tenable

SOLUTION OVERVIEW

TENABLE OT SECURITY & SERVICENOW

COMPREHENSIVE VISIBILITY, SECURITY AND EFFECTIVE RESPONSE

Business Challenge

Operational technology (OT) is any device that is managed digitally and interacts with the physical world. Digital transformation has increased the adoption of IT and OT devices in the operational environment, making them vital for operations across critical infrastructure and many verticals, such as manufacturing, energy, transportation, utilities, and more. Much like in IT, OT devices have security vulnerabilities that need to be remediated through security patching, and if that's not possible, a risk mitigation plan needs to be implemented.

Digitization has opened up additional attack vectors, keeping the attack surface continuously changing and expanding. Security teams are constantly understaffed and overwhelmed with alerts and vulnerabilities to manage. Communication between security and OT teams is also often limited because they are siloed. Organizations need advanced visibility and workflows that connect security and OT, enabling the teams to develop strong and repeatable vulnerability management and remediation processes ensuring procedural consistency and operational continuity.

Solution

Tenable OT Security serves security and OT engineers with comprehensive visibility, security, and effective response control across converged operations, without disrupting productivity. Tenable and ServiceNow unite OT security programs with workflow management so security teams can effectively secure the expanding attack surface. ServiceNow receives critical intelligence from Tenable OT Security, revealing crucial information about digital services and the infrastructure that supports them. It enables key operational processes, helping security staff to predict, prevent, and resolve service outages, minimize the risk of changes, and respond quickly to end users.

Tenable and ServiceNow collaborated to shape the ServiceNow OT data model, which was subsequently integrated into Tenable applications to provide a unified user experience. The Service Graph Connector for Tenable for Assets now effectively synchronizes and reconciles assets across Tenable Vulnerability Management, Tenable Security Center, Tenable OT Security, and the ServiceNow Configuration Management Database (CMDB). Leveraging Tenable's advanced discovery and scanning technology alongside ServiceNow's extensive CMDB, accurate asset tracking and vulnerability management becomes seamless.

servicenow

ServiceNow-Certified Solutions

- **Tenable Connector:** A simple standardized library to configure how to connect to your Tenable platform(s)
- **Service Graph Connector for Tenable for Assets:** Bi-directional asset syncing between Tenable platforms and ServiceNow CMDB
- **Tenable.ot for Vulnerability Response:** Bring all of your Tenable findings into ServiceNow Vulnerability Response and leverage all of Tenable's proprietary threat intelligence

.The Challenge

- OT environments consist of IT and OT devices that operate differently than traditional IT devices on a corporate network
- OT engineers have unique constraints limiting frequent OT device vulnerability remediation
- OT system vulnerabilities can't always be patched, requiring a mitigation plan to secure the environment via alternative means
- OT environments are an additional attack vector threat actors can use to infiltrate the corporate network, or vice versa, enter from the corporate network to attack a physical production environment

Key Benefits

- Eliminate silos by enabling security, vulnerability, and OT teams to work together
- Respond quickly and reduce errors through coordinated vulnerability response for IT, IoT and OT devices
- Extend your existing workflows and ticketing system beyond IT operations to include IoT and OT devices
- Maximize visibility, security, and control across your entire operations through streamlined vulnerability management

When fully integrated, Tenable OT Security and ServiceNow extend beyond operations into areas such as planning, application development, deployment, cost optimization, and more, creating a broad and deep data foundation that helps organizations manage the entire digital service lifecycle.

Features:

- Automated syncing of all vulnerabilities for continuous monitoring and remediation
- Automated prioritization of the most vulnerable systems
- Correlated asset details with vulnerability information for enhanced risk scoring
- Central reporting on all past and present vulnerable systems
- Vulnerability matching to assets without duplication
- ServiceNow Operational Technology (OT) Certified

Value

Tenable's partnership with ServiceNow delivers a fully integrated solution to help organizations achieve faster OT vulnerability response rates, improve operational transparency, and create a more digitally secure working environment for OT operators and information security teams. Tenable OT Security provides unobstructed visibility, comprehensive asset inventory, robust vulnerability management, and device configuration monitoring. When combined with ServiceNow's functionality, OT organizations can have confidence in the security, resilience, and highly streamlined workflows and responses within their operational environment.

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.

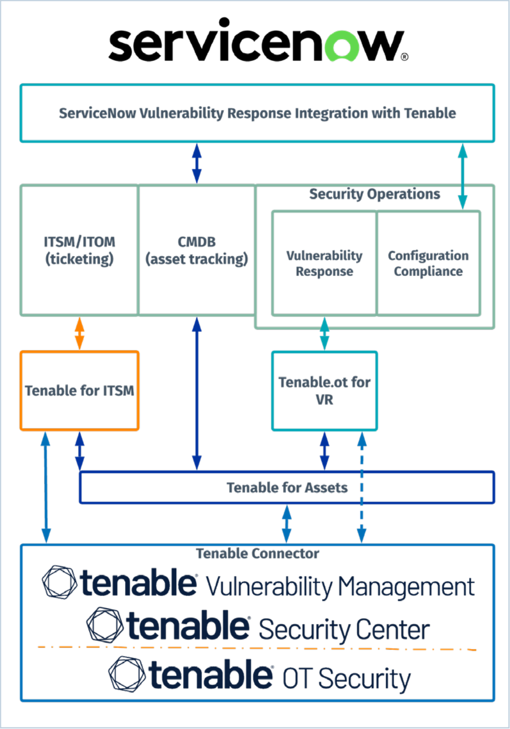
Learn more at www.tenable.com.

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.

Combined Solution



The integrated solution provides the ability to coordinate and streamline the management, prioritization and remediation of all your IT and OT vulnerabilities. Together, Tenable and ServiceNow provide improved operational efficiency and vulnerability intelligence for your applications, systems, and devices to automate the tracking of security issues to quickly and effectively respond to threats. 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. Please note: Tenable OT Security does not feed into ITSM.

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