RAPID7

SOLUTION GUIDE

Discovering, Assessing, and Remediating New Critical Vulnerabilities

A step-by-step guide to addressing new critical "named" vulns in InsightVM

TABLE OF CONTENTS

Introduction

Dealing with new critical “named” vulnerabilities is nothing to new security teams.

Yet in recent years, vulnerabilities like Heartbleed and attacks like WannaCry have made international headlines, thrusting vulnerability management into the public spotlight.

When a new critical vulnerability or attack is discovered, others are probably asking you the following questions:

- How exposed are we to this attack?
- Have we already been compromised?
- What are we doing to mitigate this risk?

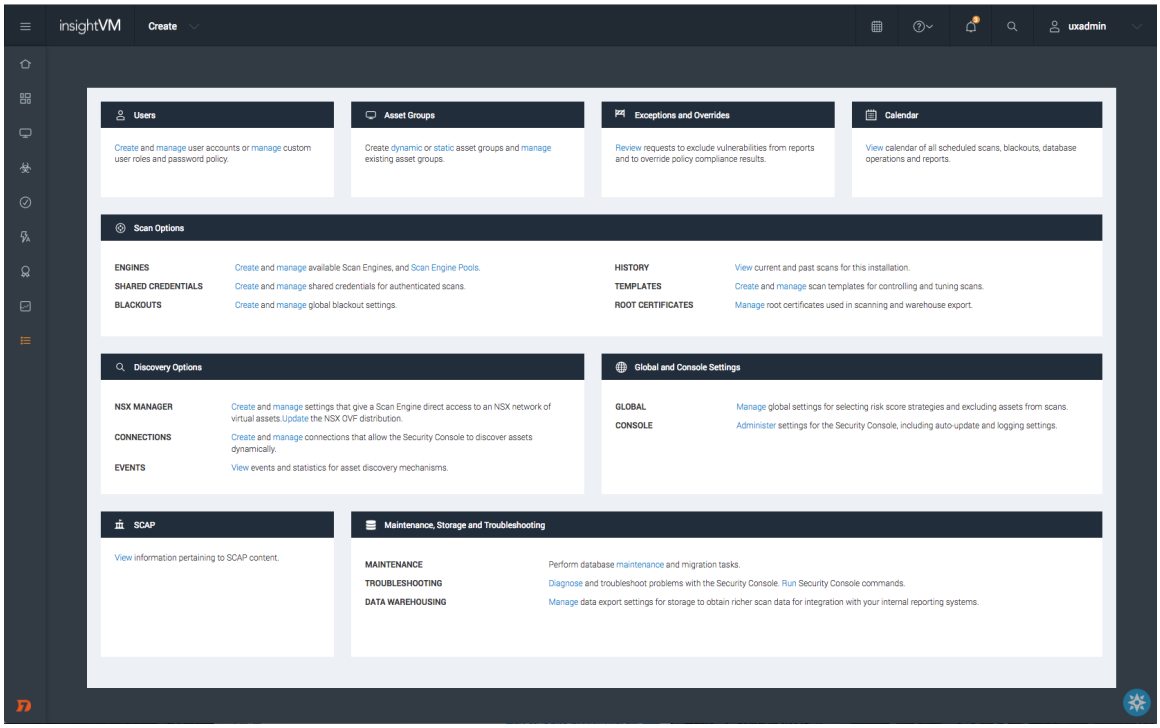
In this guide, we help you get a few steps closer to answering those questions by covering how InsightVM can:

- Launch a focused scan for a specific vulnerability or set of vulnerabilities
- Report on affected assets using dynamic filtering and Live Dashboards
- Streamline communications to help teams identify and address remediation activities

