



Automated Vulnerability Ingestion, Prioritization and Remediation

Products: Vulcan Platform, Qualys



Benefits

- Ingest Qualys vulnerability assessments within Vulcan for contextual risk-based prioritization of vulnerabilities and misconfigurations discovered.
- Shorten decision-making processes by automating key tasks within the remediation process.
- Manage all vulnerability remediation activities across cloud and on-prem environments from one single platform.
- Deploy accurate, efficient solutions on the most critical assets in the environment.
- Overcome misconfiguration that result in unscanned assets and gain visibility to your entire network.
- Unify all vulnerability data and asset inventories within Vulcan, leveraging Qualys data.

Overview

The spike of vulnerability disclosures, and the subsequent rise of vulnerabilities discovered in each network, has generated a requirement of a new approach to vulnerability management. Nowadays, in order to effectively remediate vulnerabilities, security teams need to accurately find all vulnerabilities in the network, prioritize them, and drive forward their remediation.

This integration combines Qualys' vulnerability scan results with Vulcan Cyber's remediation database & patch deployment capabilities. After Vulcan contextually prioritizes the vulnerabilities that pose the highest risk to the environment using its proprietary risk scoring algorithm, security teams can effectively remediate these high-risk items instantly by deploying the appropriate fix instantly and automatically, through the platform.



Integration Features

- Automate ingestion of Qualys scan results within Vulcan and perform automated, prioritized remediation measures to effectively reduce risk.
- Drive forward the remediation of vulnerabilities detected through predefined workflows, automating the remediation process.
- Leverage Vulcan's wide set of integrations to enrich Qualys scan results for accurate, contextual risk-based prioritization.
- Compare Qualys vulnerability scan results with asset data information to find misconfigurations resulting in unscanned assets, workloads and images in your cloud environment.

Use Case #1 Automated Vulnerability Ingestion, Prioritization and Remediation

Challenge

Security teams must overcome the endlessly-evolving threats and vulnerabilities discovered within their network. This requires identifying vulnerabilities, assessing their impact and driving forward their remediation.

Solution

Through the Vulcan-Qualys integration, Qualys scan results are ingested automatically within Vulcan. Upon ingestion, Vulcan's prioritization mechanism will identify the vulnerabilities that pose the highest risk to the environment. By contextualizing asset posture and incorporating threat intelligence, remediation efforts will be directed to the best effect. With Vulcan's automation engine, security teams will be able to scale their remediation efforts and automatically apply solutions to vulnerabilities discovered by Qualys.

Benefit

Automate the vulnerability remediation lifecycle from detection to resolution. Contextualize vulnerability scan data to improve the efficiency and productivity of all teams involved in the remediation process and leverage Vulcan's automation engine to remediate vulnerabilities at scale.

From the Platform - Automated Vulnerability Prioritization and Remediation

The screenshot shows the Vulcan Cyber platform interface. On the left, there's a sidebar with various navigation options: Dashboard, Vulnerabilities (selected), Campaigns, Automation, Assets, Solutions, Reports, and Connectors. The main area has two tabs: 'Pending (2822)' (selected) and 'In Progress'. Below this, it says 'All business group' and 'Showing 2822'. A large orange box indicates a 'High' priority vulnerability. To the right, there's a detailed view of a specific vulnerability: 'CentOS Security Update for curl (CESA-2019:1880)'. It shows a risk score of 7.4, exploitability, asset impact, and insights. On the far right, there are buttons for 'Ignore' and 'Take Action' (with dropdown menus for 'Open a ticket', 'Deploy a patch', and 'Share'). Below this, a table lists several other vulnerabilities with their names, scores (e.g., 9.8 VSS3), attack vectors (e.g., Remote), and tags (e.g., External Facing). All listed vulnerabilities have a date of 'Sep 15, 2019'.

Name	Score	Attack Vector	Tags	Date
CentOS Security Update for curl (CESA-2019:1880)	9.8 (VSS3)	Remote	External Facing	Sep 15, 2019
CentOS Security Update for curl (CESA-2019:1481)				Sep 15, 2019
CentOS Security Update for curl (CESA-2019:1587)				Sep 15, 2019
CentOS Security Update for curl (CESA-2019:1873)				Sep 15, 2019
CentOS Security Update for kernel (CESA-2019:1880)				Sep 15, 2019
CentOS Security Update for libssh2 Security Update (CESA-2019:1884)				Sep 15, 2019
CentOS Security Update for kernel (CESA-2018:1965)				Sep 15, 2019
CentOS Security Update for python (CESA-2018:2123)				Sep 15, 2019
CentOS Security Update for yum-utils (CESA-2018:2285)				Sep 15, 2019

Qualys is a security scanner that identifies vulnerabilities across networks, OSs, databases, web applications and wide variety of platforms through an integrated, robust scan engine

For more information, visit qualys.com

Vulcan Cyber is a vulnerability remediation automation platform that modernizes the way enterprises reduce their cyber risk. From detection to resolution, Vulcan automates and orchestrates the vulnerability remediation process dynamically and in scale

For more information, visit vulcan.io