INTEGRATION BRIEF

Accelerate Investigation and Response

By combining Rapid7 InsightVM and InsightIDR with Splunk Enterprise

Achieve more with a single pane view of your security events, reporting, forensics, and incident investigations. By integrating Rapid7 InsightVM and InsightIDR with Splunk Enterprise, an industry-leading platform for operational intelligence, you can detect, investigate, and respond to security threats more quickly and effectively. Rapid7 solutions collect, contextualize, and analyze data from Splunk Enterprise, equipping you to better protect against increasingly deceptive and pervasive adversaries.

Gain asset risk context during attacks with Rapid7 InsightVM

Rapid7 InsightVM is the only vulnerability assessment solution that analyzes risk across vulnerabilities, configurations, and controls with awareness of the threat landscape faced by modern networks.

Vulnerability data from InsightVM's scanning activities feeds into Splunk software so you 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.

Detect and investigate user-focused incidents with Rapid7 InsightIDR

Rapid7 InsightIDR detects and investigates indicators of user compromise across your endpoints to your cloud services, so you don't miss any attacks—including those attempted by intruders hiding behind stolen credentials (today's most common attack tactic).

You can feed data from Splunk Enterprise into InsightIDR to detect and investigate compromised user accounts and malware, and gain direct visibility into their endpoints. The combination gives you multiple visualization and investigation options, while providing defense-in-depth with pre-built user and Attacker Behavior Analytics (ABA) and deception technology.

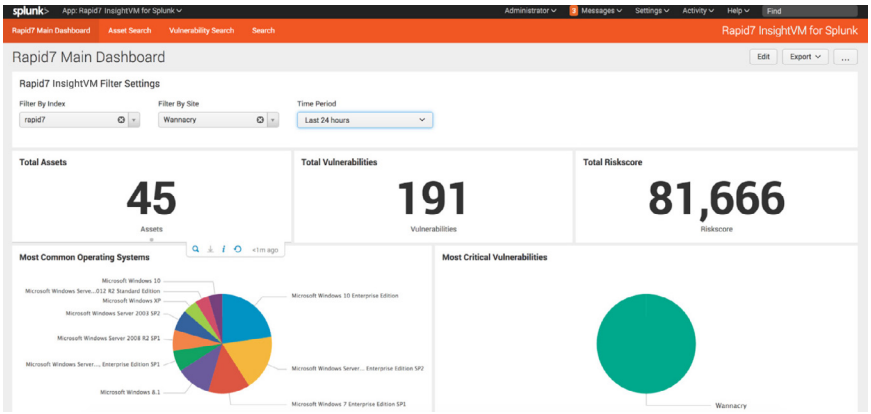
INTEGRATION BENEFITS

- Gain awareness and context around your assets' vulnerability state
- Easily detect user-focused attacks, such as compromised credentials, phishing attacks, and lateral movement
- Apply a user lens to security incidents by easily correlating assets, users, and incidents
- Conduct in-depth investigations with additional security information about each asset, e.g. ports, services, applications, and users
- Monitor your endpoints for vulnerabilities and real-time compromise with the Rapid7 Insight Agent
- Add monitoring opportunities with deception technology (honeypots, honey credentials) to detect stealthy attacker behavior
- Visualize your vulnerability data graphically for easier investigations

*All mentions of Rapid7 InsightVM associated with its integration with Splunk Enterprise also apply to Rapid7 Nexpose.

080618

Figure 1: Rapid7 Dashboard for Splunk Enterprise



Leverage the Common Information Model (CIM) with the Rapid7 Technology Add-On for Splunk

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

How It Works

Simply download the Rapid7 Splunk Technology Add-On to integrate Splunk Enterprise with Rapid7 InsightVM and InsightIDR.

What You Need

- Rapid7 InsightVM
- Rapid7 InsightIDR
- Splunk Enterprise

TAKE THE INTEGRATION FOR A SPIN

Start your 30-day trial of InsightVM and InsightIDR:
www.rapid7.com/try/insightvm
www.rapid7.com/try/insightidr

SUPPORT

Please contact Rapid7 for support at +1.866.380.8113, or visit our customer support portal.

About Splunk

Splunk Inc. (NASDAQ: SPLK) turns machine data into answers. Organizations use market-leading Splunk solutions with machine learning to solve their toughest IT, Internet of Things and security challenges. Join millions of passionate users and discover your "aha" moment with Splunk today: www.splunk.com.

About Rapid7

Rapid7 powers the practice of SecOps by delivering shared visibility, analytics, and automation that unites security, IT, and DevOps teams. The Rapid7 Insight platform empowers these teams to jointly manage and reduce risk, detect and contain attackers, and analyze and optimize operations. Rapid7 technology, services, and research drive vulnerability management, application security, incident detection and response (SIEM), orchestration and automation, and log management for organizations across the globe.

To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.