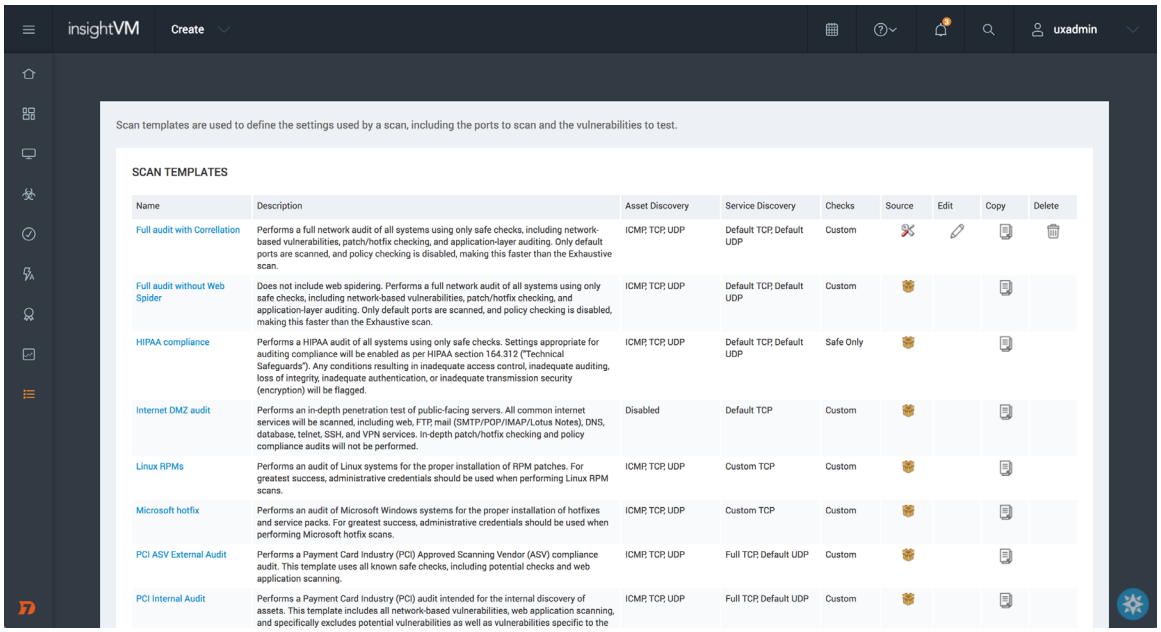
Launching focused scans using scan templates

Scan templates in InsightVM dictate the mechanics of how scans are run. Although general audit scans cover new vulnerability checks as they're released, it's recommended that you create specific templates for critical vulnerabilities that are focused only on those relevant checks, as honed scans will run significantly faster.

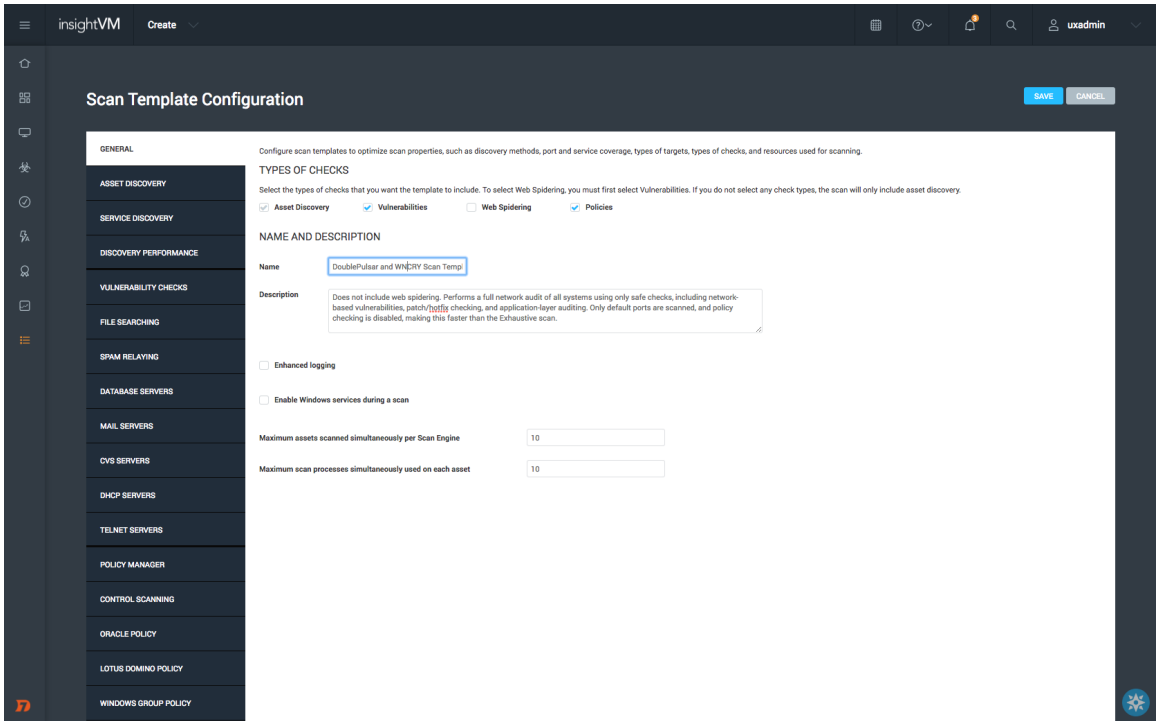
1. Under the Administration tab, go to Templates, then select Manage Templates



