SOLUTION BRIEF

Remediation that fixes and eliminates vulnerabilities

Overview

At Vulcan, we envision a world in which vulnerabilities are fixed and eliminated rather than simply managed. We want our customers to be safe in the face of attacks because they were able to proactively preempt attacks before they ever had a chance.

To make this vision a reality, our vulnerability remediation orchestration and security analytics platform has been built from the ground up to deliver a very simple but powerful value proposition:

Get fix done.

Vulcan remediation orchestration and analytics is based on three pillars:

- Prioritize. Using advanced security analytics, Vulcan prioritizes vulnerabilities based on the severity of risk in your unique environment, as well as your ability to fix them.
- Remedy. Vulcan curated remediation intelligence matches the right remedies to prioritized vulnerabilities, giving IT security teams ready-to-use solutions rather than to-do lists.
- Automate. Remediation playbooks and orchestration campaigns automate the entire fixing process, including remediation and mitigation actions, verification, and reporting all of which make it easier to monitor the remediation lifecycle.

  This solution brief focuses on Vulcan remediation playbooks and other workflow automation capabilities that are at the core of the “automate” value delivered through the Vulcan remediation orchestration platform.

Become a fixing machine

CHALLENGE

Let's be honest: The remediation workflow is pure chaos, draining a lot of time and energy. Complex, multi-phase, and tedious remediation tasks are carried out across numerous teams, each with its own mindset, priorities, and tools.

SOLUTION

Vulcan integrates with your existing ITSM, configuration management, and patch deployment tools to turn complex fixing processes into step-by-step workflows, automating as many of the steps as possible, from ticket routing to the patching itself.

Vulnerability remediation automation is no longer a nice-to-have but a must-have. One of the key factors identified as causing patching delays is reliance on manual techniques. When risk tolerances and vulnerability remediation workflows are clear, it is possible to turn many manual tasks into rules-based workloads, such as: opening service tickets and assigning them to the right team, tracking the progress of the assessment/remediation process, and managing the patch testing/staging/rollout pipeline.

The next step is to pull these rules-based workloads into a playbook in order to dramatically streamline and, where possible, automate the remediation process. Reporting policies and SLAs can also be easily translated into rules for automatically generating and distributing reports in the required format.

Whether a patch, configuration change, workaround, or compensating control, the recommended Vulcan solution can be deployed automatically and with a high level of predictability-reducing the likelihood of downtime and improving collaboration among all stakeholders.

BENEFIT

Don't just find vulnerabilities, eliminate them. Fix at scale while scaling down backlog. Streamline.Fix.Repeat.

Integrations

	ITSM FRAMEWORKS	CONFIGURATION FRAMEWORKS		PATCH DEPLOYMENT FRAMEWORKS
Current Integrations	**Jira, ServiceNow**	**CrowdStrike**	**Ansible, Chef, Puppet**	**Ivanti, SCCM**
Overview	Combines ITSM ticketing and cross-team collaboration with Vulcan remediation and tracking for a clear, coherent view of remediation progress	Creates auto-generated customizable mitigating actions orchestrated across relevant asset groups	Creates auto- generated reme- diation scripts to orchestrate configuration changes and fixes at scale for relevant asset groups	Leverages patch deployment and management platforms to orchestrate remediation on relevant asset groups
Features	▪ Creates tickets in Vulcan, including automated creation via pre-defined playbooks ▪ Assigns actionable tickets (w/vulnerability data, solutions, SLAs, etc.) to relevant people ▪ Constant visibility into ticket status, SLAs ▪ 2-way integration: actions updated in Vulcan and the ITSM framework	▪ Automatically ingests asset data into Vulcan ▪ Detects vulns on assets ▪ Provides customizable fixes to apply via CrowdStrike	▪ Automatically ingests asset data into Vulcan ▪ Prioritizes remediation actions by applying context & business logic to vulnerabilities detected in the assets ▪ Drives forward remediation via predefined workflows, with maximal automation ▪ Full visibility into infrastructure & apps, risk posture	
Benefits	▪ Create & track all tickets in Vulcan ▪ Auto-assign tasks to team members ▪ Centralize vulnerability remediation communications ▪ Track head-to-head remediation performance	▪ The user can select a suggested remedy, or customize a remedy as desired ▪ Single-pane remediation management of all assets, environments, accounts, and regions ▪ Centralized visibility of remediation processes, workflows, playbooks	▪ Customizable scripts ▪ Auto-generate & deploy targeted solutions on critical infrastructure	▪ Auto-generate & deploy targeted solutions on critical infrastructure

