Investigate and Respond to Security Incidents Faster and More Efficiently with Rapid7 and Splunk

INTEGRATION BENEFITS
- Security context awareness into the vulnerability state of assets
- Easy detection of user-focused attacks, such as compromised credentials, phishing attacks and lateral movement
- Single pane view into your security events, reporting, forensics, and incident investigation
- User lens to security incidents by easily correlating assets, users, and incidents
- In-depth investigations with additional security information about each asset, e.g. ports, services, applications, users
- Automated vulnerability data import on a scheduled basis to correspond with latest scans
- Security alerts in Splunk triggered by UserInsight incident detection
- Data visualization to see graphically your vulnerability data for easier investigations
- Drill down capabilities for quicker analysis

Solution Overview
Splunk is the leading software platform for real-time operational intelligence, enabling organizations to search, monitor, analyze, and visualize machine-generated big data coming from websites, applications, servers, networks, sensors, and mobile devices. Rapid7’s IT security data and analytics solutions collect, contextualize, and analyze the security data you need to fight an increasingly deceptive and pervasive adversary.

The integrated solution enables security operations professionals to detect, investigate, and respond to security threats more quickly and effectively. It integrates Rapid7 Nexpose and Rapid7 UserInsight with Splunk Enterprise to provide vulnerability management and incident detection data.

Rapid7 Nexpose provides valuable asset risk context during attacks
Rapid7 Nexpose is the only vulnerability management solution that analyzes risk across vulnerabilities, configurations, and controls with awareness of the threat landscape across the modern network.

Vulnerability data from Nexpose scans feeds into Splunk software so users can create alerts, raise alarms, or take other operational actions when attacks are happening on assets affected by vulnerabilities. This provides more insight into the current risk state of an organization’s infrastructure.

Rapid7 UserInsight helps detect and investigate user-focused incidents
Rapid7 UserInsight finds the attacks you’re missing by detecting and investigating indications of compromised users from the endpoint to the cloud. UserInsight detects attackers even when they are hiding behind stolen user credentials - today’s most common attack tactic.
Data available in Splunk can now be easily fed into Rapid7 UserInsight to detect and investigate user-focused security incidents, such as the use of compromised credentials, phishing attacks, and suspicious behavior. UserInsight can feed these alerts back to Splunk for further correlation and visibility leveraging Splunk software as the single pane of glass for security activities in a company’s Security Operations Center (SOC).

Rapid7 Splunk App Complies with Common Information Model (CIM)

The Rapid7 Splunk App complies with the Common Information Model (CIM), opening Rapid7 security data and analytics up to any other CIM compliant applications. CIM is an open standard that defines how managed IT systems are represented as a common set of objects and relationships between them. This is intended to allow consistent maintenance of these managed elements, independent of their manufacturer or provider.

HOW IT WORKS
Simply download the Rapid7 Splunk App to integrate Splunk Enterprise with Rapid7 Nexpose and Rapid7 UserInsight.

WHAT YOU NEED:
- Rapid7 Nexpose 5.x
- Rapid7 UserInsight
- Splunk Enterprise 6.x

Single pane view into your security events, reporting, forensics, and incident investigation

About Splunk Inc.

Splunk Inc. (NASDAQ: SPLK) provides the leading software platform for real-time Operational Intelligence. Splunk® software and cloud services enable organizations to search, monitor, analyze and visualize machine-generated big data coming from websites, applications, servers, networks, sensors and mobile devices. More than 7,900 enterprises, government agencies, universities and service providers in 100 countries use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, prevent fraud, improve service performance and reduce cost. Splunk products include Splunk® Enterprise, Splunk Cloud™, Splunk Storm®, Hunk™ and premium Splunk Apps. To learn more, please visit http://www.splunk.com/company.

About Rapid7

Rapid7 is a leading provider of security data and analytics solutions that enable organizations to implement an active, analytics-driven approach to cyber security. We combine our extensive experience in security data and analytics and deep insight into attacker behaviors and techniques to make sense of the wealth of data available to organizations about their IT environments and users. Our solutions empower organizations to prevent attacks by providing visibility into vulnerabilities and to rapidly detect compromises, respond to breaches, and correct the underlying causes of attacks. Rapid7 is trusted by more than 4,150 organizations across 90 countries, including 34% of the Fortune 1000. To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.

Figure 1: Nexpose Dashboard for Splunk Enterprise