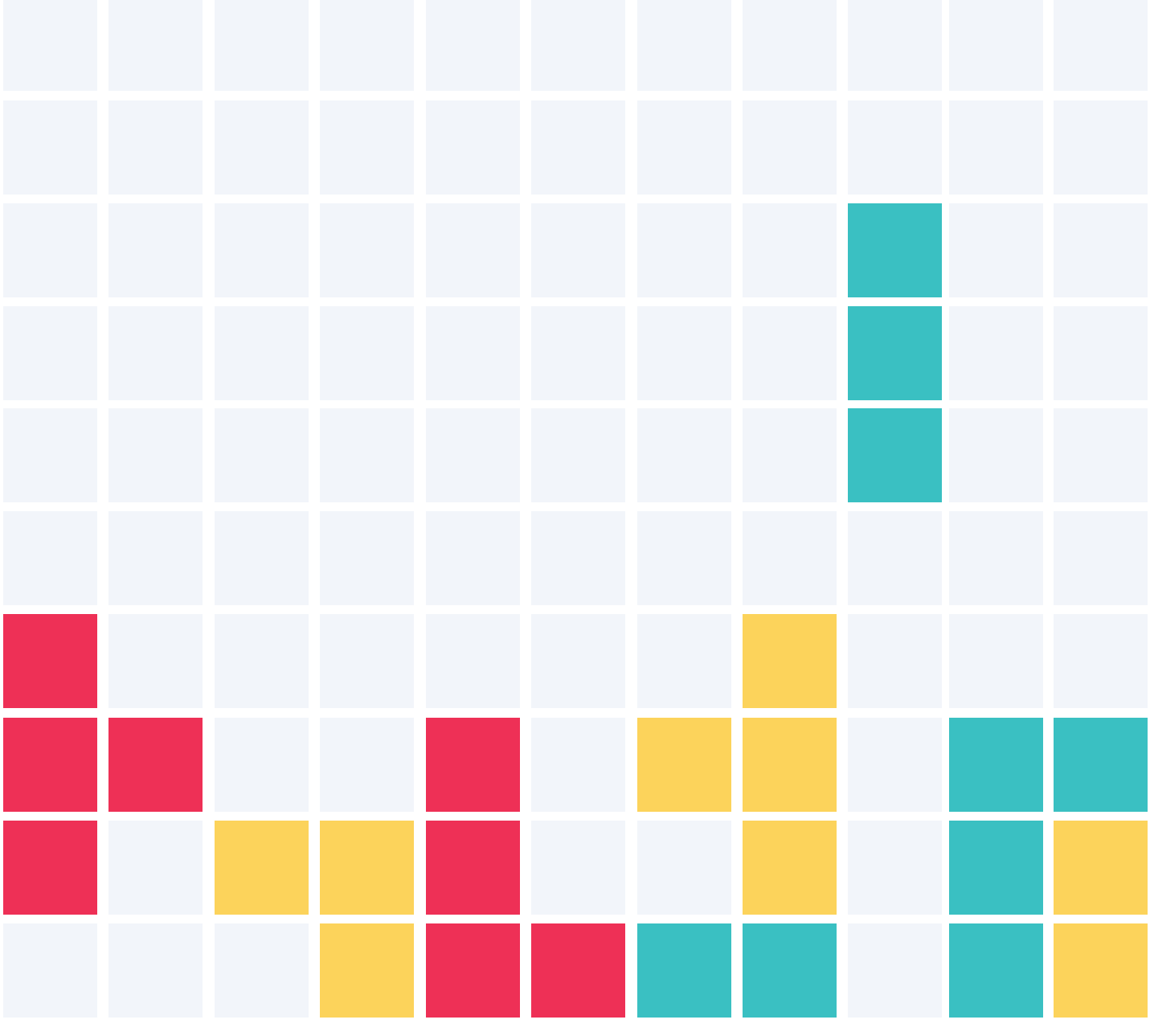
VULCAN

Going Beyond Prioritization - Remediating Vulnerabilities at Scale

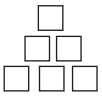
Nowadays, enterprises are unable to scale their vulnerability remediation processes effectively. The modern hybrid environment is ever-changing, and when combined with the growing risk of known vulnerabilities, traditional processes are becoming an immense challenge.

At Vulcan, we're modernizing the way enterprises reduce their cyber risk.



Key Benefits

From detection to resolution, we automate and orchestrate the vulnerability remediation process dynamically and at scale. Vulcan's platform enables security teams, for the first time, to drive forward the remediation of vulnerabilities and misconfigurations, rather than adhere to prioritization.



