WHITEPAPER

The difference between legacy and modern vulnerability management

VULCAN™

Introduction

Vulnerability remediation is the process of finding the security weak spots in your digital infrastructure, then finding and applying remedies to these potential threats. Although it sounds straightforward, in practice, vulnerability remediation is perhaps best described by Yaron Levi, CISO, Blue Cross and Blue Shield of Kansas City as "[security] trying to manage a mountain of work they usually have little to no control over by pushing other overtaxed teams, such as IT and engineering, to remediate during non-ideal times."

This white paper explores the ever-growing challenges to effective vulnerability remediation. It then pinpoints the true vulnerability management end-game of detecting the vulnerability and applying the right fix as quickly as possible, plus easily verifying that you're done with that vulnerability. In short, it is time to "get fix done." This paper also provides some vulnerability remediation best practices and traps to avoid, with a special emphasis on the importance of automation. In the end, it describes how the Vulcan Cyber® platform goes beyond traditional vulnerability remediation to deliver vulnerability remediation orchestration by helping security and IT operations teams prioritize, remedy, automate, and analyze.

Modern vulnerability management: More challenging than ever

Threats to network security have been exacerbated by the technological changes and advanceswe've seen over the past few years. In the 1990s and early 2000s, there were relatively few vulnerabilities and each company team took care of its own. But with the birth of the cloud and changes in enterprise infrastructure, networks have become more exposed to external threats.

With companies having embraced public cloud infrastructures, open-source software, and third-party SaaS solutions, their exposure has grown while real-time visibility into potential vulnerabilities has shrunk. Complex multi-cloud, hybrid architectures, as well as highly diverse stacks comprising multiple vendors andsolutions, make it especially challenging to keep networks secure.

The switch to agile development and rapid code releases has further increased this risk with more and more public-facing software being deployed without being adequately tested. In addition, the substantial adoption of 24/7 SaaS products makes it harder for sites to shut down to perform maintenance or remediate vulnerabilities. This combination of agile development and the demand for continuous availability has resulted in companies' core, mission-critical software being continuously vulnerable.

In turn, these factors have caused a veritable flood of vulnerabilities, with companies having too little time and resources to solve them all. The result: Flexible, intelligent, powerful, and cost-effective vulnerability remediation is more important than ever.

Vulnerability Management Vs. Vulnerability Remediation

Vulnerability remediaiton, also known as the modern VM, is the part of vulnerability management where the rubber meets the road and threats are mitigated.

Vulnerability management focuses on:

- **Knowledge:** Staying knowledgeable about and up-to-date on new security threats through information automatically collected from security product vendors, system updates, and threat intelligence reports.

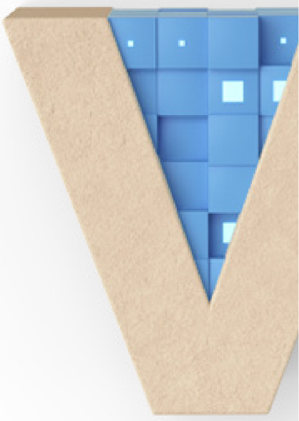
- Discovery/Visibility: Having visibility into how your systems' components interact, how many instances you have of key software, where the access points to your network are, who "owns" what, etc.

- **Configuration**: Setting clear rules and practices for configuring software across multiple instances in different physical installations.

- **Assessment:** Scheduling frequent periodic and surprise-assessment scanning sessions to identify new vulnerabilities.

- **Prioritization:** Prioritizing vulnerabilities based on your specific network to determine which vulnerabilities actually pose the greatest risk to your network.

Effective **vulnerability remediation** focuses on "get fix done" in order to preempt threats before they can cause harm. Good vulnerability remediation involves multiple teams—including management, developers, IT, and security management—working across departments to both harden security and find the most efficient way to fix the vulnerabilities in the system. Whenever possible, automation is used, not only to save time and money by working at scale, but also to ensure consistency.



Getting started with Vulnerability Remediation

While every company is unique, we recommend your vulnerability remediation plan contain the following elements:

- **Increase company awareness of vulnerabilities:** Communicate with your partners in the C-suite, as well as IT, security, and DevOps managers, about the importance of vulnerability remediation and the ways they can participate and make the most of the shared effort.

- **Guard your CI/CD pipeline:** New technologies necessitate new remediation strategies. Today, more vulnerabilities are being pushed to production and measures need to be taken to protect the CI/CD pipeline. There are a number of excellent free scanning programs and other open-source tools that can help you reduce or remediate vulnerabilities to safeguard your pipeline.

- **Have a complete inventory of your network's assets:** You cannot accurately assess the threat posed by vulnerabilities in your network without complete visibility of your network, i.e., what assets are connected to it and how they interact.

- **Know which vulnerabilities are out there and prioritize according to risk:** It's easy enough to find a list of vulnerabilities with "objective" ratings of their severity, such as the CVSS, but your security team needs to prioritize vulnerabilities by their potential impact on your specific environment. Vulnerability ratings are inherently subjective, since exploiting the same vulnerability impacts each environment differently. Therefore, the same vulnerability should be treated differently in each network.

- **Think twice before you patch**: There's no doubt that applying a patch is often the best way to remediate a vulnerability. But patches can be risky and often break production, especially if the software involved interacts with other software. Sometimes, a mere change in configuration could be enough to safeguard your network. That's why Vulcan Cyber developed its proprietary remediation intelligence database—and Remedy Cloud as the free, community version of the database—to inform security teams of the most efficient solution to any security threat. This solution, which could be a patch, configuration change, or workaround, would be the least disruptive to production. The solution can be deployed automatically using your preferred deployment or security tool.

