

TENABLE APPLICATION SUITE FOR SERVICENOW®

MANAGE YOUR CYBER EXPOSURE WITHIN SERVICENOW

BUSINESS CHALLENGE

The threat landscape is continuously changing and organizations are constantly struggling with understanding the full picture when it comes cyber risk for their converged IT and OT assets along with elastic cloud environments. The communication and tracking of work between security and IT teams is often limited due to the lack of having a centralized system to identify the most critical vulnerabilities. This hinders the ability to effective manage the remediation workflow process to stay on top of complex threats and growing security requirements. Without a way to manage and centralize these processes, organizations are at risk with slow response times that ultimately increase their cyber risk.

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 effectively automate remediation response based on cyber risk. The integrated solution provides a cohesive platform for both IT and security teams to streamline the vulnerability management, prioritization and remediation of your converged IT/OT and cloud 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

servicenow

TECHNOLOGY COMPONENTS

- Tenable.io, Tenable.sc 5.7 or Tenable.ot 3.11
- Tenable Connector
- Tenable for Assets
- Tenable ITSM
- Tenable for Vulnerability Response
- ServiceNow Paris, Quebec or Rome
- ServiceNow Domain Separation (Optional)

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

ABOUT TENABLE

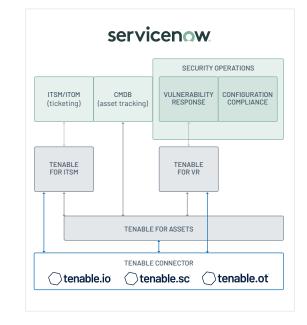
Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.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 multi-step 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, predicts, 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.

Learn more at servicenow.com

COMBINED SOLUTION



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.

servicenow Service Management				🗂 Good 🔹 🛞 Nick Kee	ଲାଟ ଟେଟିଡିଭି
🖓 wher 🛛 🛞	<		F	y T 🗄 *** Update Start Investigation	Close/Defer Delete 🛧 🗸
e \star O					
Volverability Response	Select security tag				
Overview					
Remediation Overview	Number	WT0312647	State	Open \$	
▼ Wiresbildes	Source	Tenable.io	Assignment group	٩,	
Waterability Groups	Risk rating	3 · Medium	Assigned to	٩,	
Vulnerable items	Pisk score	40	Greated	2029-12-16 15:48:49	
Open	Winesbillty	TDN-122784	(D) List opened	2023-12-16	
Assigned to Ne	Configuration item	epo59	A O Updated	2019-12-17 00:00:13	
Assigned to My Groups	Vulnerability Configuration Details Notes				
Ny Approvals	Summary The remote Windows host is affected by multiple vulnerabilities.				
Ungrouped Vulnerable Items					
▼ Ubraries	Severity		Exploit exists	No	
NND	Vulnerability score (x3)		Exploit attack vector	-None-	
CWE	Vulnerability score (x2)	53	Explait skill level	-None-	
Third-Party	VPR Score	15	Date published	2019-03-12	
▼ Vulnerability Scarving			Last modified	2018-10-31	
Frances Losses	These	The remote Windows host is missing security update 44858	183 or cumulative update 4485881. It is, therefore, affected by multiple vulnerabilities : - A	A remote code execution vulnerability exists when the	

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: <u>store.servicenow.com</u> Installation and configuration documentation: <u>docs.tenable.com</u> For support please visit: <u>community.tenable.com</u> Watch <u>Tenable Apps for Service Now — Value Overview</u> on YouTube Case Study — <u>Fortune 500 Oil & Gas Company</u>

() tenable

0HT2021TEMABLE, INC. ALL RIGHTS RESERVED. TEMABLE, TEMABLE, ID. NESSUS, ALSIDI, INDEOY, LUMIN, ASSURE, AND RELATION ROMOR ARE REGISTERED TRADEMARKS OF TEMABLE. INC. OR ITS AFFLIATES. TEMABLE. SO, TEMABLE O, T. LE AD, EXPOSIBLE, AL AND THE CYBER EXPOSIBLE COMPANY ARE TRADEMARKS OF TEMABLE. INC. OR ITS AFFILIATES. HIP ROMOLITISTO RESPURCES ARE TRADEMARKS OF TEMADEMARKS OF TEMABLE. INC. OR ITS AFFILIATES.

Solution Overview / ServiceNow AppSuite / 120221