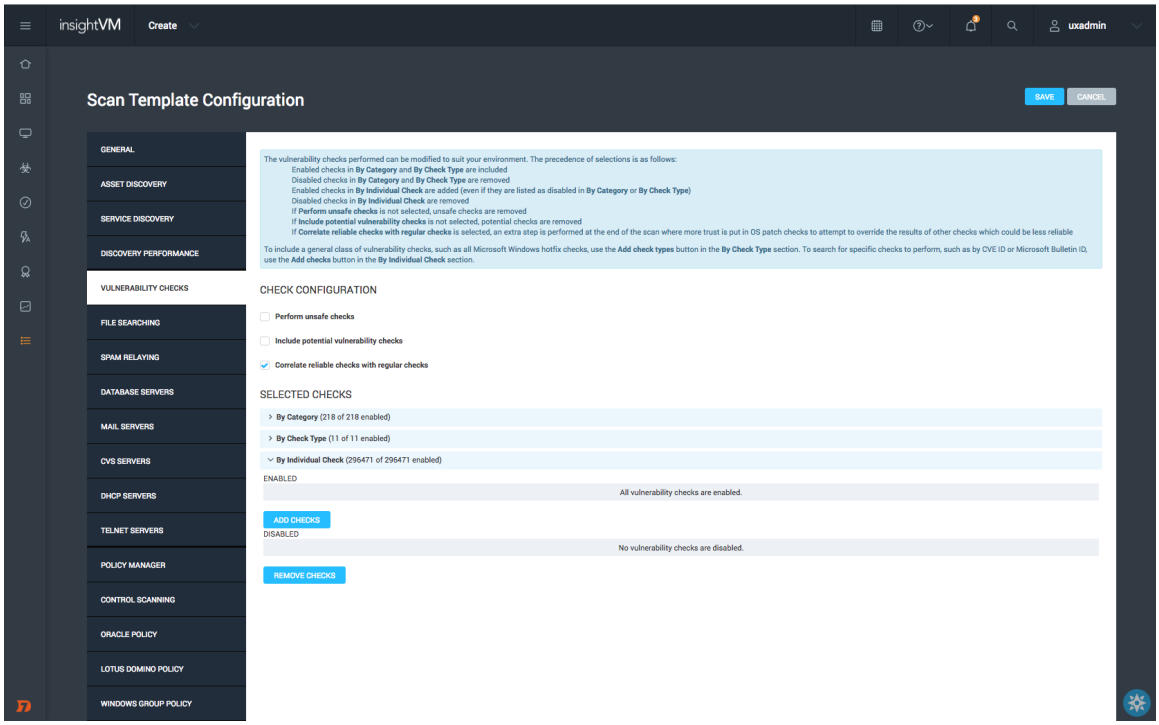
2. Copy the following template: “Full audit without Web Spider”



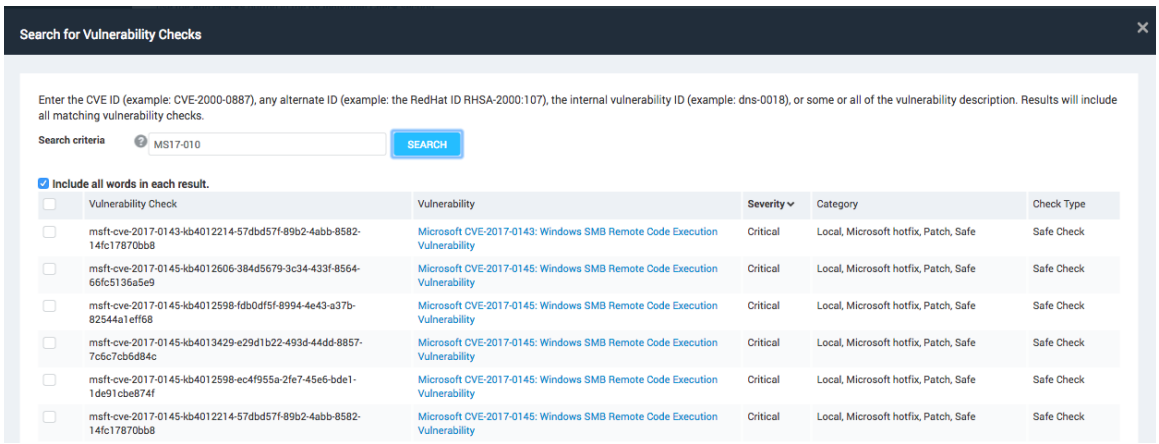
Don’t forget to give your copy a name and description. In this example, we’ll name our template “Double Pulsar and WNCRY Scan Template.”



3. Click on Vulnerability Checks, then By Individual Check.



4. Add in the specific CVEs or vulnerabilities you are scanning for and click save. In this example, we used “MS17-010”; you can also use individual CVEs.

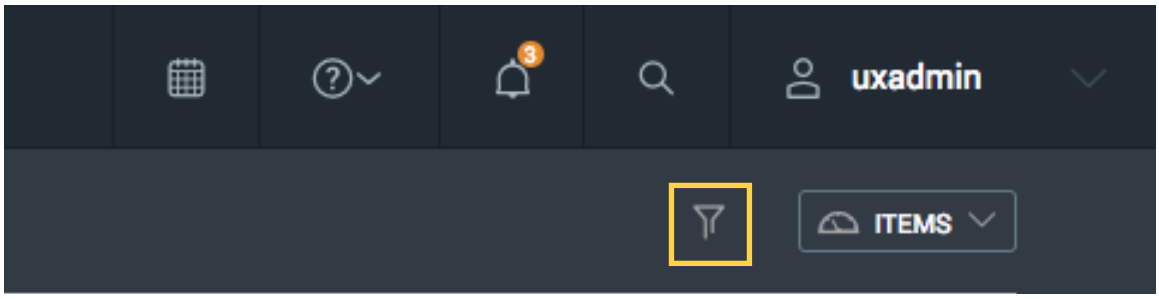


5. Save the template and run a scan to identify all assets affected by those vulnerabilities.

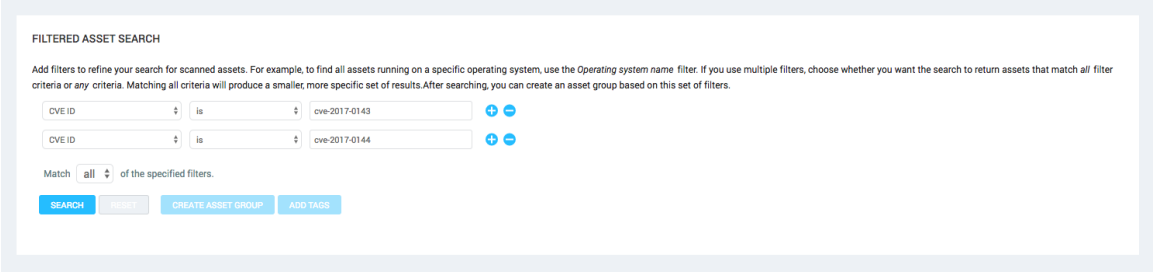
Reporting on affected assets with Dynamic Asset Groups

Once assets have been scanned, create a Dynamic Asset Group for reporting and tagging that will update whenever new assets affected by this vulnerability are found (and fixed).

