Automated Vulnerability Management and Response

Benefits
- Ingest Tenable vulnerability alerts within Demisto for playbook-driven enrichment and response.
- Accurately identify threats, classify them according to risk and severity, and provide deep insights into every single alert.
- Shorten investigation and decision-making by automating key tasks into the analyst review cycle.

Compatibility
- Products: Demisto Enterprise, Tenable.sc, Tenable.io.
- Platform: Platform independent.

Overview
Vulnerability management is strategic to security operations and encompasses all computing assets. So, in order to effectively remediate vulnerabilities, security teams often grapple with having to correlate data and map context across environments.

This integration combines Tenable’s comprehensive vulnerability management capabilities with Demisto’s security orchestration and automation to help security teams standardize their incident response processes, execute repeatable tasks at scale, and accelerate time to detect and remediate vulnerabilities.

Integration Features:
- Automate ingestion of Tenable vulnerability scan results within Demisto for playbook-driven enrichment and response.
- Perform CVE enrichment on assets from scan results, calculate and assign vulnerability severity scores.
- Perform automated and/or manual remediation actions based on severity level according to predefined workflows.
- Leverage hundreds of Demisto third-party product integrations to enrich Tenable alerts and coordinate response across security functions.
USE CASE

AUTOMATED VULNERABILITY INGESTION, ENRICHMENT AND RESPONSE

Challenge: With ever-evolving threats and vulnerabilities, security teams are continuously in catch-up mode identifying vulnerabilities, assessing their impact, and remediating them through patching and configurations.

Solution: With the Demisto-Tenable integration, Tenable alerts are automatically ingested into the Demisto platform. Upon ingestion, automated playbooks enrich and add context to these alerts by remotely executing Tenable actions within Demisto. The playbook then hands off control to security analysts for further investigation or remediation.

Benefit: The solution will help analysts prioritize alerts based on severity level and the threat actor behind the attack, shortening the time from detection to response from hours to minutes. A more standardized process implemented via automated playbooks can pave the way to more proactive vulnerability management.

About Tenable
Tenable®, Inc. is the Cyber Exposure company. Over 27,000 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 25 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

About Demisto
Demisto, a Palo Alto Networks company, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Demisto, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit www.demisto.com.