INTEGRATION BRIEF

Streamline Your Vulnerability Remediation Workflow

With Rapid7 InsightVM and ServiceNow ITSM

Being proactive about security means more than just conducting frequent security assessments of your enterprise assets. The key to securing your organization comprehensively is mitigating the risk of vulnerabilities with proper remediation steps. But it's a bit harder than it sounds: Security teams can have challenges communicating with their IT counterparts, who are responsible for actually applying remediation steps.

Integrating Rapid7 InsightVM with ServiceNow ITSM seamlessly folds remediation instructions into IT's existing workflows by automatically opening tickets when new vulnerabilities are discovered, and closing tickets when those vulns are fixed. But it doesn't stop there: Additionally, you can assign tickets to the correct teams, customize the level of detail included, report when they're closed, and double-check they've been successfully remediated with subsequent scans. In short, track progress in *real time*, rather than wait to see if issues have been fixed in the next scan.

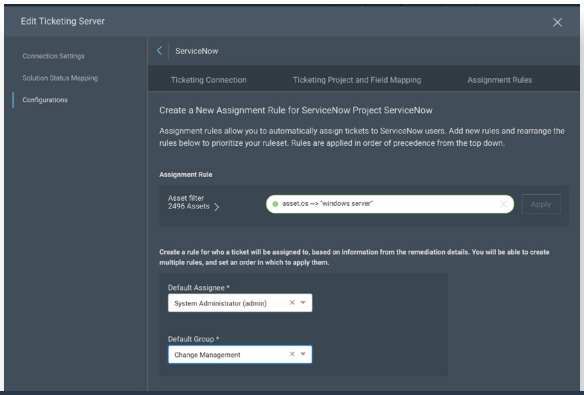
*All mentions of Rapid7 InsightVM associated with its integration with ServiceNow ITSM also apply to Rapid7 Nexpose.

INTEGRATION BENEFITS

- Streamline workflows with IT by utilizing the native ticketing solution leveraged by your IT operations team
- Automatically generate tickets within ServiceNow ITSM after a Rapid7 InsightVM scan is completed
- Create customizable tickets that can be opened by specific severity thresholds, sites, or asset groups
- Customize tickets with the level of detail appropriate for specific audiences and contexts
- Leverage closed-loop integration to mark vulnerabilities as "awaiting verification," until InsightVM validates the fix
- Configure and deploy the integration with ease

062718

Figure 1: Configuring ServiceNow tickets within InsightVM



Create a New Assignment Rule for ServiceNow Project ServiceNow

Assignment rules allow you to automatically assign tickets to ServiceNow users. Add new rules and rearrange the rules below to prioritize your ruleset. Rules are applied in order of precedence from the top down.

Assignment Rule

Asset filter
2496 Assets

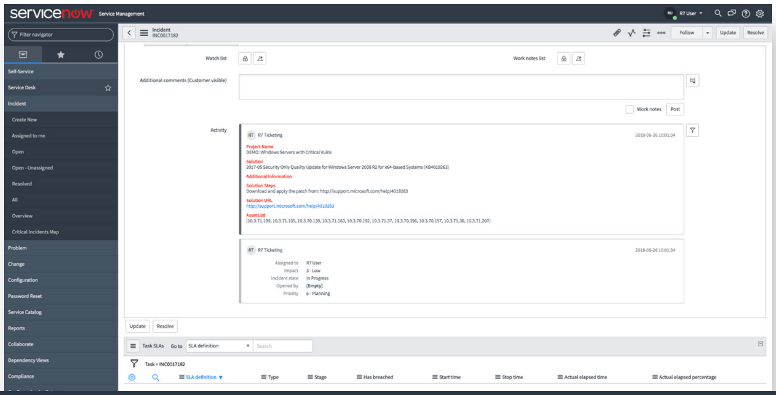
asset.os ~> "windows server"

Create a rule for who a ticket will be assigned to, based on information from the remediation details. You will be able to create multiple rules, and set an order in which to apply them.

Default Assignee *: System Administrator (admin)

Default Group *: Change Management

Figure 2: Viewing remediation instructions and progress within ServiceNow



Incident
INC0017182

RT R7 Ticketing 2018-06-26 10:01:34

Project Name
DEMO: Windows Servers with Critical Vulns

Solution
2017-05 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB4019263)

Additional Information

Solution Steps
Download and apply the patch from: http://support.microsoft.com/help/4019263

Solution URL
http://support.microsoft.com/help/4019263

Asset List
[10.3.71.199, 10.3.71.105, 10.3.70.139, 10.3.71.163, 10.3.70.192, 10.3.71.37, 10.3.70.196, 10.3.70.157, 10.3.71.30, 10.3.71.207]

RT R7 Ticketing 2018-06-26 10:01:34

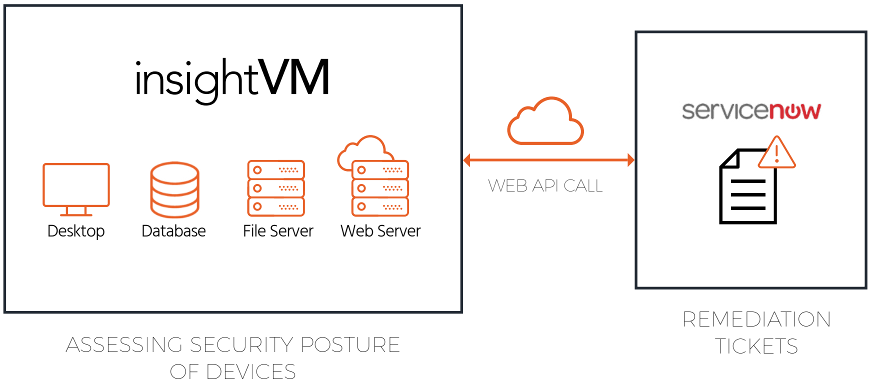
Assigned to: R7 User
Impact: 3 - Low
Incident state: In Progress
Opened by: [Empty]
Priority: 5 - Planning

Task = INC0017182

Want to see this integration for yourself? Start your 30-day trial of InsightVM at www.rapid7.com/try/insightvm.

HOW IT WORKS

InsightVM conducts a scan to assess the risk posture of the systems within your organization. The vulnerability data is then processed for each host. Next, at periodic intervals, the ServiceNow ITSM connector queries InsightVM for the latest vulnerabilities; remediation tickets are either created or closed accordingly. In the case of the former, a ServiceNow ITSM Administrator can then assign the tickets to the proper teams for remediation.



SUPPORT

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

About ServiceNow

ServiceNow is the enterprise IT cloud company. They transform IT by automating and managing IT service relationships across the global enterprise. Organizations deploy our services to create a single system of record for IT and automate manual tasks, standardize processes, and consolidate legacy systems. Using their extensible platform, their customers create custom applications and evolve the IT service model to service domains inside and outside the enterprise. ServiceNow transforms IT from the department of no to the department of now.

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.