tenable

SOLUTION OVERVIEW

TENABLE FOR SERVICENOW® VULNERABILITY RESPONSE

AUTOMATING RESPONSE TO CYBER EXPOSURE

BUSINESS CHALLENGE

Security and IT Teams struggle with identifying and managing their vulnerabilities, but more importantly, fail to do this with a scalable approach. Not being able to assign and track actual vulnerability remediation leads to long response times, errors, operational inefficiencies of Vulnerability Response programs.

SOLUTION

The Tenable® integration for ServiceNow® Vulnerability Response offers best-in class, closed loop remediation by combining ServiceNow's industry-leading security orchestration, automation, and response engine with Tenable's market leading Cyber Exposure platform.

The integrated solution provides both IT and Security teams the ability to coordinate and streamline the management, prioritization and remediation of all your vulnerabilities. Together, Tenable and ServiceNow provide vulnerability intelligence for your applications, systems and devices, while automating the tracking of security issues to quickly and effectively automate response to vulnerabilities.

VALUE

The Tenable App for ServiceNow Vulnerability Response provides:

- Automated syncing of all vulnerabilities for continuous monitoring and remediation
- Centralized reporting on all past and present vulnerable systems
- Easily scheduled remediation scans for closed-loop remediation (Tenable.sc only)
- Fully customizable while maintaining upgradability
- Unique fields are included and tracked across records, VPR is viewable
- Configured scheduling to receive the most up to date vulnerability information

servicenow™

TECHNOLOGY COMPONENTS

- Tenable.io, Tenable.sc 5.7 or Tenable.ot 3.11
- Tenable for Assets
- Tenable for Vulnerability Response
- ServiceNow Paris, Quebec or Rome
- ServiceNow Security Operations Vulnerability Response
- ServiceNow Domain Separation (Optional)

KEY BENEFITS

- **Respond quickly, reduce errors** through automation and orchestration
- **Reduce risk, exposure and loss** by prioritizing the most critical items to fix first
- **Improve operational efficiency** with coordinated response across IT and security teams
- **Scale processes** via parallel, repeatable and measurable workflows
- **Closed-loop remediation** via targeted re-scans

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

ABOUT SERVICENOW

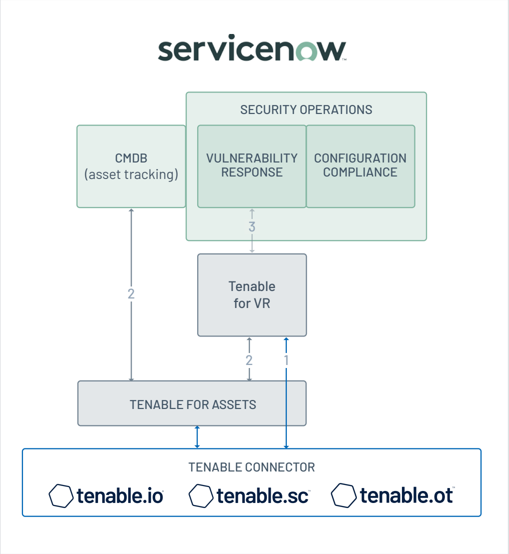
ServiceNow was started in 2004 with the belief that getting simple stuff done at work can be easy, and getting complex multi-step tasks completed can be painless. From the beginning, ServiceNow envisioned a world where anyone could create powerful workflows to get enterprise work done. Today, ServiceNow's cloud-based platform simplifies the way we work through a structured security response engine. ServiceNow Security Operations automates, predicts, digitizes, and optimizes security and vulnerability response to resolve threats quickly based on business impact. Reduce manual processes and increase efficiency across security and IT teams. ServiceNow is how work gets done.

Learn more at servicenow.com

FEATURES

With this integration, you can:

- Sync vulnerabilities from one or more instances of your Tenable platforms
- All Tenable platform fields are available on the corresponding records in ServiceNow, including VPR from Tenable
- Ensure CI's exist for all machines with vulnerabilities. (powered by Tenable for Assets)
- Launch remediation scans once patches have been applied (Tenable.sc only
- Automatically close vulnerable items when a vulnerability has been confirmed to be remediated (by Tenable)
- Leverage Tenable for Assets app matching and creating for all CI's



HOW IT WORKS

1. Get Vulnerabilities to sync from Tenable into ServiceNow VR
2. Use Tenable for Assets to get the correct CI for the given vulnerability to be imported
3. Create/Update Vulnerable item with data from Tenable

MORE INFORMATION

You can get the latest apps here: store.servicenow.com

Installation and configuration documentation: docs.tenable.com

For support please visit: community.tenable.com

Watch Tenable Apps for Service Now — Value Overview on YouTube

Case Study — Fortune 500 Oil & Gas Company