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 #1  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 handoff control to security analysts for further investigation or remediation.
**USE CASE #2**

INTERACTIVE, REAL-TIME INVESTIGATION FOR COMPLEX THREATS

**Challenge:** While standardized, repeatable playbooks can automate commonly performed tasks to ease analyst load, an attack investigation usually requires additional tasks such as pivoting from one suspicious indicator to another to gather critical evidence, drawing relations between incidents, and finalizing resolution. Running these commands traps analysts in a screen-switching cycle during investigation and a documentation-chasing cycle after investigations end.

**Solution:** After running enrichment playbooks, analysts can then gain greater visibility and new actionable information about the vulnerability by running Tenable commands in the Demisto War Room. For example, if playbook results throw up alert details, analysts can retrieve details for a given vulnerability or get specific device information and also run commands from other security tools in real-time using the War Room, ensuring a single-console view for end-to-end investigation.

**Benefit:** The War Room allows analysts to quickly pivot and run unique commands relevant to incidents in their network from a single window. All participating analysts will have full task-level visibility of the process and be able to run and document commands from the same window. They will also prevent the need for collating information from multiple sources for documentation.

---

**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.