SOLUTION OVERVIEW

TENABLE FOR SERVICENOW® ITSM

OPTIMIZE YOUR SECURITY PROGRAM WITHIN YOUR SERVICENOW ENVIRONMENT

Business Challenge

Vulnerability management programs are constantly plagued with manual remediation processes that prove to be inaccurate, time consuming and pose communication barriers between security and IT teams. Sending weekly emails and spreadsheets to track vulnerability information lacks scalability and increases the risk for the organization.

Solution

The Tenable® integration for ServiceNow® Information Technology Service Management (ITSM) allows you to bring rich vulnerability information from Tenable into ServiceNow to automate the creation of tickets for high and critical vulnerabilities. This allows you to bridge the digital divide between the Security Teams and the IT remediators by sharing one common operating environment, using the industry-leading ITSM platform from ServiceNow.

Value

The Tenable for ITSM integration provides the ability to:

- Replace manual methods of emails, spreadsheets and documents for sharing vulnerabilities across teams
- Gain enhanced visibility into your vulnerability program
- Deploy an entry-level solution for customers without the ServiceNow Vulnerability Response module
- Have a common view of vulnerability tickets across IT and Security teams
- Utilize a solution to close the knowledge gap between IT and Security teams, which can now both work from the same playbook of vulnerabilities

Technology Components

- Tenable for ITSM
- Tenable Vulnerability Management and/or Tenable Security Center
- Tenable Connector
- Service Graph Connector for Tenable for Assets
- ServiceNow Vancouver, Washington DC
- ServiceNow Domain Separation (Optional)

.Key Benefits

- **Respond quickly and reduce errors** through automation and orchestration
- **Reduce risk, exposure, and loss** by prioritizing the most critical items to fix first
- **Improve operational efficiency** by standardizing process
- **Increase communication** with coordinated response across IT and Security Teams

About Tenable

Tenable® is the Exposure Management company. Approximately 43,000 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 approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.

Learn more at www.tenable.com.

About ServiceNow

ServiceNow (NYSE: NOW) makes the world work better for everyone. Our cloud-based platform and solutions help digitize and unify organizations so that they can find smarter, faster, better ways to make work flow. So employees and customers can be more connected, more innovative, and more agile. And we can all create the future we imagine. The world works with ServiceNowTM.

For more information, visit www.servicenow.com.

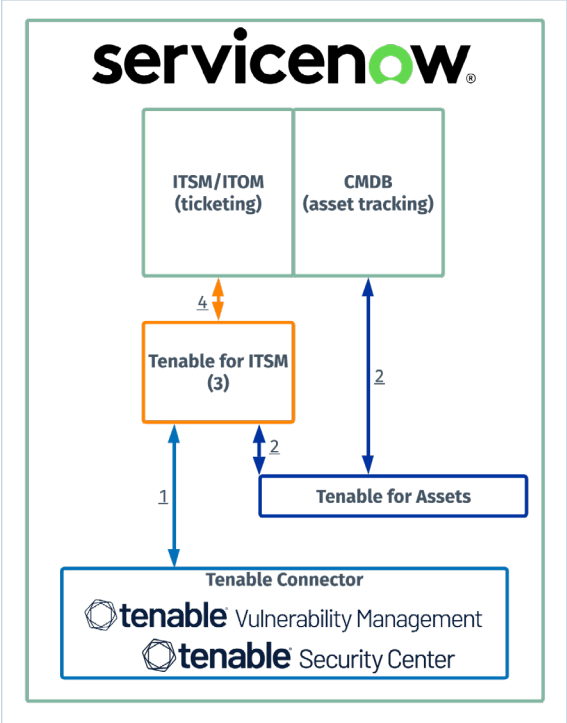
Features

With this integration, you can:

- Convert all high and critical Tenable vulnerabilities directly into ServiceNow incidents/tickets using rules
- Sync all high and critical vulnerabilities into ServiceNow ITSM
- Manage your vulnerabilities from Tenable within ServiceNow

How it works

1. Sync vulnerabilities from Tenable into ServiceNow Vulnerability Response
2. Use Service Graph Connector for Tenable for Assets to get the correct CI for the given vulnerability to be imported
3. Create/Update the vulnerability record in Tenable for ITSM
4. Run configured rules against vulnerabilities and create/update incidents in ServiceNow



More Information

Get the latest Tenable apps for ServiceNow here: store.servicenow.com
Installation and configuration documentation: docs.tenable.com
For support please visit: community.tenable.com