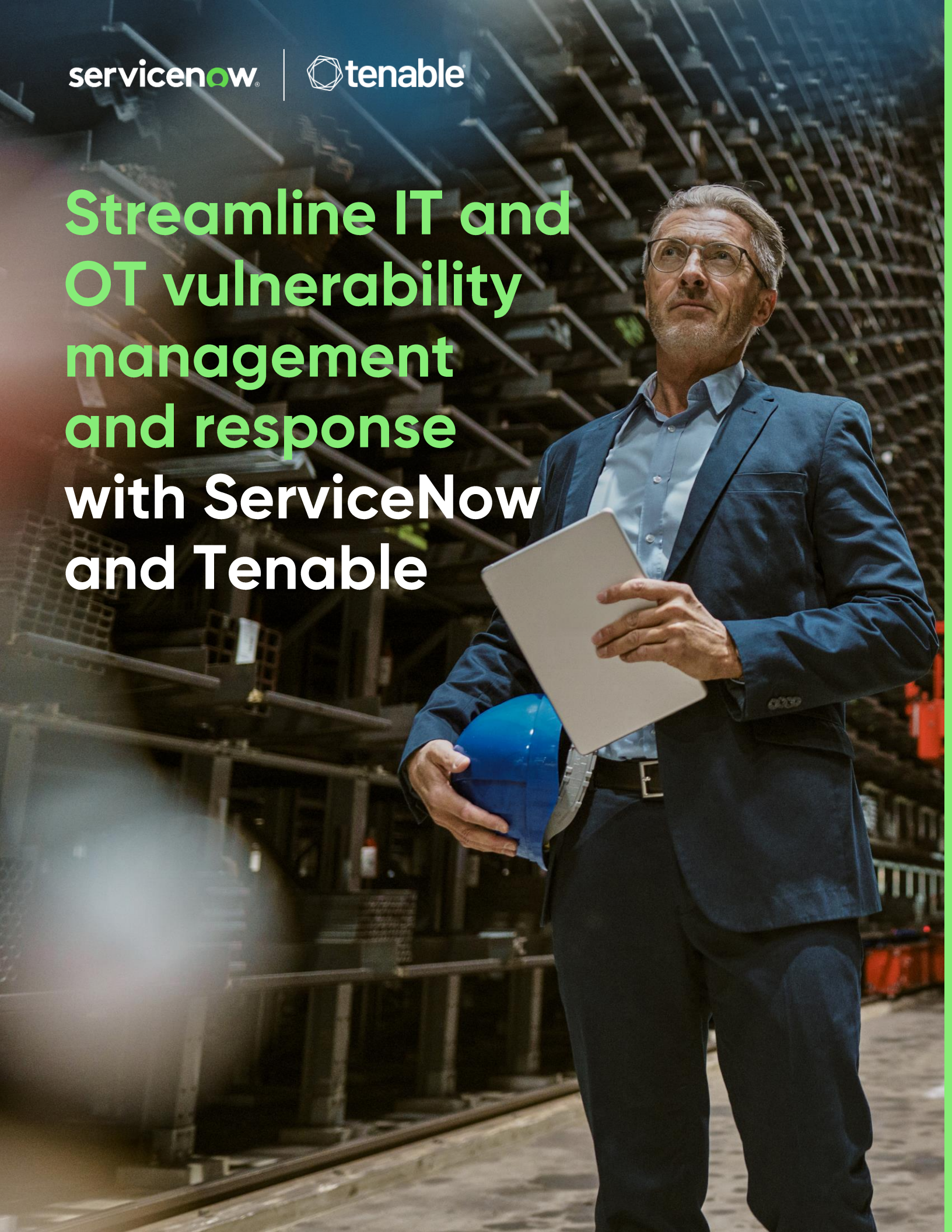
servicenow | tenable

Streamline IT and OT vulnerability management and response with ServiceNow and Tenable



Industrial operations are changing.

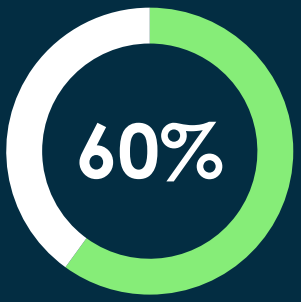
Industry 4.0 initiatives are transforming industrial facilities while bringing connectivity to once air-gapped industrial control systems (ICS) and operational technology (OT) devices. Converging informational technology (IT) with operations allows for more efficiency—but at the risk of an increased attack surface. In this highly connected environment, asset management—across both IT and OT—becomes much more complicated.

Couple this with an asset management process that often leaves OT assets unaccounted for due to manual processes and paperwork, and more challenges arise. A siloed approach limits visibility and with asset information likely incomplete or inaccurate, unaddressed vulnerabilities remain. When you can't track all your assets, know how they are configured, and how critical they are to operations, it's impossible to take an efficient approach to vulnerability management and response.