Use cases
IT service management and ticketing

These use cases are relevant for the current ITSM integrations: Jira and ServiceNow.

Tracking remediation progress including change management and DevSecOps processes

CHALLENGE

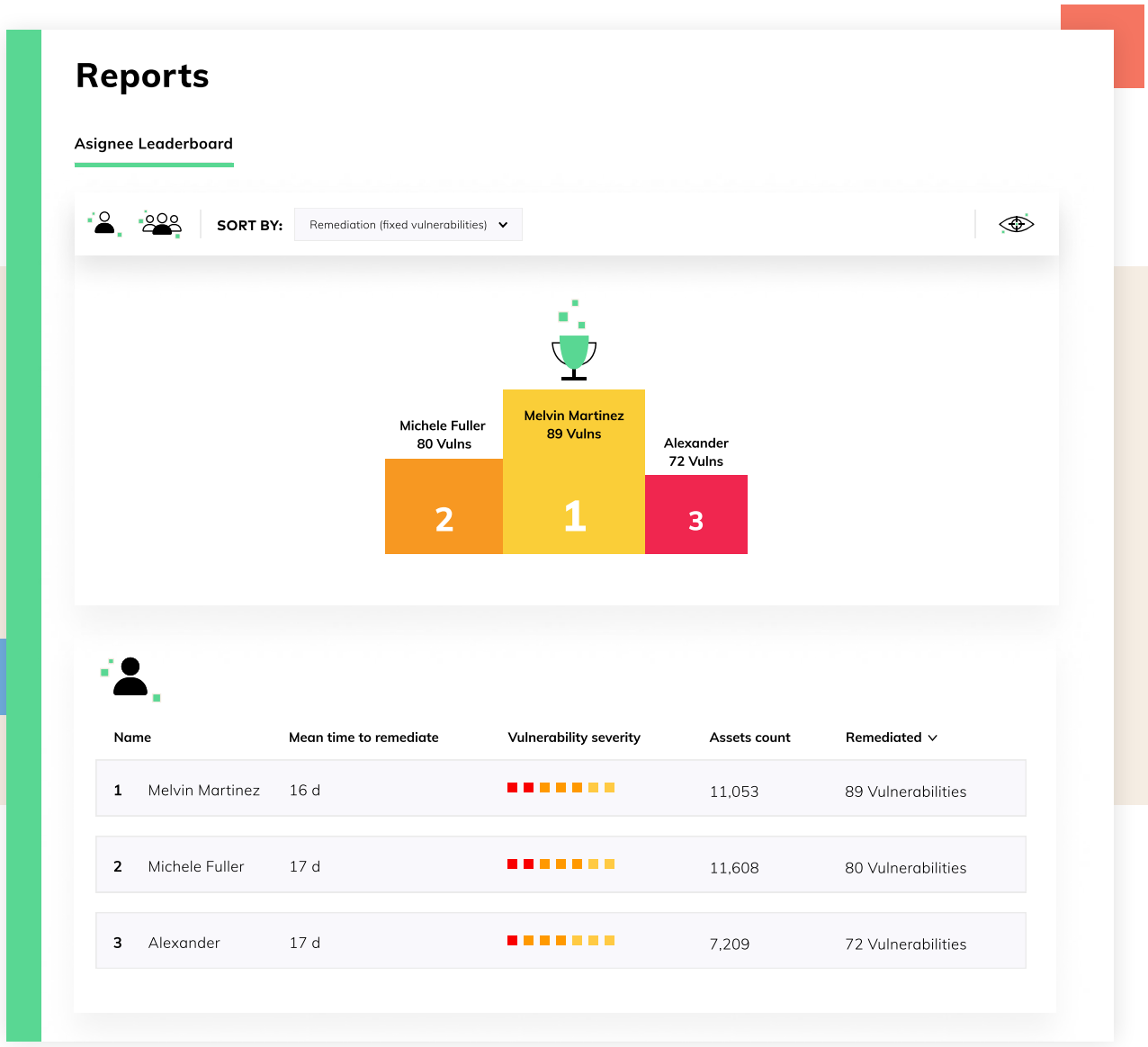
With so many teams involved in vulnerability remediation, it is difficult to effectively track and report progress. Having a clear method to create, track, and follow up on tasks—including change management and DevSecOps processes—is key to meeting business-critical SLAs and security posture requirements.

