creative. It means security professionals are in constant reactive mode. Splunk solutions support security professionals who practice creative risk scenario and pattern-based thinking using mathematics and statistical analysis. We now have more than 30 Splunk Apps specific to security available on Splunkbase™. We look forward to showcasing a few of our latest solutions at Black Hat 2012."

Splunk will offer demonstrations of the following applications at Booth #320:

Advanced Threat Detection (preview) — The newest advanced threats bypass traditional security point solutions and require the enterprise to go beyond the use of vendor-supplied signatures to determine that an attacker is inside the network. Understanding the difference between normal and abnormal behaviors is key to finding these threats as patterns in large data or event sets. This requires the use of statistical analysis to look for outliers and behavioral anomalies, which represents a 'mostly math' big data approach that's never in danger of becoming obsolete.

Splunk App for Palo Alto Networks Firewall 2.0 — The Splunk App for Palo Alto Networks Firewall 2.0 takes in data from Palo Alto Networks firewalls to provide additional visibility, insight and analysis of the next-generation of security threats. Splunk provides analysts with the big data analytics, statistical analysis, and visualizations needed to support common sets of metrics and support long term trending of security events. This includes views of events captured by a virtual instance of a Palo Alto Network firewall.

Splunk App for FireEye 2.0 — FireEye delivers a unique solution to the market that is enhanced by Splunk software's big data and long term trending capabilities. The Command and Control (CnC) aspects of advanced malware detected by FireEye are monitored by Splunk software. The Splunk App for FireEye 2.0 then adds the additional data and context required to understand the threat trends across applications and business services. Unlike Security Information and Event Management systems (SIEMs) that require up front data normalization and limit your views of the data, users get access to all FireEye alert data without compromise.

Splunk App for Enterprise Security —The Splunk App for Enterprise Security provides out-of-the-box security content that, combined with the core Splunk engine, delivers a next-generation security intelligence solution for monitoring 'known threats', support for forensic investigations, big data analytics to help identify advanced or 'unknown threats,' and dashboards for security posture and investigation workflows.

Splunk for Cisco Security — The combination of Splunk and Cisco Security Management products provides a single view of the security environment to facilitate incident investigations, enforce policies and meet compliance mandates. The Splunk for Cisco Security Solution delivers a rich security experience by providing additional insights from data generated by Cisco security products. It offers a single interface visibility into data provided by multiple Cisco security products including the Cisco IronPort Email and Web Security Appliances, Cisco Client Security Agent, Cisco firewalls, and Cisco IPS.

Splunk App for NetFlow — Users of the Splunk App for NetFlow now have the ability to capture netflow binary records (using nfdump) and feed them to Splunk to produce dashboards and reports measuring traffic usage by source, destination, protocol, and more.

Black Hat USA 2012 celebrates 15 years as one of the most significant information security events in the world. More than 6,500 digital security experts, public, private sector security professionals, and underground hackers will attend Black Hat to uncover groundbreaking new vulnerabilities and new security tools for the first time. For more information on the conference please go to http://www.blackhat.com/usa/.

For the latest on Splunk security solutions, please go to the Splunk website at http://www.splunk.com/view/enterprise-security-app/SP-CAAAE8Z.

About Splunk Inc.
Splunk Inc. (NASDAQ: SPLK) provides the engine for machine data™. Splunk® software collects, indexes and harnesses the massive machine data continuously generated by the websites, applications, servers, networks and mobile devices that power business. Splunk software enables organizations to monitor, search, analyze, visualize and act on massive streams of real-time and historical machine data. More than 4,000 enterprises, universities, government agencies and service providers in over 80 countries use Splunk Enterprise to gain operational intelligence that deepens business understanding, improves service and uptime, reduces cost and mitigates cyber-security risk. To learn more, please visit www.splunk.com/company.

SOURCE Splunk Inc.

News Provided by Acquire Media