SOLUTION OVERVIEW

Business Challenge

The attack surface and threat landscape are continuously changing and organizations are constantly struggling with knowing their full picture of cyber risk when it comes to their IT, cloud and OT assets. The communication between security and IT teams is often limited due to the lack of having a centralized system to identify the most critical vulnerabilities and manage the remediation workflow process to stay on top of complex threats and growing security requirements. Without this tight integration, organizations are at risk with slow response times and poor visibility into their Cyber Exposure.

Solution

The Tenable® integration with ServiceNow® offers best-in-class security by combining ServiceNow's industry-leading security orchestration, automation, and response engine with Tenable's market leading Cyber Exposure platform to quickly and effectively automate remediation response based on actual risk. The integrated solution provides a cohesive platform for both IT and security teams to streamline the vulnerability management, prioritization and remediation of all your organization's critical assets.

Value

The Tenable suite of ServiceNow apps provide:

- Tenable Connector: A simple standardized library to configure how to connect to your Tenable platform(s)
- Tenable for Assets: Bi-directional Asset Syncing between Tenable Platforms and ServiceNow CMDB
- Tenable for IT Service Management: Bring Tenable Critical and High Severity findings into ServiceNow as incidents to start building out workflow/process
- Tenable for Vulnerability Response: Bring all of your Tenable findings into ServiceNow Vulnerability Response and leverage all the powerful pre-built functionality of Vulnerability Response

Technology Components

- Tenable.io/Tenable.sc
- Tenable Connector
- Tenable for Assets
- Tenable for ITSM
- Tenable for Vulnerability Response
- ServiceNow Orlando or Paris

Key Benefits

- Respond quickly, reduce errors through automation and orchestration
- Closed-loop remediation via targeted re-scans
- Reduce risk, exposure and loss by prioritizing the most critical vulnerabilities to fix first
- Improve operational efficiency with coordinated response across IT and security teams
- Scale processes via parallel, repeatable and measurable workflows
The diagram above shows the relationship between the Tenable Suite of ServiceNow Apps for Vulnerability Response, Ticketing (ITSM), Asset Tracking (CMDB) and the Tenable Connector.

This image above shows a vulnerable asset within ServiceNow that contains vulnerability information such as risk rating, risk score and the Tenable Vulnerability Priority Rating (VPR).

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