1. Click on the filter icon in the upper right corner of the InsightVM console, just under the search button.



2. Use the CVE ID filter to specify the which CVEs apply to you. For example, “CVE-2017-0143” and “CVE-2017-0144.”

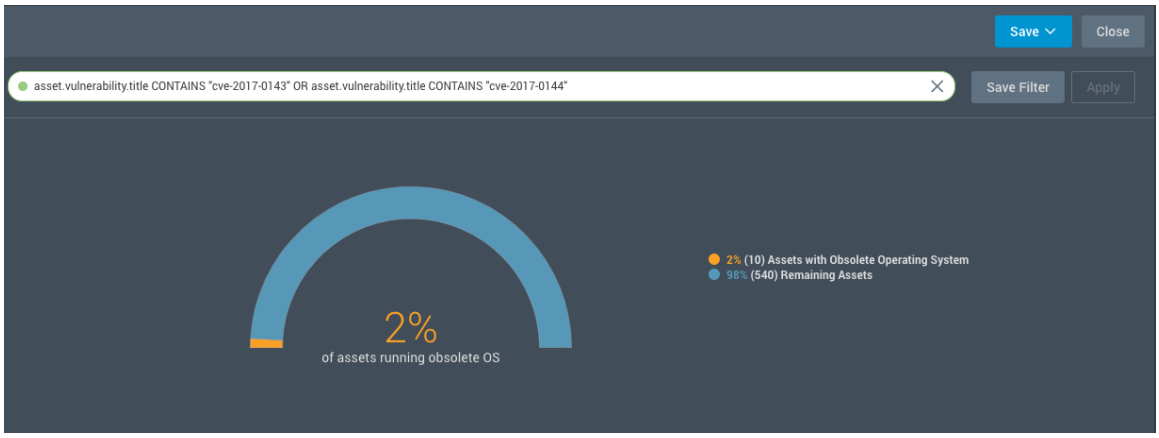


This asset group can now be used for reporting and tagging to quickly identify exposed systems.

Visualizing affected assets with Live Dashboards

Live Dashboards in InsightVM can be customized with various cards on specific topics and trends, and most cards can be filtered down by simple query language. These filters scope dashboard cards down to the specific assets that are affected by a critical vulnerability. Use the filter “asset.vulnerability.title” to specify the appropriate vulnerabilities.

In the example below, we use “CVE-2017-0143” and “CVE 2017-0144” and filter using the following: asset.vulnerability.title CONTAINS “cve-2017-0143” OR asset.vulnerability.title CONTAINS “cve-2017-0144” [1]

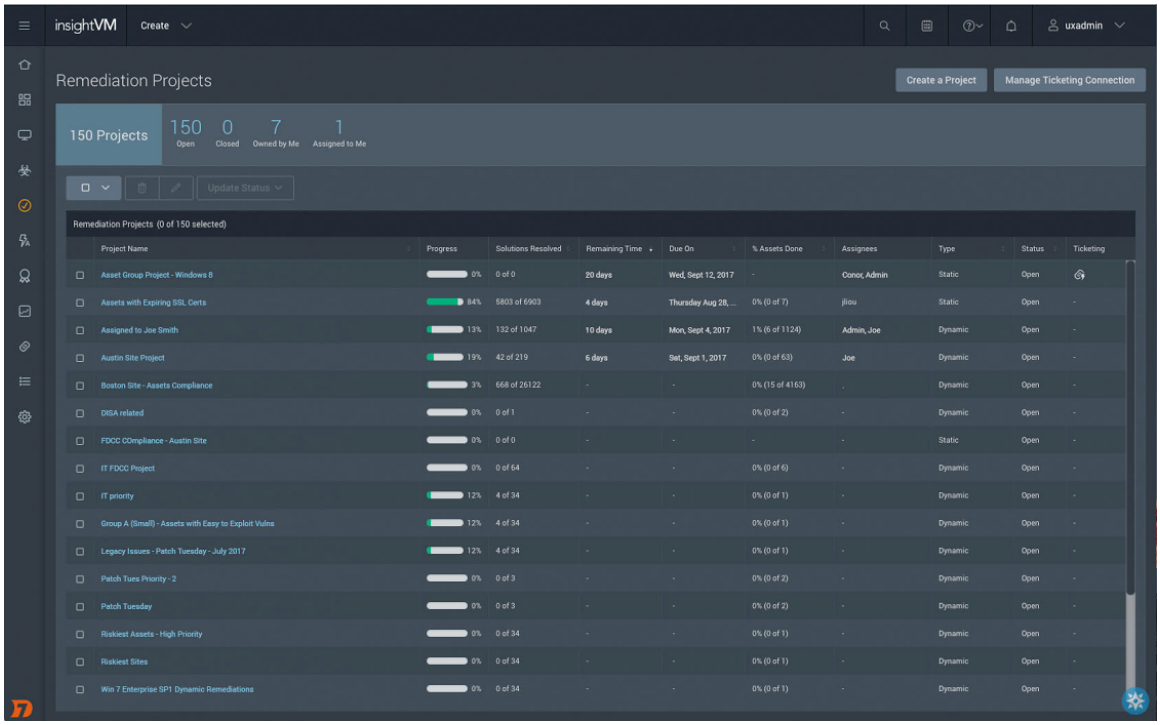


[1] Note: You can use either “asset.vulnerability.title” or “vulnerability.alternateids” for these commands; the latter is useful for groups of vulnerabilities like Microsoft advisories on the format MS17-010, while the former is useful for specific vulnerability titles or CVEs.