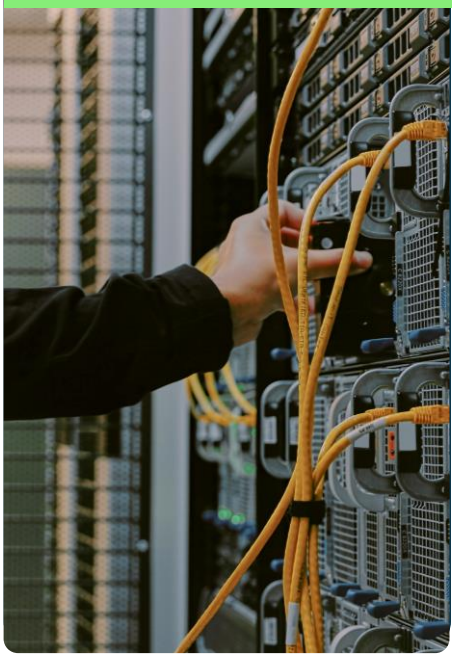
Yet even with a comprehensive view of all assets, you need a strategic approach for detecting and prioritizing vulnerabilities. Every day brings thousands of vulnerabilities to address. How can you identify the ones that pose the biggest threats?

Then, there's the management of remediation. When security teams are responsible for identifying and assessing vulnerabilities and IT teams manage the remediation, work happens in silos. This delays remediation efforts—resulting in more time exposed to threats that could bring your enterprise to a halt. You need an approach that simplifies your processes and drives frictionless collaboration between IT and security teams.

Tenable and ServiceNow provide streamlined IT and OT vulnerability management. With a comprehensive approach to easily view, prioritize, and remediate converged IT and OT vulnerabilities all in one place—maximizing uptime.



of organizations say by spending time chasing down false positives and minor vulnerabilities, **the most dangerous vulnerabilities continue to expose valuable assets.***



Gain comprehensive visibility

Unify prioritization

Automate remediation workflows

servicenow | tenable

Gain comprehensive visibility across your entire IT and OT estate.

It's impossible to run a successful vulnerability management program without a comprehensive view of all your assets in one place. End-to-end visibility is the foundational tool for protecting your enterprise from unplanned downtime.

Using a secure platform, gain a complete view of all your IT and OT devices and capture more dynamic information about each asset.

Map all IT and OT assets

- ✓ Gain visibility across your entire IT and OT estate, then automate the process of finding and mapping assets.
- ✓ Capture dynamic information, including system interconnectivity, data on updates or upgrades, and business criticality.
- ✓ Easily identify how vulnerabilities in one asset may impact the entire system.
- ✓ Support cross-team visibility with a secure platform that is accessible from anywhere.

Increased connectivity of OT devices to internet-facing systems and services is a primary reason organizations have seen their attack surface grow.

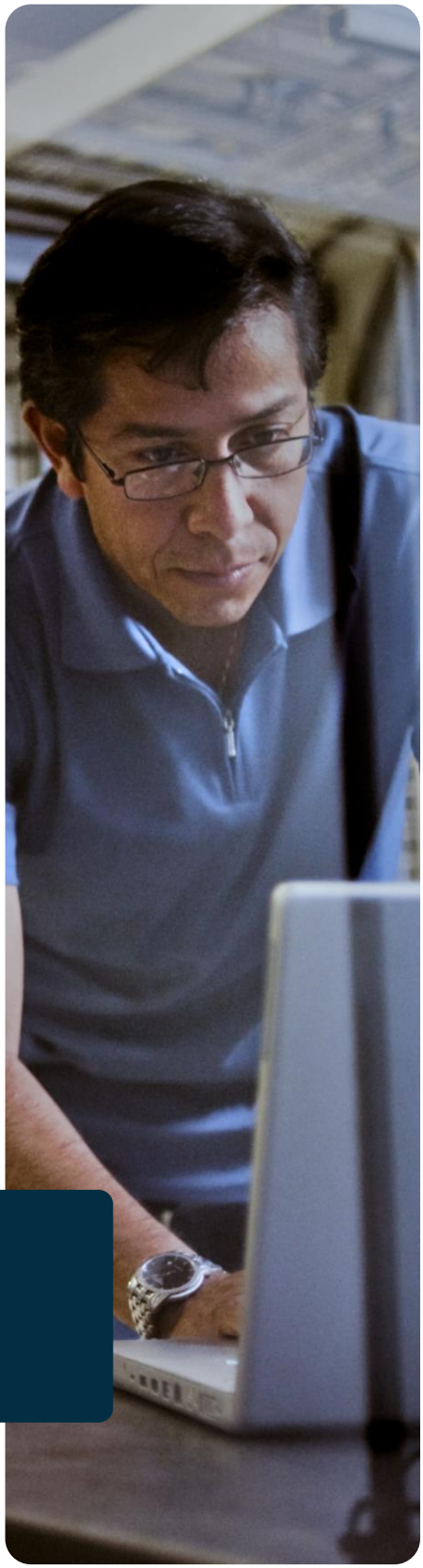
Enterprise Strategy Group: Security Hygiene and Posture Management, 2021

servicenow | tenable

Unify prioritization with a digitized workflow approach.

Limited resources and siloed data constrain security teams from operating efficiently. Visibility is an issue, but even organizations with complete visibility face the challenge of quickly and accurately identifying risk.