Prioritize High-Risk Vulnerabilities

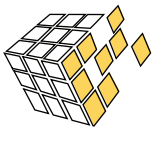
Prioritize the vulnerabilities in your network according to the specific risk they pose to your environment, minimizing workload and costs.

Improve Efficiency

Scale up your remediation process through pre-defined workflows and automate the remediation process, minimizing vulnerability dwell time.

Report Remediation Progress Intuitively

Measure the efficiency of remediation measures taken internally and deliver straightforward reports to executives.

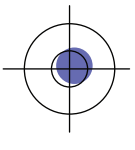


Leverage Existing Investments

Intergate with your existing Security, IT and DevOps tools to enhance your remediation capabilities and draw greater value than ever before.

Align Security, IT and DevOps with Business Objectives

Establish cross-enterprise alignment and empower stake-holders to make informed decisions, through transparency to the enterprise's risk posture.



Make Unscanned Assets a Thing of the Past

Unscanned assets are blind-spots in our environment, inevitably leaving us exposed. Gain the visibility you need to manage your remediation process.

Contextual Risk-Based Prioritization

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 should prioritize vulnerabilities according to the specific risk they pose to their environment.

Our prioritization mechanism focuses on four key metrics:

Security Risk

Our Platform integrates with the existing security tools used via APIs. By extracting the security data, Vulcan is able to create a full view of the coverage of the environment.

Business Impact

When prioritizing vulnerabilities, the business functions of assets must play an integral role. By connecting to CMDBs and incorporating our asset criticality feature, our prioritization mechanism incorporates the business value of each asset.

External Threats

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

Asset Posture

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

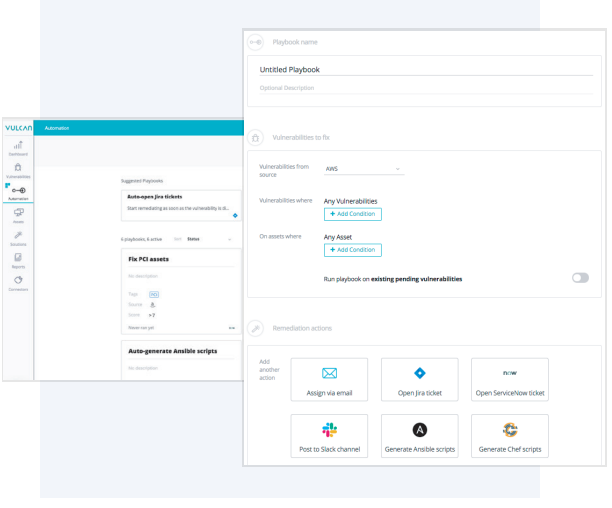
Asset Management

Through its wide set of integrations, Vulcan Cyber creates a clear view of the security posture of the assets in the environment, putting the extracted data into context. Vulcan is able to both prioritize and drive remediation steps through its integrations, promoting a holistic approach to vulnerability remediation. As such Vulcan Cyber leverages the current investments made by the enterprise to bring about effective remediation processes.

Automating and Orchestrating Vulnerability Remediation

At Vulcan, we promote a remediation-focused approach.
Contextual prioritization is a crucial first step, but it won't suffice. In order to truly improve the security posture of the enterprise, security teams need to remediate the vulnerabilities in their digital environment. This is why, the Vulcan platform is remediation driven, orchestrating and automating the remediation process at scale.

Vulcan's automation framework enables security teams to use remediation playbooks, tailored specifically to each environment. These playbooks drive remediation steps when desired criterion is met, enabling security teams to scale their remediation processes. From detection to resolution, the Vulcan platform automates and orchestrates the cyber hygiene lifecycle across infrastructure, applications, and codebase. As such, Vulcan puts an end the inefficient, manual vulnerability response processes, preventing downtime and inevitable human errors.



Remediation Intelligence

The diversity and flexibility of infrastructures and applications have created a wider threat landscape than ever before. Combined with enterprise software being more interconnected than ever, patching one component in production may have devastating implications on the business. Through Vulcan's Remediation Intelligence, the world's largest database of solutions for vulnerabilities, security teams are empowered with the most efficient solution for every vulnerability, a solution that can be deployed automatically.

From patching your Linux server using configuration management tools, through preventing exploitations by using your firewall, WAF or endpoint security product, the most appropriate solution may vary vastly between enterprises. Through Vulcan's Remediation Intelligence, the platform cherry-picks the single most effective solution that would be least disruptive to production and drives it forward automatically.