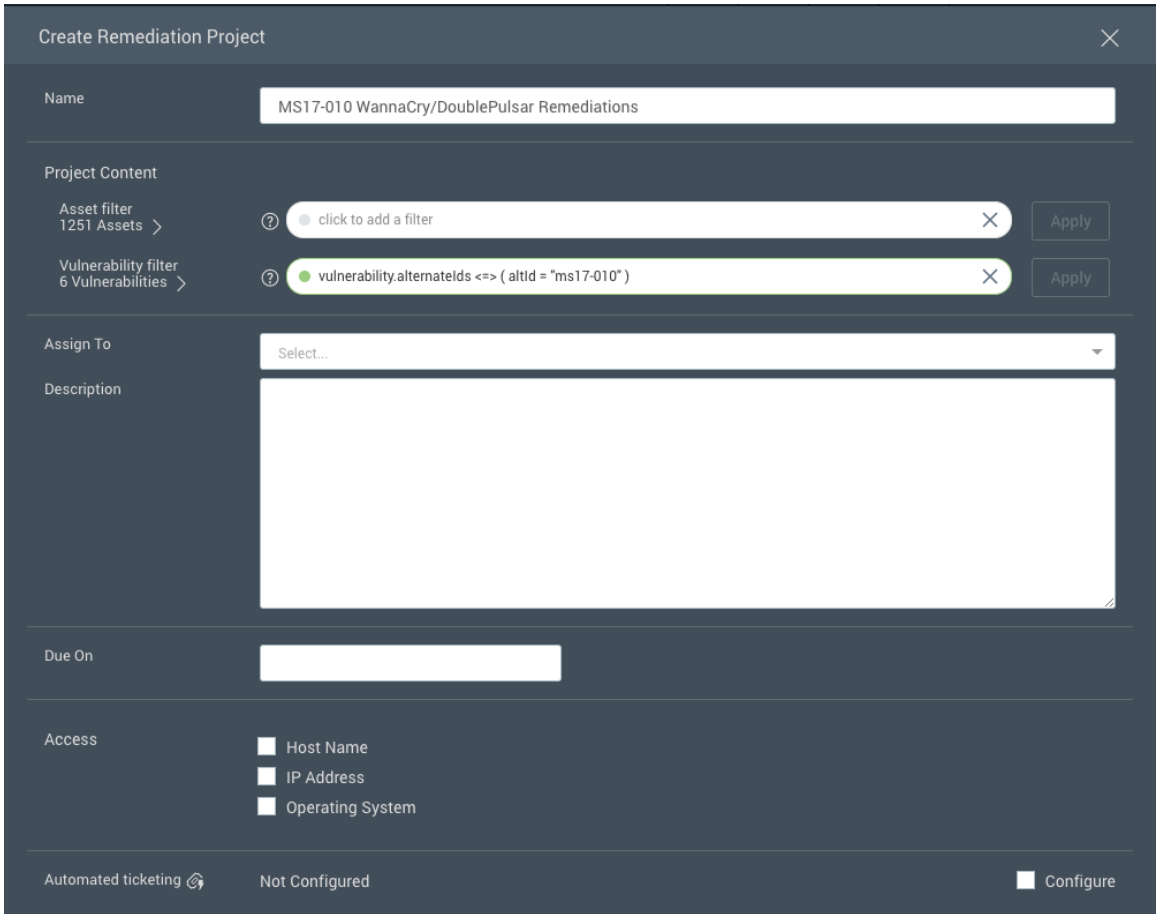
Creating Remediation Projects

Once you identify your exposure to a critical vulnerability, you want to ensure it's fixed as rapidly as possible across your entire network. Remediation Projects in InsightVM let you quickly send remediation steps to the specific team members responsible for affected systems, and track their progress in real time to patch vulnerabilities in a timely manner.

1. Go to the Projects tab and click Create a Project.



2. Name the project, and use the following format for your filter: “vulnerability.alternateIds”. In the example below, we use “MS17-010”; you can also use individual CVEs.



3. Give the project a description, configure who is responsible for remediation, and set appropriate access levels.

   If you use Jira Software or ServiceNow ITSM, you can also configure the automatic ticketing integration between InsightVM and Jira or ServiceNow to automatically assign tickets to the right people. This project will update automatically as vulnerabilities get fixed, or as newly vulnerable devices are discovered.

Using these steps, you’ll be able to easily assess, prioritize, and remediate any new critical vulns that come up.

Check out blog.rapid7.com for the latest threat analyses and advisories.

To get started for free, visit rapid7.com/try/insightVM.

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Customers around the globe rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, visit our website, check out our blog, or follow us on Twitter.