Automate cyber exposure response using Tenable and ServiceNow

The challenge

Unpatched vulnerabilities leave your organization exposed. With the discovery of a security vulnerability, time is of the essence for rapid, seamless execution of remediation processes. The tight integration between your cyber exposure and security response platforms can be the difference between keeping your IT environment safe, or becoming the victim of a breach.

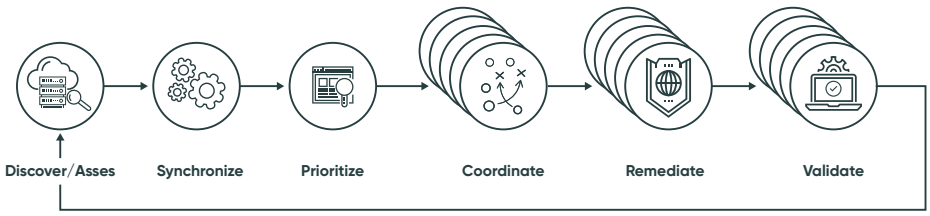
The attack landscape is continuously changing and growing, while security teams are constantly understaffed yet overwhelmed with both alerts and vulnerabilities. Communication between security and IT teams is also often limited because they are siloed. Existing IT staff typically deal with many areas of IT operations, so it's difficult for them to stay on top of evolving complex threats and growing security requirements.

Bringing advanced vulnerability visibility into workflows that connect security and IT enables you to develop strong and repeatable vulnerability management and remediation procedures–ensuring operational consistency.

The Solution

Tenable™ and ServiceNow offer an industry-leading security solution by combining powerful vulnerability assessment with a security orchestration, automation, and response engine to quickly and effectively remediate security weaknesses. The integrated solution provides you with a single response platform for continuous visibility and critical context across the enterprise. It enables decisive actions and granular remediation process control to protect your organization from risk, exposure, and loss.

Together, Tenable and ServiceNow provide vulnerability intelligence for your applications, systems, and devices, while automating the tracking of security issues while minimizing the time spent on manual processes. Integrations provide the seamless import of Tenable.io™ and Tenable SecurityCenter® scan data into ServiceNow® Security Operations, eliminating the traditional silos between security and IT often present in an organization.



Tenable's comprehensive solution includes complete visibility into your enterprise to ensure you have the context for informed action with the first cyber exposure platform designed to protect any asset on any computing platform.

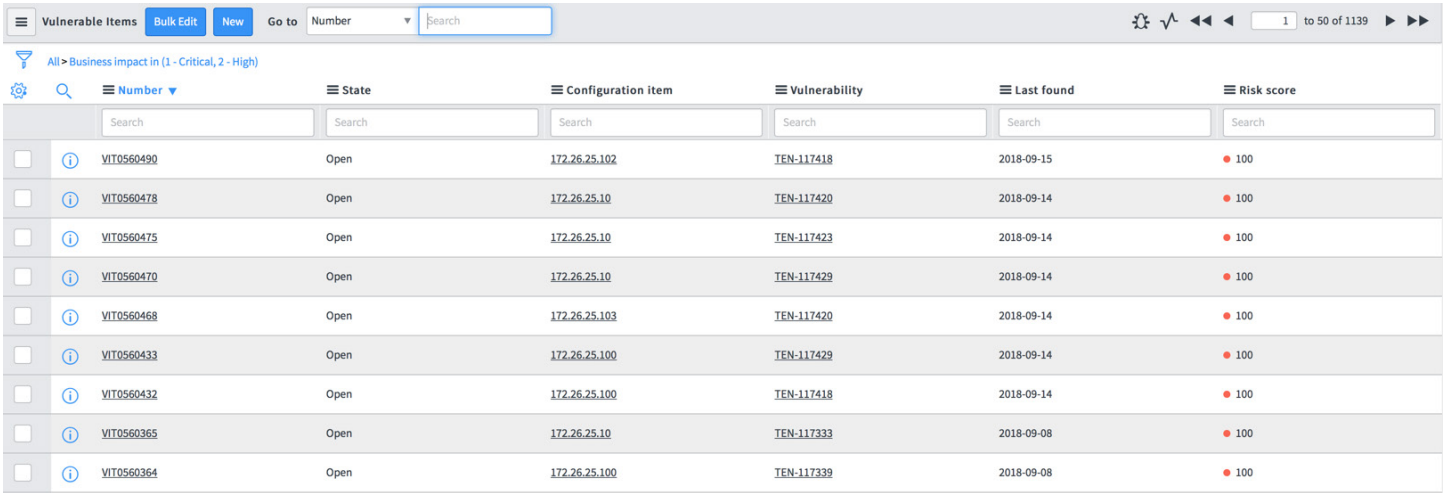
Integration with the ServiceNow® Configuration Management Database (CMDB) means vulnerable assets are prioritized by both severity of the vulnerabilityand the criticality of the asset. A configurable risk score calculator provides granular prioritization in Security Operations to ensure the most critical threats are addressed first. Additionally, asset data can be synced between Tenable.io and ServiceNow to ensure you have complete and accurate visibility of your network available to both security and IT teams.

