Solution Brief

Tenable and ServiceNow

Maximize Remediation With Vulnerability Data

The Challenge

Achieving IT Operations uptime goals and meeting the IT Security team's risk objectives can be challenging. With the discovery of a security vulnerability, time is of the essence for rapid, seamless execution of remediation processes. The tight integration between your vulnerability detection solution and your IT service management (ITSM) platform, such as ServiceNow, can be the difference between keeping your IT environment safe or falling out of compliance and being victim of a breach.

The attack landscape is continuously changing and growing, but staffing levels for ITSM administration are usually static since the economic climate requires everyone to "do more with less." Existing ITSM 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 and remediation data into ITSM workflows reduces your reliance on highly specialized vulnerability response professionals for day to day operations and enables you to develop strong and repeatable vulnerability management and remediation procedures, ensuring operational consistency.

The Solution

Tenable™ and ServiceNow offer best-in-class security by combining the industry's leading ITSM application with powerful vulnerability detection 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 and compliance intelligence for your applications, systems and devices, while automating the tracking of security issues and minimizing the time needed for manual processes. The integration provides the seamless import of Tenable SecurityCenter® scan data into ServiceNow Security Operations, eliminating the traditional security silos often present in an organization. Tenable's comprehensive solution includes unique sensors to ensure you have the visibility and context for informed action. Sensors include active scanning, agent scanning, intelligent connectors, passive listening and host data.

ServiceNow enables granular manipulation of vulnerability data transfer queues to improve automated workflows and reports. With the integrated scan data, administrators can use the ServiceNow console to drill down into vulnerability data and better guide remediation processes. The automated workflows can reduce human errors and ensure completeness of data. This also reduces the need for specialized, highly experienced security personnel to diagnose and prioritize threat remediation, and to ensure compliance. The Tenable for ServiceNow Security Operations application will be available at no charge on the ServiceNow app store for customers who own both ServiceNow Security Operations and Tenable SecurityCenter.

Components:

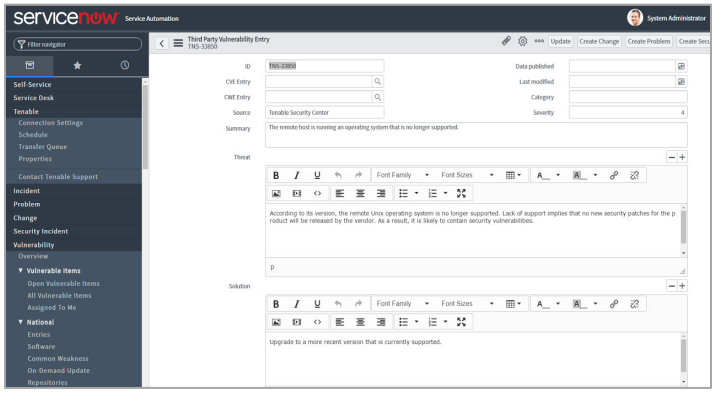
- Tenable SecurityCenter 5.x or higher
- Tenable SecurityCenter administrator account dedicated to ServiceNow integration
- ServiceNow subscription to Security Operations "Module"
- ServiceNow MID server installed and registered within your ServiceNow instance

Benefits:

- **Automatically delivers scan results** from Tenable's unique sensors for continuous monitoring of network and host vulnerabilities
- **Eliminates silos of security data** with automated workflows and reports in ServiceNow that enhance visibility of IT vulnerabilities, how they may affect your network and how to fix them
- **Enhances response** by automatically prioritizing workflows without requiring manual intervention and specialized knowledge about security or compliance
- **Minimizes errors** by providing Tenable vulnerability data in ServiceNow ticketing format with context and details for immediate action

How It Works

1. ServiceNow schedules data request task from Tenable SecurityCenter
2. SecurityCenter returns vulnerability & remediation data based on request parameters
3. ServiceNow Security Operations leverages data from SecurityCenter to prioritize remediation activities
4. ServiceNow Security Operations workflows assign and track remediation activities using input from SecurityCenter data
5. Report on vulnerability remediation status through ServiceNow Security Operations



The ServiceNow Security Operations console enables administrators to drill down on vulnerability scan data imported from Tenable SecurityCenter, revealing granular information that helps direct remediation teams to quickly fix urgent vulnerabilities.

The Tenable and ServiceNow integrated solution gives your security team a single-response platform for complete visibility and control in assessing and responding to incidents and vulnerabilities. To learn more about ServiceNow solutions, visit servicenow.com. To learn more about Tenable solutions, visit tenable.com.

About ServiceNow

ServiceNow is changing the way people work. With a service-orientation toward the activities, tasks and processes that make up day-to-day work life, we help the modern enterprise operate faster and be more scalable than ever before. Customers use our service model to define, structure and automate the flow of work, removing dependencies on email and spreadsheets to transform the delivery and management of services for the enterprise. ServiceNow enables service management for every department in the enterprise including IT, human resources, facilities, field service and more. We deliver a 'lights-out, light-speed' experience through our enterprise cloud – built to manage everything as a service. To find out how, visit servicenow.com.

About Tenable

Tenable™ transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss. With more than one million users and more than 21,000 customers worldwide, organizations trust Tenable for proven security innovation. Tenable customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus® and leaders in continuous monitoring, by visiting tenable.com.

tenable™

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact