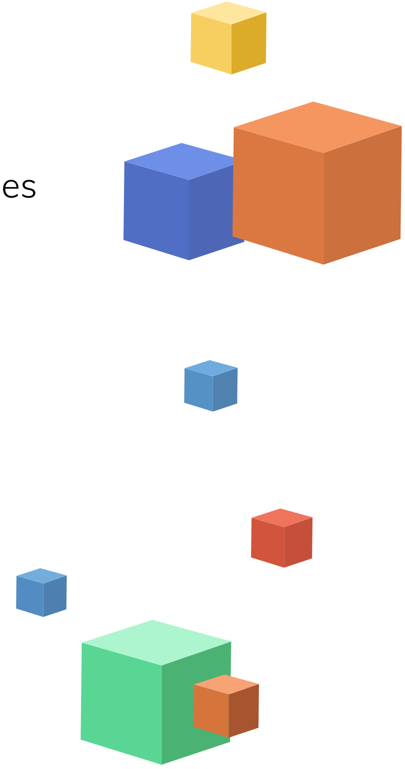
WHITEPAPER

The top five mistakes everybody makes in vulnerability management

VULCAN™

Common mistakes in vulnerability management

Table of contents



The stakes in vulnerability management continue to rise. The average cost of a data breach in the United States in 2020 rose to [$8.64 million](), up 5% over 2019. And we are also starting to see [stiff fines from regulators]() for lapses in securing personal data. With new vulnerabilities being added every week and older ones still being exploited, it's no wonder that CISOs and other security leaders are striving to harden their vulnerability remediation programs.

In this white paper, we describe the top five mistakes that commonly stymie effective vulnerability remediation:

- Focusing only on the latest headlines
- Not automating remediation
- Divided teams
- Too many network blind spots
- Misaligned priorities

#1 - Chasing the headlines

Spectacular breaches or dramatic exploits tend to get a lot of media attention. Management is going to want to know if your company is prepared for whatever is making headlines, whether it is a zero-day vulnerability, a new phishing method, or any of the other vulnerabilities that are in the news. But that doesn't mean your security team should be planning their steps based on what the media is reporting. In fact, basing your efforts solely on what's in the news can blind you to less publicized exploits that are actually hurting your company right now.

That's what happened to Equifax. Its breach was not due to a zero-day attack, but rather an exploit that had been seen "in the wild" and for which a solution had been posted. And this is not an unusual situation. In the 2020 Ponemon/IBM report on the state of vulnerability management, 42% of the respondents stated that their company's data breaches occurred because an available patch for a known vulnerability was not applied.

The crux of the matter is that your vulnerability remediation efforts must always be focused first on the vulnerabilities that pose a clear and immediate threat to your network.

You need to be aware of and evaluate the high-profile threats, but you must also be able to explain to stakeholders and your peers which threats really matter, and which ones don't.

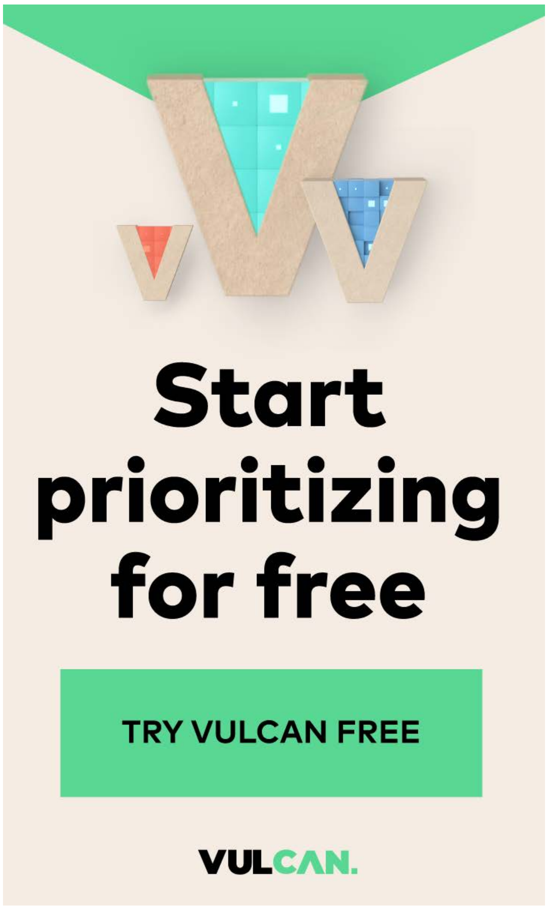
Your ability to distinguish between relevant and irrelevant threats and to communicate this clearly will help you get the buy-in you need for setting the right priorities and creating an effective vulnerability remediation strategy.

#2 - Fear of automation

In the era of self-contained networks and data centers, it was possible even for large companies to manually manage their vulnerability remediation efforts. The situation, however, has shifted radically over the past decade. Changes in the modern enterprise environment, the wide range of software and tools in networks today, and shift in software development cycles have led to a skyrocketing number of vulnerabilities. Over 30,000 new vulnerabilities have been discovered in the past two years alone. That's simply too many for any team to handle manually.

Automation is the key to businesses being able to remediate vulnerabilities as quickly, consistently, and accurately as possible, at scale. Through automation, security teams can ensure that the same remediation solution is driven consistently—and in real time—to all instances throughout a network. Automated scripts also ensure that complex multi-step remediation solutions are correctly implemented.

In general, automation puts an end to manual vulnerability response processes, which are tedious and inefficient, prone to error, and simply unable to scale to handle the many complex and interrelated applications on your network.



#3 - Siloed teams

The third top mistake is failing to relieve the all too common tension among security, operations, and development teams—all of which are involved in vulnerability remediation processes. The security team is all about “safety first,” while operations is focused on “zero downtime” and development on “move fast and break things.”

Effective communication coupled with sound management can overcome this gap and ensure a robust end-to-end vulnerability remediation process, including verification of fixes across all vulnerability-instances.

First, make sure that vulnerability remediation is understood as a business issue and a company-wide goal by everyone, from line-of-business managers to development and operations teams. This shared mindset is key to a collaborative vulnerability remediation process.

Second, make sure everyone is speaking a common language. It’s not enough to simply give a list of CVEs to IT personnel. Security teams must phrase their requirements in terms that make sense to the teams implementing the solutions. Additionally, remember to point out which vulnerabilities are a priority and require attention first; plus, whenever possible, supply a solution instead of just indicating a problem.

Finally, strive to use quantitative benchmarks that align with your company’s specific needs and processes; in other words, create mechanisms to help measure and demonstrate the vulnerability remediation progress that’s been made. Note that choosing the right benchmarks is essential to ensuring your teams are focused on the right KPIs. For example, instead of tracking the total number of vulnerabilities remediated in a month, you would be better off measuring the risk posture of the most critical business groups in the environment.

#4 - Too many blind spots

Having a complete list of your network’s assets and understanding their dependencies as well as how they can be accessed is an essential part of any vulnerability remediation program. This may seem like a rather straightforward process, but gathering a complete inventory is more complicated than you might expect with today’s distributed and complex architectures.

Good asset management allows teams to implement a more intelligent vulnerability management process and overcome common vulnerability remediation challenges.
Some examples of proper management include:

- **Focused prioritization:** A USB-based vulnerability, even if it has a high CVSS score, does not pose an imminent threat to cloud-based assets.

- **Full coverage:** Avoid scenarios where your security team, say, decides to patch a detected vulnerability using Chef and it seems like “everything” was patched, when, in reality, there remain unknown assets on which the patch was not installed and which are still vulnerable.

- **Avoid unnecessary patching:** Consider a vulnerability that is exploited via an attack through a specific port in your network. Armed with this knowledge, you may decide to simply block the port in its firewall and neutralize the vulnerability, rather than apply a potentially risky patch.

#5 - Misaligned priorities

Last, but certainly not least, is the problem of incorrect priorities in remediation. Given the number of vulnerabilities out there, you've got to have a prioritization methodology that keeps you focused on what really matters. And this means more than just avoiding the hype surrounding threats in today's headlines. It requires taking a fresh look at the conventional approach to prioritization.

Many companies use the Common Vulnerability Scoring System (CVSS) scores as the basis for their remediation decisions. These scores range from 0-10, with 9.0-10.0 being regarded as "critical." Not surprisingly, many companies have adopted the philosophy of "remediate all vulnerabilities marked as critical first" and address other issues thereafter—if they find the time and resources to do so.

While this might sound intuitively correct, in practice, it is not the right methodology. Nowadays, security teams need to adopt a risk-based approach and focus on the vulnerabilities that pose the greatest and most imminent threat to their network. So, when prioritizing vulnerabilities, it's important to remember that CVSS scores and other similar metrics refer to technical risk with no actual context, when every network, in reality, is unique. The same exploit will have a different impact on different environments and therefore the threat that these vulnerabilities pose must be considered differently.

A contextual approach takes into consideration not only the technical severity of the vulnerability, but also the different functions of the assets, their configurations, and their security posture, as well as external threats that may augment the risk posed.

For example, a vulnerability scored as a "medium" threat that is being exploited in the wild may be more dangerous than a "critical" threat that has no known exploits. In fact, cybercriminals may be more likely to choose a lower-ranked vulnerability with a known exploit precisely because they know that critical vulnerabilities are usually the ones fixed first.

Vulcan Cyber to the rescue

The common mistakes described above can result in calamitous consequences and, if overlooked, can leave your environment dangerously exposed. The Vulcan Cyber® risk management platform helps you avoid these all-too-common mistakes by focusing on the following:

Prioritization:
Our platform prioritizes vulnerabilities based on the threat they pose to your unique network. Instead of buying into the hype and news coverage or following non-contextual metrics, Vulcan applies a risk-based approach that takes your environment into account and prioritizes vulnerabilities accordingly.

Visibility:
Through a wide set of integrations, including asset inventories, vulnerability assessment tools, deployment tools, and configuration management tools, the Vulcan Cyber platform gives you complete visibility into your network, flagging misconfigurations and blind spots that your tools might miss.

Collaboration:
Through its different integrations, Vulcan Cyber also allows each team to continue using its own tools while also having access to a single source of truth and central platform across which teams can collaborate in order to achieve seamless, end-to-end vulnerability remediation.

Remediation:
The Remedy Cloud is an AI-based knowledge base that presents each detected vulnerability with a contextual risk score, the number of affected vulnerability-instances, and all relevant remediation options. Scripts for all the leading deployment tools are created at the click of a button.

Automation:
Vulcan Cyber automates remediation so that threats are dealt with promptly, consistently, and effectively. Vulcan Cyber playbooks are clear, intuitive, and easily customized to your specific environment.

VULCAN.™