- **Re-scan:** Finally, make sure the problem is truly gone, by scanning and validating that the threat has been removed from the system.

Many of these steps can be completed more efficiently if your company's vulnerability remediation solution includes a vulnerability remediation intelligence database and vulnerability threat intelligence. These tools ensure you have the latest information from vendors, forums, and other sources on vulnerability remediation alternatives, including the advantages and disadvantages of each.

The benefits of automation

As you implement your vulnerability remediation program, you should aim to automate the work as much as possible. In general, automation saves time and improves the consistency and quality of remediation. For many companies, automation is the only practical way to implement remediation due to the size and complexity of the networks and components involved.

Here are some examples of how automation improves your vulnerability remediation efforts:

- **Reduces manual errors:** This lets your team avoid errors associated with manually performing repetitive, mundane tasks and instead focus their energy on areas where they can add more value.

- **Reduces vulnerabilities in your CI/CD pipeline:** Automatic scanning keeps an ever-vigilant eye on your pipeline, reducing the risk of you deploying compromised code.

- **Curated remediation intelligence as a service that saves time and effort:** Instead of having your team search for different solutions themselves, have the information retrieved automatically from vendors, forums, and other sources of information. Better still, incorporate a vulnerability remediation database that retains and analyzes this information, for a smart remediation process.

- **Vulnerability prioritization focused on the right threats:** Automating your evaluation of the threats to your network, or selecting a solution that does this for you, will keep your team focused on the most important vulnerabilities, thus remediating threats in the optimal order.

- **Solutions are applied consistently:** In networks that have multiple instances of the same component, automation guarantees that the same remediation method is applied to each one.

- **Solutions are applied continuously:** Some solutions may need to be applied continuously, not just once. Automation makes it possible to remediate using automated scripts and playbooks.

- **Solutions are applied in the correct order:** There are cases where multiple solutions need to be applied to one component or a group of components. An automated script performs the steps in the correct order, which is particularly important if there are multiple instances of components.

- **Enterprise-grade scalability:** Automation makes remediation at scale extremely efficient, cutting costs and resource demands.

Vulnerability Remediation traps and how to avoid them

With many different vulnerability remediation approaches out there, it's important to avoid wasting time and money on the common traps described below.

TRYING TO PATCH EVERYTHING

It's understandable that you want to remediate every vulnerability. But with tens of thousands of vulnerabilities being discovered each year, that's simply impossible. Moreover, patching has its own risks, so it is important to reserve patching for cases where it is truly the most efficient course of action. Sometimes, a change in configuration settings is sufficient. Other so-called "threats" may actually pose no risk to your environment. In such cases, you may be better off not taking any action for the time being and focusing on more critical problems.

FOCUSING ON THE WRONG THREATS

But how do you identify the most important threats? True, there's the Common Vulnerability Scoring System (CVSS), which ranks vulnerabilities' severity. But before focusing only on threats scored as "critical," be aware that many vulnerabilities with a lower rating have active exploits, while some "critical" ones are too difficult or simply not accessible for threat-actors to use effectively. In other words, if you focus only on critical problems as ranked by objective metrics like CVSS, you may end up ignoring threats that pose the greatest risk to your company while wasting your efforts on ones that don't.

BELIEVING THE HYPE

With security such a popular topic, the media is also looking out for critical problems that could turn into disasters. Unfortunately, the press can exaggerate the importance of vulnerabilities, just like the experts may. Consider the Spectre and Meltdown threats. Both were much promoted at the time yet ended up being much ado about nothing. Anyone swept along with the hype ended up wasting time and money without making their systems any more secure. A mature vulnerability remediation program is essential to maintain focus on the vulnerabilities that matter to your business.

The Vulcan Cyber approach

The Vulcan Cyber risk management platform provides vulnerability remediation that allows security teams to safeguard digital environments against threats and misconfigurations. This effectively achieves the vulnerability management end-game of get fix done.

The Vulcan Cyber platform:

- **Prioritizes,** pinpointing business-critical threats according to the unique risk they pose to the environment.
- **Remedies,** offering a range of options, from configuration changes to patches based on your network's specific characteristics.
- **Automates,** scaling up the remediation process through workflow automation and orchestration across multiple teams.
- **Analyzes,** providing a clear view into end-to-end remediation campaigns to ensure work is optimized, service level agreements are met, risk is actually reduced, and compliance is achieved.

The platform prioritizes security threats based on the subjective risk they pose to the environment, enabling security teams to focus on the most critical vulnerabilities to their organization. This is done by incorporating security data extracted from threat intelligence gathered from dozens of feeds:

- Security tools
- Business data derived from CMDBs
- Network architecture and asset configuration data obtained from infrastructure integrations (vSphere, AWS, GCP, etc.)
- Patch, configuration and deployment tools (Chef, Puppet, MS Intune, etc.)
- Service management tools (ServiceNow, Jira, Azure Boards)

This way, security teams can rest assured that they're dealing with the right threat at the right time.

The Vulcan Cyber proprietary remediation intelligence database, also now available as a community resource known as Remedy Cloud, provides curated solutions and fixes from vendors, forums, and other sources on remediation alternatives. This way, security teams can assess the most efficient solution to any security threat, one that is the least disruptive to production.

The platform is designed to orchestrate vulnerability remediation, promoting both off-the-shelf and customizable playbooks to ensure threats are removed in the most consistent, safe, and efficient way possible. Vulcan Cyber helps the vulnerability management discipline fulfill its promise with an orchestration framework that allows security and IT teams to remediate at scale.

To see the Vulcan Cyber Remediation Orchestration Platform in action, schedule a demo with a member of the Vulcan Cyber team today.