BENEFIT

Improve the remediation process by tracking and measuring the performance of teams and key personnel through intuitive reporting. Centralize all communications around vulnerability management tickets and gain instant visibility into ticket statuses and open tasks.

SOLUTION

Through integration with your Jira or ServiceNow framework, Vulcan logs every action taken and provides a centralized source of truth regarding remediation progress. Vulcan externalizes this progress for all teams, creating clear, end-to-end visibility.



Automated ticket creation and ticket close

CHALLENGE

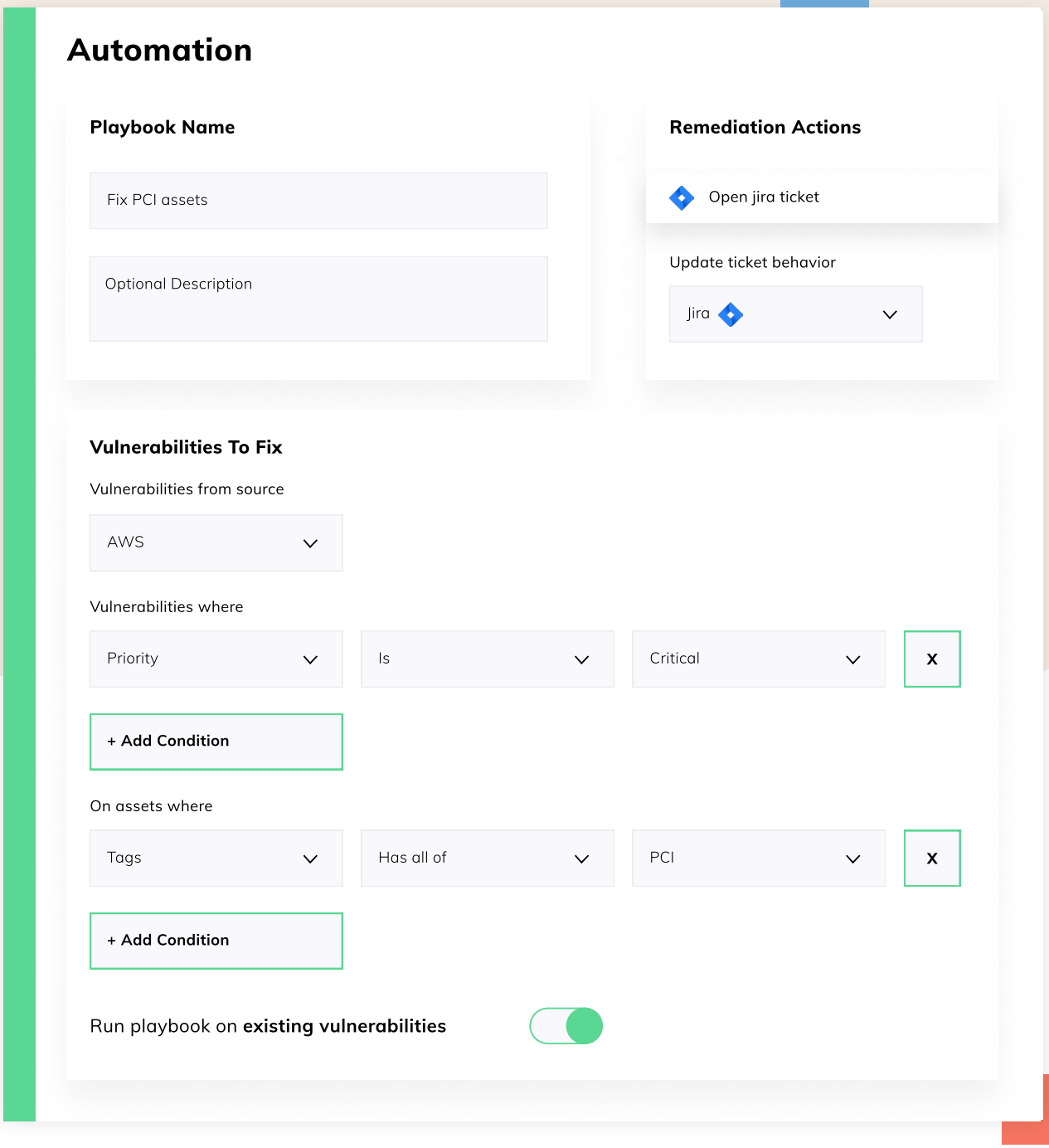
It is very time-consuming and unscalable to manually open and assign remediation tickets for each detected vulnerability—and then close those tickets when done.

