Vulcan FAQ ■ June 2019

Vulcan Cyber Vulnerability Remediation Platform Frequently Asked Questions

At Vulcan Cyber, we're modernizing the way enterprises reduce their cyber risk. From detection to resolution, we automate and orchestrate your vulnerability response process dynamically and in scale.

VULCAN

Frequently Asked Questions

Vulcan Cyber is a Vulnerability Response Automation Platform which enables security teams to take back control and turn vulnerabilities, misconfigurations and other cyber hygiene issues into actionable insights. With us, you and your team can focus on the most business critical vulnerabilities, according to the risk they pose to your unique environment. Our platform automates the process of vulnerability remediation, providing you with the best solution - the solution that would least be disruptive to production, in the form of a patch, a configuration change or workaround.

How does Vulcan automate vulnerability response?

Our approach strives to end the mundane, inefficient, manual vulnerability response processes; to prevent downtime and inevitable human errors, by relying on our proprietary remediation intelligence. From patching your linux server using configuration management tools like Ansible or Chef, through preventing exploitations by using your firewall, WAF or endpoint security product, our database of solutions for vulnerabilities empowers security teams with the most efficient solution for every vulnerability. A solution that can be deployed automatically.

With our automation framework, security teams can pre-define playbooks that will drive action when a desired criteria is met. This process can be either fully or semi-automated, depending on the change management process. By creating unique playbooks, tailored to your environment and needs, our platform will scale your response processes.

How does Vulcan prioritize?

While traditional TVM vendors tend to rely on objective metrics, like raw CVSS scores and prioritize vulnerabilities accordingly, it’s crucial to understand that vulnerabilities are forever subjective - exploiting the same exact vulnerability will have a different impact on different environments, and as such, should be treated differently. Having this in mind, security teams ought to prioritize vulnerabilities according to the specific risk they pose to their environment. Our prioritization mechanism focuses on four key metrics:

Security data

We integrate with the existing security tools used today in order to extract security data, creating a clear picture of all vulnerabilities in the system. From tools like Qualys, Rapid7, SourceClear and WhiteSource to name a few, we connect via APIs to give you a full view of the coverage of your environment.

Business data

Different assets play different functions in every system, and therefore cannot be treated alike. When prioritizing vulnerabilities, business needs must play an integral role. By connecting to CMDBs and incorporating our asset criticality feature, the business importance of the assets is taken into consideration by our prioritization algorithms.

Asset data

Through integrations across inventories, deployment tools and asset management tools, we're able to create a clear view of your network, gaining a better understanding of the asset configurations, security posture and status

Threat Intelligence

Vulnerabilities don't exist in a vacuum. By connecting to over 50 threat intelligence feeds, we are able to associate whether known IOCs are being used to compromise specific vulnerabilities.

How do we Deploy

Our platform is a SaaS based solution that ties into your existing infrastructure through bidirectional APIs. From there, the platform provides a single pane of glass for you to review, understand, prioritize, and take action on your data.

Who is Vulcan right for?

Companies of every size! If you feel like you're constantly putting out fires instead of driving your vulnerability remediation process yourself, you've come to the right place. Our platform is the answer to any company feeling the pain of vulnerability management.
We're in lots of different sectors: Tech, Finance, HealthCare, Retail, EDU, Government, Manufacturing, and many more.