In Partnership with

tenable™

Benefits

- Eliminate silos of security data by enabling security, vulnerability, and IT teams to work together.
- Prioritize response by combining Tenable vulnerability data with ServiceNow business context to find the most critical vulnerabilities.
- Respond quickly by automatically delivering data from Tenable's cyber exposure platforms to ServiceNow® Security Operations.



Number	State	Configuration item	Vulnerability	Last found	Risk score
VIT0560490	Open	172.26.25.102	TEN-117418	2018-09-15	100
VIT0560478	Open	172.26.25.10	TEN-117420	2018-09-14	100
VIT0560475	Open	172.26.25.10	TEN-117423	2018-09-14	100
VIT0560470	Open	172.26.25.10	TEN-117429	2018-09-14	100
VIT0560468	Open	172.26.25.103	TEN-117420	2018-09-14	100
VIT0560433	Open	172.26.25.100	TEN-117429	2018-09-14	100
VIT0560432	Open	172.26.25.100	TEN-117418	2018-09-14	100
VIT0560365	Open	172.26.25.10	TEN-117333	2018-09-08	100
VIT0560364	Open	172.26.25.100	TEN-117339	2018-09-08	100

Vulnerability findings imported from Tenable into ServiceNow Security Operations are prioritized by risk score, which can include vulnerability severity or age, the criticality of the affected asset, and more in its calculation.

When security and IT teams both work in ServiceNow, hand-offs of vulnerability remediation tasks are simple. Automated workflows reduce time spent on manual process, and integrated remediation targets and service level agreements ensure all tasks are complete across teams. Security teams get visibility into the status of IT tasks while sensitive security data is kept confidential. Dashboards and reporting provide greater visibility into status, performance, and security posture.

The Tenable and ServiceNow integrated solution gives your security team a single response platform for complete visibility and control in assessing and responding to vulnerabilities. The Tenable for ServiceNow Security Operations applications are available from the ServiceNow Store for customers of both the Vulnerability Response application of ServiceNow Security Operations and Tenable.io or Tenable SecurityCenter.

About Tenable

Tenable™, Inc. is the Cyber Exposure company. Over 24,000 organizations of all sizes around the globe rely on Tenable to manage and measure their modern attack surface to accurately understand and reduce cyber risk. As the creator of Nessus®, Tenable built its platform from the ground up to deeply understand assets, networks and vulnera- bilities, extending this knowledge and expertise into Tenable.io™ to deliver the world's first platform to provide live visibility into any asset on any computing platform. Tenable customers include over 50 percent of the Fortune 500, large government agencies and organizations across the private and public sectors. Learn more at **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 multistep 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, 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. For more information, visit **servicenow.com**.

servicenow