INTEGRATION BRIEF

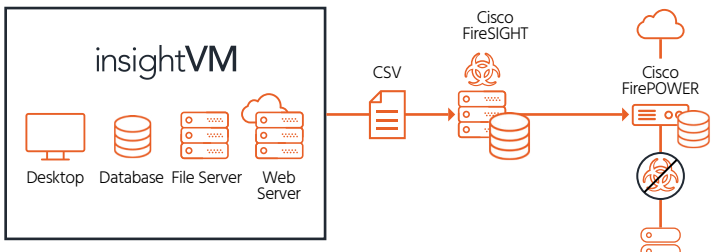
Stop Real-Time Threats

With Cisco FireSIGHT and Rapid7 InsightVM or Nexpose

Threats are evolving at a faster pace every day, but making sure that you're constantly aware of your organization's vulnerabilities can be a daunting challenge. Active vulnerability scanning needs to be supplemented with intelligent, preventative security measures to give a comprehensive picture of your security posture and your organization's exposure to real world attacks. Leveraging Rapid7's InsightVM or Nexpose solutions within Cisco's FireSIGHT Management Center gives you the confidence to stop attacks with the most accurate security data available.

HOW IT WORKS

An InsightVM* scan is conducted to assess the risk posture of the systems within your organization. The InsightVM connector generates a CSV file containing all the vulnerability and asset data, which then gets pushed to Cisco FireSIGHT Management Center. Once in FireSIGHT Management Center, the data gets combined with the vulnerability and asset information that already exists in the Host Map. From there, if malicious network traffic is detected that matches a known vulnerability on the host, the Impact flag gets raised accordingly; this signals with confidence that the attack will be successful, and can be stopped by enabling the IPS rule.



Assessing Security Posture of Devices

*All mentions of Rapid7 InsightVM associated with Cisco FireSIGHT also apply to Rapid7 Nexpose.

INTEGRATION BENEFITS

- Stop threats in real-time with IPS rules that are enabled with a high impact flag
- Gain deeper insight by utilizing InsightVM or Nexpose active scanning technology to reach assets that may not be visible to Cisco FireSIGHT
- Receive greater contextual information about each asset in FireSIGHT Management Center such as vulnerabilities, OS, applications, services, etc.
- Reduce false positives by importing InsightVM data and correlating attacks with vulnerabilities to raise the impact flag
- Automate vulnerability data import on a scheduled basis to correspond with latest scans

101817

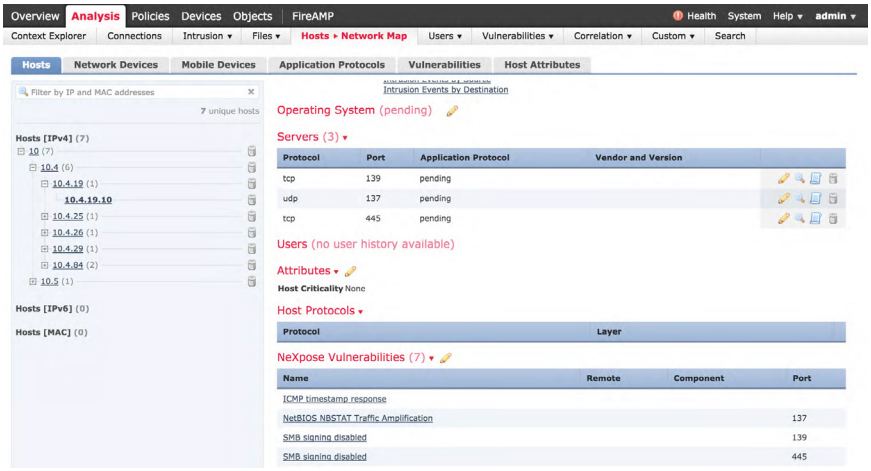
Overview of Integration Process

- **Step 1:** Rapid7 InsightVM performs a security assessment.
- **Step 2:** An XML report is generated with the latest vulnerability findings.
- **Step 3:** InsightVM connector connects to Cisco FireSIGHT Management Center and pushes a CSV file with latest vulnerabilities and asset details.
- **Step 4:** FireSIGHT Management Center adds the corresponding vulnerabilities to its Host Map database and pushes it out to each sensor.
- **Step 5:** Rules can be enabled to stop the corresponding attack.

What You Need

- Rapid7 InsightVM or Rapid7 Nexpose
- Cisco FireSIGHT Management Center 5.x

Figure 1: Cisco FireSIGHT Management Center with Rapid7 vunerability data



SUPPORT

Please contact Rapid7 for support or assistance at +1.866.380.8113 or support@rapid7.com.

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. Cisco delivers intelligent cybersecurity for the real world, providing one of the industry's most comprehensive advanced threat protection portfolio of solutions across the broadest set of attack vectors. Cisco's threat–centric and operationalized approach to security reduces complexity while providing unmatched visibility, consistent control, and advanced threat protection before, during, and after an attack. For more information visit www.cisco.com/go/security.

About Rapid7

Rapid7 is a leading provider of security data and analytics solutions that enable organizations to implement an active, analytics-driven approach to cybersecurity. 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.

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