A risk-driven approach that combines vulnerability data, threat intelligence, and asset criticalities can help you streamline remediation efforts and focus on vulnerabilities that are most likely to be exploited.



Evaluate vulnerabilities holistically

- ✓ Identify vulnerabilities across IT and OT using a combined list, eliminating security blind spots.
- ✓ Streamline vulnerability management to improve cross-team coordination.

Determine highly exploitable vulnerabilities

- ✓ Identify vulnerabilities that are likely to be exploited based on threat intelligence, past threat patterns, and NVD data.
- ✓ Reduce guesswork, reactionary remediation efforts, and wasted resources by focusing on the top 3% of vulnerabilities that have been or will likely be exploited.
- ✓ Use predictive prioritization to track changes to vulnerability criticalities in real time.

57% of organizations don't know which vulnerabilities pose the highest risk to their business.*

servicenow | tenable

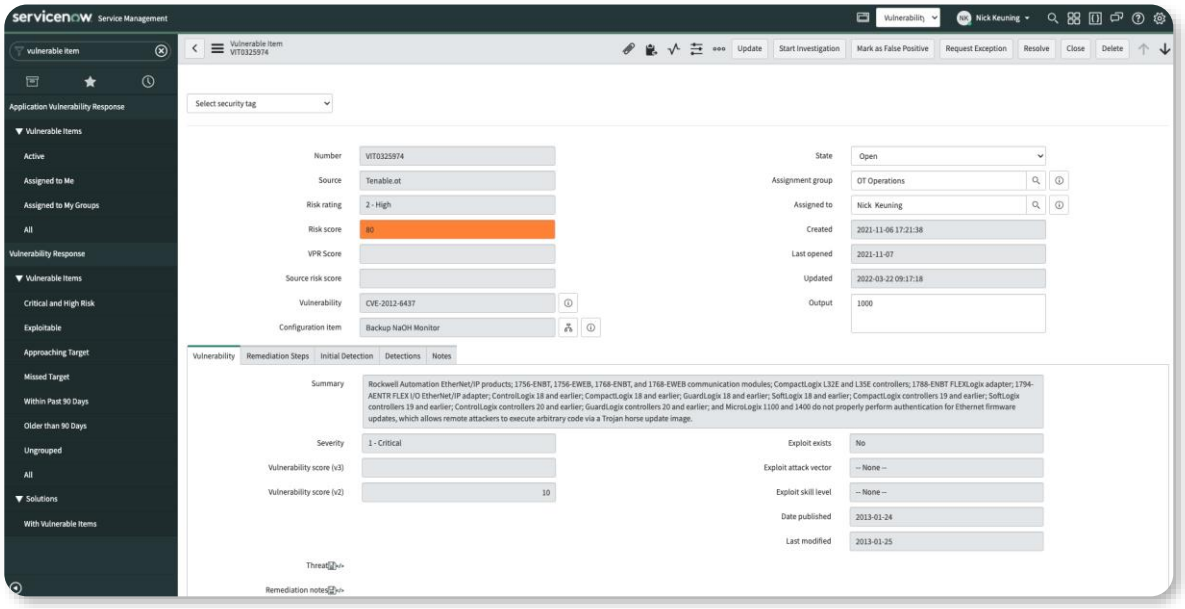
Automate end-to-end remediation workflows.

You have remediation processes in place—but they don't always go according to plan. When remediation efforts face delays due to manual processes and siloed data, organizations are left exposed.

You can quickly and effectively take an automated response to end-to-end remediation efforts based on actual risk with the Now Platform®. Then, validate whether your vulnerability remediation actions were successful and close the loop.

Implement a coordinated, automated response

- ✓ Unify remediation workflows in one place, so you can act on prioritization recommendations faster and reduce errors.
- ✓ Use automated digital workflows to connect the right people at the right time with the information they need to address the vulnerability with automated digital workflows.
- ✓ Drive frictionless collaboration between IT and security teams with automated emergency response workflows that notify stakeholders and create high-priority patch requests for IT.
- ✓ Easily identify vulnerabilities with similar threat characteristics with an enterprise view—enabling a quick response to future threats.



Bring vulnerability context from Tenable into an automated ServiceNow workflow, quickly routing remediation tasks to the right OT Ops/remediation team member.

Take a comprehensive approach to vulnerability response.

New technologies continue to drive innovation within operations and IT, connecting more devices. The problem? This contributes to an expanded attack surface that a traditional vulnerability management approach is not well-equipped to handle. Isolated siloes, disconnected teams, and manual processes make it challenging to gain a complete view of all threats and vulnerabilities across all endpoints—let alone easily prioritize and remediate them.

It's time to take a new approach to vulnerability management—one that's truly comprehensive, addressing vulnerabilities across your entire IT and OT environment.

Tenable and ServiceNow power the future of streamlined security operations by converging IT and OT visibility, prioritization, and remediation all in one place.

Learn more about ServiceNow Security Operations.

Learn more about Tenable vulnerability management products.

*Ponemon: The state of vulnerability management in the cloud and on-premises

servicenow | tenable