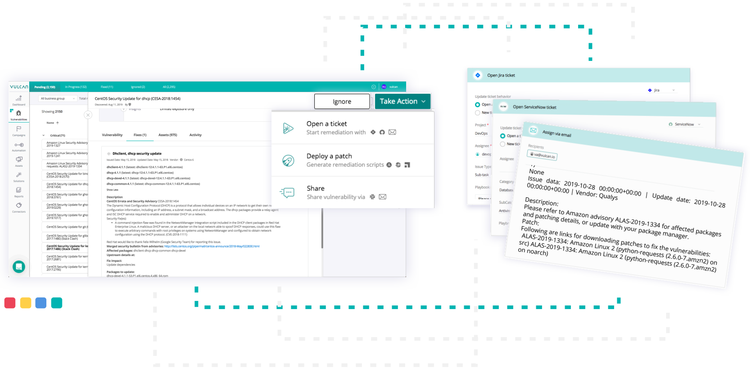
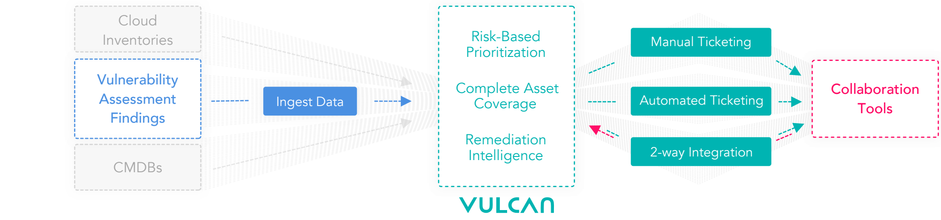


Automating Scan Results Into Actionable Remediation Tickets

OVERVIEW

Nowadays, vulnerability remediation processes have become more intricate than ever before. The diversity and flexibility of infrastructures and applications have created a wider threat landscape. Combined with enterprise software being more interconnected and business-critical, patching one component in production may have devastating implications on the business.

Moreover, the spike of vulnerability disclosures and the subsequent rise of vulnerabilities discovered in each network has generated a requirement for a new approach to vulnerability management.

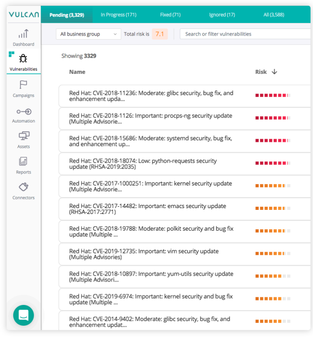


The Vulcan platform enables security teams to effectively reduce cyber-risk. From detection to resolution, the platform automates and orchestrates the vulnerability remediation lifecycle at scale.

THE PROCESS

Detect

The first step of the vulnerability remediation process is accurately finding all vulnerabilities residing within the network. By ingesting findings from various vulnerability assessments in your corporate environment or production, from infrastructure, through code project to pen-test results, the platform is able to unify all vulnerability data within a single point of view.



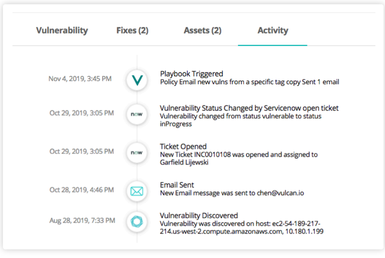
Prioritize

Moreover, by enriching these scan results with data derived from asset inventories and various threat intelligence sources, the platform is able to perform contextual risk-based prioritization of all vulnerabilities and misconfigurations detected. Thus, Vulcan enables security teams to focus on the most business-critical vulnerabilities within the network.

Enrich

By integrating with ticketing systems, the platform is able to enrich each ticket created, populating it with all the information required to drive remediation. Through Vulcan's Remediation Intelligence database, containing millions of remediation actions (be it patches, configuration changes or compensating controls), each ticket is updated with the most effective solution to the vulnerability. Thus, the platform facilitates the process, creating predictability for the solutions deployed. It reduces the likelihood of downtime and so improves cross-team collaboration.

Collaborate



Vulnerability remediation has become very complex. It requires continuous collaboration between different teams, and many enterprises lack the ability to effectively track and report progress. As a result, having a clear method to create, track and follow up on tasks can be the difference between meeting SLAs and requirements or staying vulnerable and susceptible to breaches.
Leveraging the collaboration tools that are in place today, Vulcan creates visibility throughout the entire remediation process. The platform integrates with all instances used by the organization and sheds light on the progress made.

Automate

Vulcan's automation framework enables teams to scale the remediation of vulnerabilities and misconfigurations and effectively reduce their cyber risk. By adopting the manual processes and policies that are in place today, the platform can generate customizable workflows. These, in turn, will automatically generate and assign tickets to the appropriate teams. As so, the platform puts an end to the inefficient, manual remediation processes, automating the orchestration of key remediation steps.