SOLUTION

Through bi-directional API integration with Jira or ServiceNow, Vulcan playbooks can automatically open and assign vulnerability remediation tickets, as well as orchestrate all remediation steps including closing a ticket after the required action has been validated and verified. At all times, teams have access to intuitive ticket status and Scale up and streamline the vulnerability.

BENEFIT

Remediation process with automated ticket creation, tracking, and closure. Provide all stakeholders with a centralized view of ticket status.



Automated ingestion and patch deployment

These use cases are relevant for the current patch deployment framework integrations: Ivanti and SCCM.

Automated vulnerability ingestion and prioritization

CHALLENGE

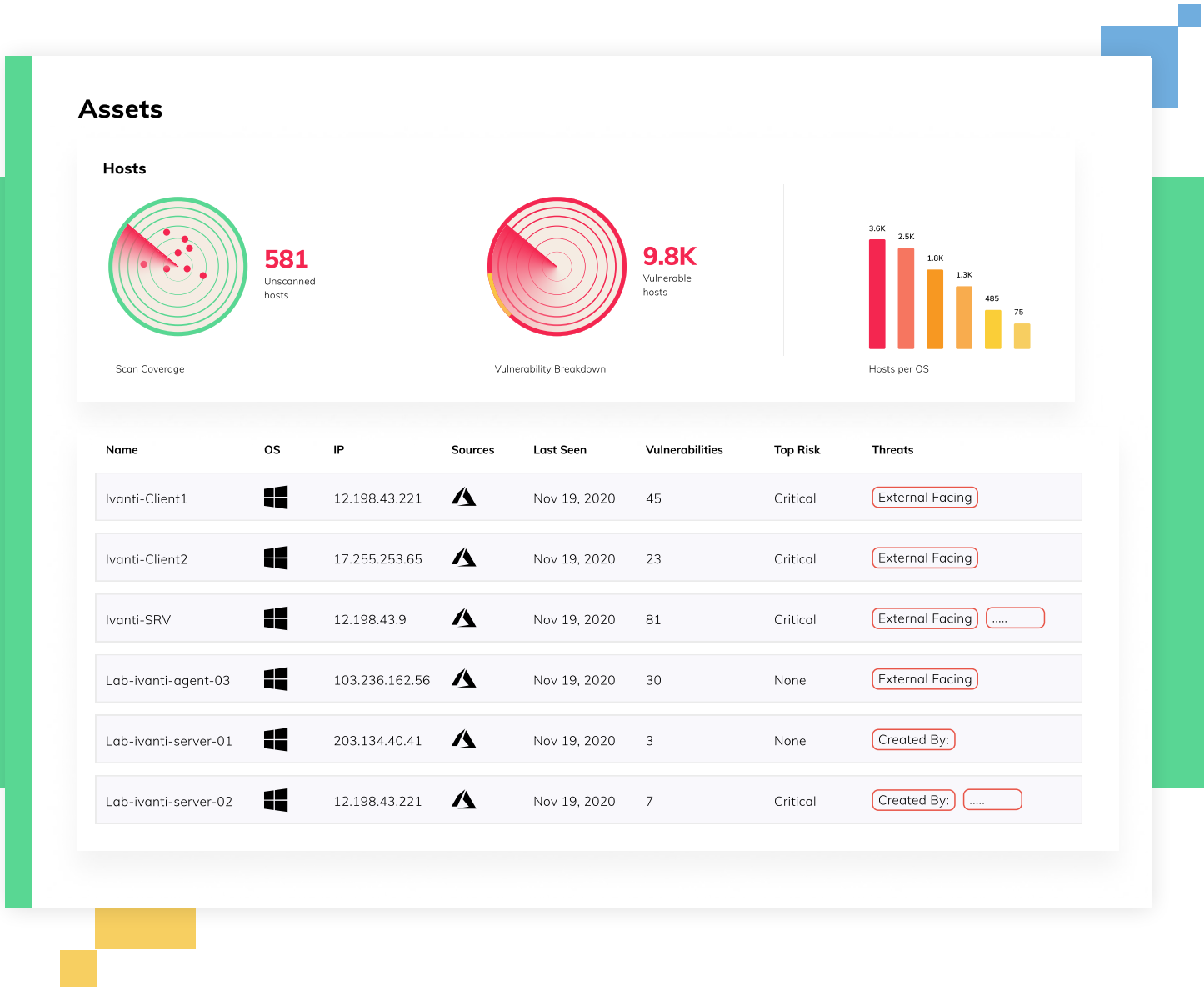
Running effective vulnerability remediation programs at scale is very difficult if remediation tasks are not prioritized according to the risk that detected vulnerabilities pose to the organization's specific environment.

SOLUTION

Vulcan automatically and continuously ingests asset data from the organization's Ivanti or SCCM asset discovery and patch deployment framework. Vulcan then prioritizes remediation tasks by identifying which of the vulnerabilities detected for these assets pose the highest risk in light of data enrichment, such as context, business logic, and threat intelligence.

BENEFIT

By highlighting the organization's biggest risks, this integration allows teams to focus their remediation efforts on the vulnerabilities that matter most.



Automated remediation

Vulcan doesn't stop automating the work of remediation until fix is done. Even when the vulnerabilities are discovered, prioritized, remedies identified and routed to the correct teams, there is still a ton of work to be done. In fact, executing the fix is often the most tedious and difficult step in the process. Automation at this point is critical.

Fortunately Vulcan integrates with the automation tools that IT and network operations teams, patch managers and DevOps pros trust and use every day. Vulcan plugs the patches, configuration scripts, mitigating actions, compensating controls and workarounds directly into the respective tools as appropriate. This is an example of Vulcan remediation orchestration using automated patch management:

CHALLENGE

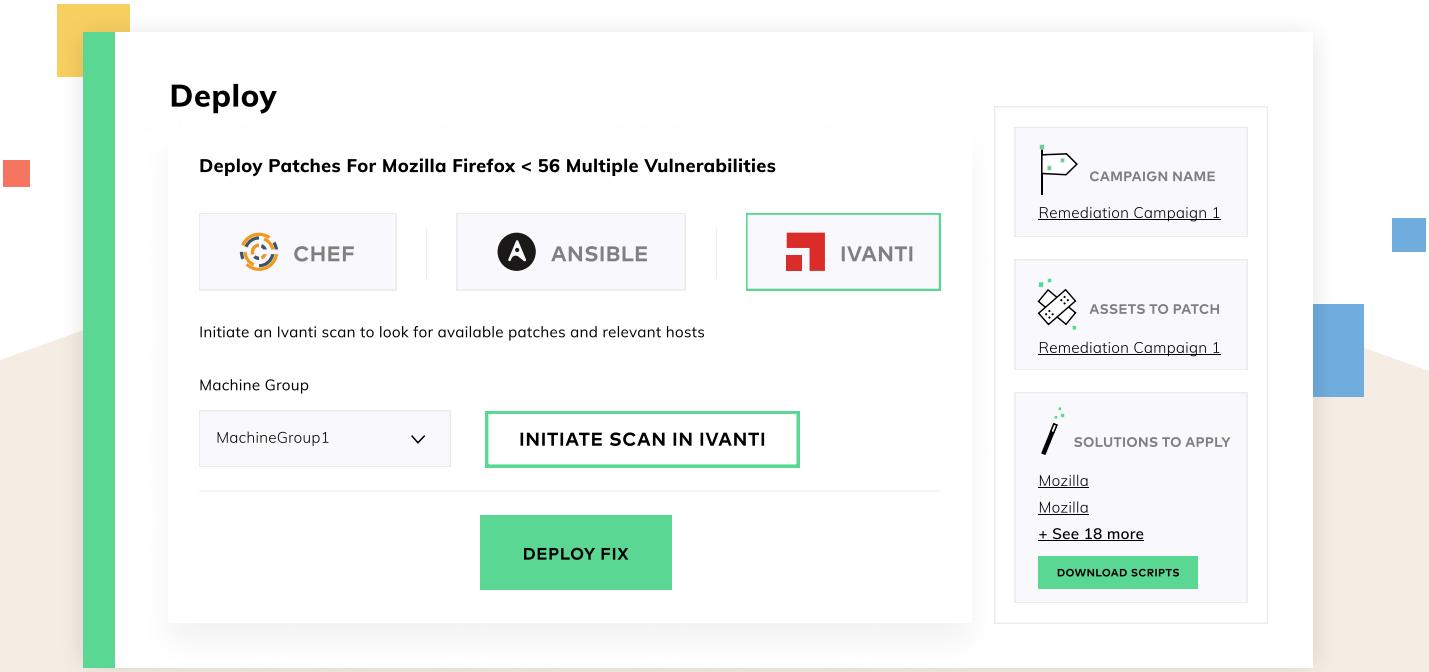
Deploying the correct patch on the right asset is the last mile in a successful remediation process. However, it is incredibly challenging to verify effective execution given the complexity of enterprise-level vulnerability remediation.

SOLUTION

Ensure smooth cross-organizational deployments—including validation and verification with a stack that combines Vulcan's remediation orchestration automated workflows and risk-based prioritization methodology with an organization's Ivanti or SCCM patch deployment engine.

BENEFIT

Vulcan hands teams the exact priorities, remedies, and automation they need to get fix done—as quickly and easily as possible.



About Vulcan

The powerful Vulcan remediation orchestration and security analytics platform hands teams the exact priorities, remedies, and automation they need to get fix done. Unlike typical vulnerability management tools that simply give you an endless to-fix list, Vulcan prioritizes based on both severity and fixability, hands you the ideal remedy for the job, then orchestrates and automates the entire fixing process. That's why industry leaders like Snowflake, Clarivate, Informatica, and Blue Cross Blue Shield already use Vulcan to fix more vulnerabilities while spending 85% less time doing so.

Get fix done.

Starting today by using Vulcan Remedy Cloud or by requesting access to Vulcan Free. If you'd like more information before diving in we'd be happy to provide a custom demo for your team.

VULCAN.

Contact us at hello@vulcan.io
See more at www.vulcan.io