Automated Vulnerability Data Enrichment and Response

Benefits

- Seamlessly integrate vulnerability intelligence into your incident workflows.
- Eliminate dead time by using one platform to collaborate, investigate, and document.
- Shorten investigation and decision-making by automating key tasks in the incident lifecycle.

Compatibility

- Products: Demisto Enterprise, Risk Based Security’s VulnDB
- Platform: Platform independent

Vulnerability management is strategic to security operations and encompasses all computing assets. So, in order to effectively remediate vulnerabilities, security teams often have to correlate data and map context across environments. And with thousands of new vulnerabilities disclosed each year, security teams need a scalable way to identify critical assets at risk and resolve any associated vulnerabilities quickly.

This integration combines comprehensive vulnerability intelligence from Risk Based Security’s VulnDB® with Demisto’s security orchestration and automation platform 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 the ingestion of vulnerabilities affecting your asset inventory within Demisto for playbook-driven enrichment and response.
- Enrich investigation data with VulnDB’s intelligence on the latest vulnerabilities in end-user software and 3rd party libraries.
- Leverage hundreds of Demisto third-party product integrations to coordinate response and remediation across security functions.
- Run thousands of actions (including for VulnDB) interactively via a ChatOps interface while collaborating with other analysts and Demisto’s chatbot.
USE CASE #1  AUTOMATED DATA ENRICHMENT AND INCIDENT RESPONSE

**Challenge:** If security teams use different solutions for data enrichment and incident response, it can be tough to track the lifecycle of an incident due to fragmented information distributed across multiple locations. As a result, time is spent chasing data and completing low-level tasks rather than in actual remediation and resolution.

**Solution:** VulnDB alerts can trigger Demisto playbooks that automate enrichment and context addition for vulnerabilities before handing control over to the security analyst for further investigation. Automated tasks can include retrieving vendor and product information, CVE and vulnerability details, enriching endpoint and CVE data through relevant tools, creating tickets, quarantining endpoints and sending email communications. This balance of automated and manual ensures that security analyst time is not wasted in repetitive tasks but is focused on making critical decisions and drawing inferences.

**Benefit:** Automation of repetitive, manual tasks streamline incident lifecycle processes to speed and execute incident triage and resolution at scale.

USE CASE #2  INTERACTIVE, REAL-TIME INVESTIGATION FOR COMPLEX THREATS

**Challenge:** Apart from running automated actions, attack investigations usually require additional real-time tasks such as pivoting from one suspicious indicator to another to gather critical evidence, draw relations between incidents and finalizing resolution.

**Solution:** Demisto provides a single platform where analysts have visibility into correlated indicators from products across their security stack. They can gain new actionable information about a vulnerability by running VulnDB commands in the Demisto War Room. Analysts can also run commands from other security tools in real-time, ensuring a single-console view for end-to-end investigation. The War Room auto-documents all playbook and analyst actions and with time, will provide suggestions on analyst assignments and actions based on incident type and previous actions.
About VulnDB
VulnDB is the most comprehensive and timely vulnerability intelligence available and provides actionable information about the latest in security vulnerabilities via an easy-to-use SaaS Portal, or a RESTful API that allows easy integration into GRC tools and ticketing systems. VulnDB allows organizations to search and be alerted on the latest vulnerabilities, both in end-user software and the 3rd Party Libraries or dependencies. For more information, visit www.riskbasedsecurity.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.

Benefit: All participating analysts will have full task-level visibility into the process and be able to run and document commands from the same window. Auto-documentation of all automation and analyst actions allow for reports to be generated quickly for executive review or post-investigation debriefs.