SOLUTION BRIEF

Splunk and Keysight: Put Time On The Side of Your Security Team

Joint Solution Overview

These days we hear a lot about security response times and ways to speed breach and threat detection and response. We hear less about the time—and effort—spent identifying and delivering the data needed to drive these processes efficiently in the first place.

Together, Splunk and Keysight deliver integrated, automated solutions for alerting your cyber defense team to possible threats and extracting the right data needed to take action—in seconds and minutes instead of hours and days. Splunk Enterprise Security (SIEM) and Splunk Phantom (SOAR) form the “nerve center” of a security operations center, enhancing customers’ ability to quickly generate and curate security alerts and respond immediately with automated playbooks. Keysight’s intelligent network visibility solutions work with Splunk products to speed delivery of the right packet, flow, and metadata to every element of your security infrastructure.

In the face of higher traffic volumes, more complex threats, and a perennial shortage of skills and resources, the joint solution alleviates the strain on IT and security teams with seamless intelligence and integration. Automating routine tasks makes security operations (SecOps) more efficient and cohesive across your entire hybrid network infrastructure. Increased visibility and control translate into faster detection and containment of threats in less time and with less effort.

Highlights

- Accelerate and automate threat identification and mitigation
- Improve efficiency by automating predictable tasks via playbooks
- Extend the capability and value of existing security tools
- Leverage IxFlow security metadata to maximize the value of Splunk
- Download from Splunkbase

KEYSIGHT TECHNOLOGIES

How It Works

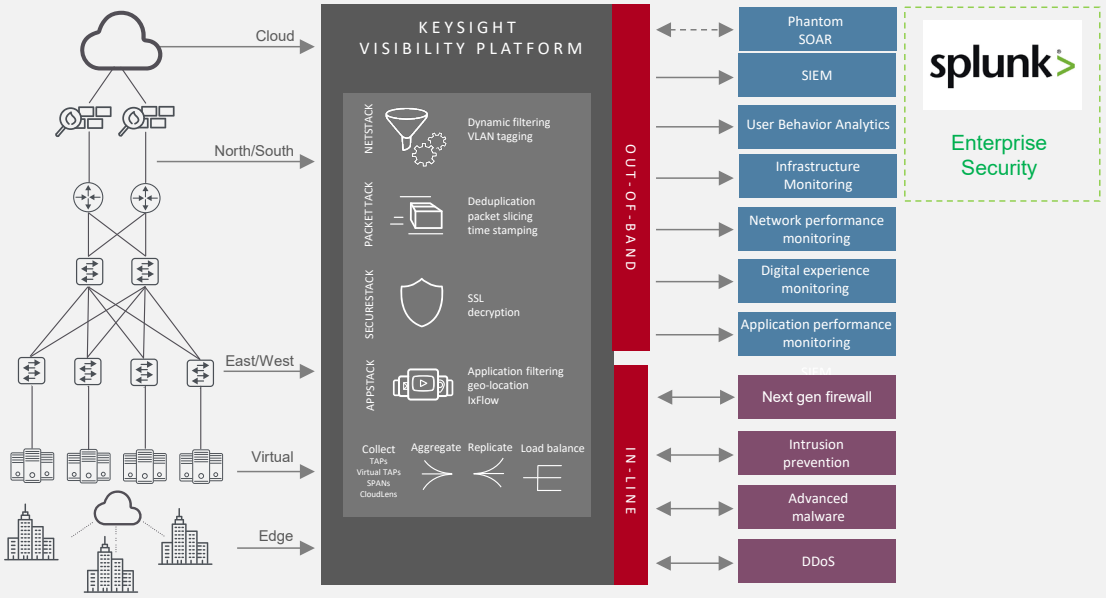
Security experts and best practices increasingly rely on machine/log data and automation to accelerate the process of “finding the needle in a haystack.” Splunk Enterprise Security analyzes log data from the network as well as flow and metadata from Keysight’s Vision network packet brokers and other sources to quickly spot anomalies. These anomalies are validated and incorporated into well-qualified and actionable alerts.

Splunk Phantom then automates and orchestrates repetitive security tasks to “force multiply” your team’s efforts and reduce response times by executing playbooks at machine speed. Alerts from Phantom can be used by Keysight’s Vision network packet brokers (NPBs) to isolate, aggregate and streamline the right packet and flow data to your security monitoring tools for analysis.

Granular packet data is often critical for troubleshooting and threat hunting, yet too voluminous to ingest all packets. Keysight’s Splunk Phantom integration allows enterprises to capture only the packets of interest to save significant time and money.

Keysight’s flexible visibility intelligence:

- Captures and delivers relevant raw packets from the network
- Adds valuable context in the form of flow and metadata – includes detailed data about applications, devices, known threats, and geolocation that can be analyzed in Splunk Enterprise Security using the IxFlow Splunk App
- Integrates with Splunk Phantom to automate analysis and remediation steps to gather more data
- Promotes rapid drill-down analysis on the security tools you already own



Phantom APIs and Keysight's App for Phantom and the IxFlow Splunk App provide seamless integration of intelligent visibility that reduces time and effort to address everyday security challenges such as:

- Identifying & containing distributed denial of service (DDoS) and domain name server (DNS) attacks
- Detecting malware and other encrypted exploits
- Blocking outbound or insider attacks

Why Use Splunk and Keysight

Together, Splunk Enterprise Security, Splunk Phantom, and Keysight's Vision NPBs deliver exponential productivity gains and relief for overworked security teams. By automating and orchestrating security operations (SecOps), the integrated Splunk and Keysight solution lets your team get to the heart of the matter and mount the right response faster. Splunk Enterprise Security and Splunk Phantom combine to combat threats with advance analytics, actionable intelligence, playbook automation, and infrastructure orchestration that extends across your entire security environment.

About Splunk

Splunk is the world's first Data-to-Everything Platform designed to remove the barriers between data and action, so that everyone thrives in the Data Age. We're empowering IT, DevOps and security teams to transform their organizations with data from any source and on any timescale. With more than 6,000 employees in 27 offices worldwide, we're building a future where data provides clarity, elevates discussion and accelerates progress for innovators in IT, security, DevOps and more.

splunk>

www.splunk.com

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES

This information is subject to change without notice. © Keysight Technologies, 2019 - 2022, Published in USA, January 11, 2022, 3121-1069.EN