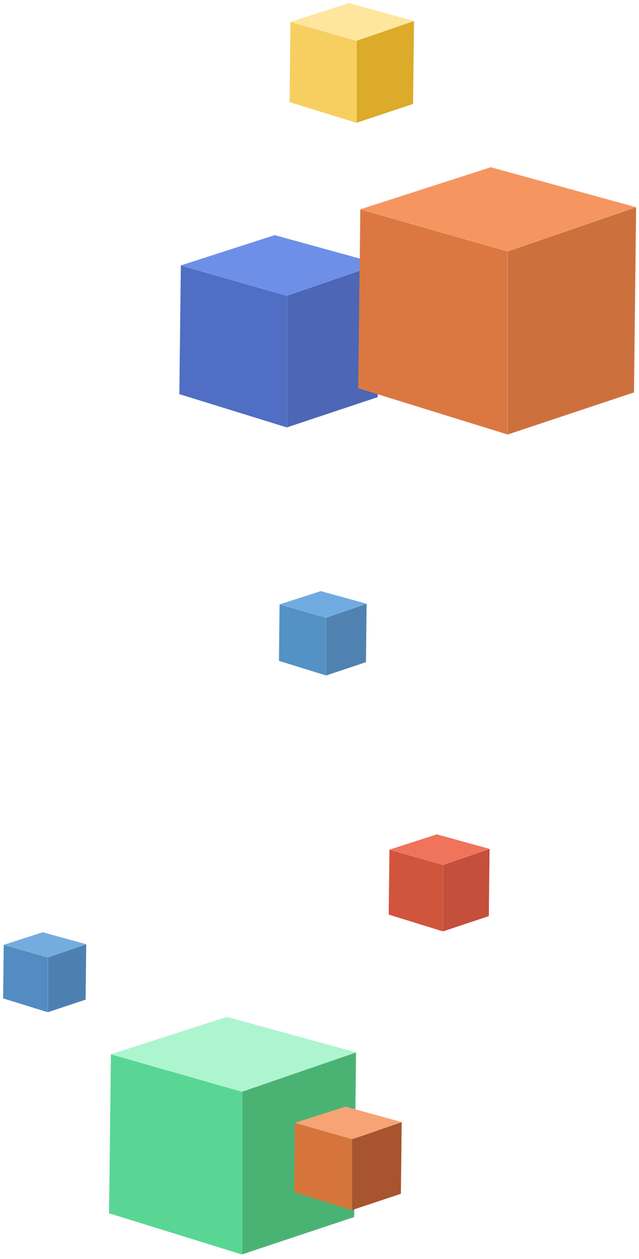
WHITEPAPER

The Business Case for Vulnerability Remediation Orchestration

VULCAN™

Table of Contents



Executive Summary

Today, medium-to-large enterprises spend about 345 hours per week on vulnerability detection and remediation. This translates into an annual FTE cost of about $1,350,000. An additional ~70 hours are spent each week on documentation, reporting, and coordination among teams, bringing the total annual direct cost to around $1,600,000.

The root causes of enterprise vulnerability remediation inefficiency are:

- Manual processes that are time-consuming, not scalable, and harder to implement consistently
- Tension between the different mandates and risk perspectives of security and operations teams (maximum protection versus minimum downtime)
- Cumbersome, disjointed vulnerability remediation workflows, with many handoffs and poor orchestration between siloed security, operations, and development teams

Vulnerability remediation orchestration platforms like Vulcan Cyber® can reduce the time spent on vulnerability detection, remediation, and reporting by 85-90%[1], saving the enterprise as much as $1,440,000 each year while improving its security posture with 100% coverage and risk-based prioritization. These savings are achieved because the Vulcan Cyber platform can:

- **Prioritize:** It uses contextual and smart prioritization to pinpoint the ~2% of new vulnerabilities discovered each week that are truly critical for your specific organization, versus the industry benchmark of identifying ~15% of new vulnerabilities as critical.
- **Focus:** The platform reduces the number of fixes that are deployed on an urgent basis. Emergency patches are more expensive, typically taking 50% more IT person-hours to deploy than non-urgent patches and causing greater disruption throughout the enterprise.
- **Remedy:** Vulcan Cyber automatically identifies the optimal fix by leveraging extensive remediation intelligence data and advanced analytics.
- **Automate:** It reduces time to remediation by up to 90% through automated remediation playbooks and by providing a single source of truth for seamless cross-team collaboration.

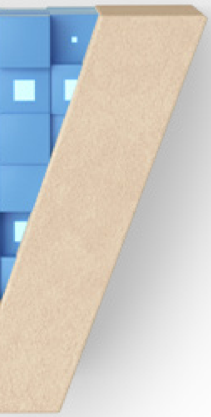
[1] Assuming full automation, after a gradual implementation process.

Introduction

Although YoY global IT spending is expected to drop by 10% in 2020 due to the COVID-19 crisis, it still stands at a whopping $1.05 trillion. In other words, enterprise IT budgets are large. However, they are not infinite, and IT managers must juggle the hardware, software, services, and personnel demands from diverse teams—operations, security, development, and so on. This juggling act becomes even more challenging in enterprises with centralized IT budgets that must also meet the needs of the various lines of the business.

With each team, department, and business unit convinced that its IT requirements are paramount, budgetary decisions must be based to the greatest extent possible on quantifying, comparing, and prioritizing business value to the enterprise. To what extent does any given OPEX or CAPEX budget line contribute to better business outcomes by, for example, reducing operational costs, enhancing the customer experience and the brand, or ensuring regulatory compliance?

This business case helps IT executives quantify the direct and indirect ROI that their enterprises can expect to gain from investing in platforms and processes that enhance the efficiency of their vulnerability remediation programs.



The Enterprise Vulnerability Remediation Landscape

Before jumping into the business case details, it is important to understand two major issues that currently impact enterprise vulnerability remediation: The inherent tension between operational and cybersecurity risk management, and the scope of resources being deployed today by enterprises due to inefficient vulnerability remediation processes.

OPERATIONAL RISK VERSUS CYBERSECURITY RISK: A CONUNDRUM

Vulnerability remediation in an enterprise often takes place within the context of a critical tension between the cybersecurity risk managed by the security team and the operational risk managed by the operations team.

The mandate of security teams is to close the gaps that could result in exploited vulnerabilities with potentially devastating direct and indirect costs for the enterprise. Thus, they diligently monitor corporate assets for vulnerabilities. When a vulnerability is detected, they pass it on to the operations team for remediation, but often without the analysis or recommendations that would make the task more actionable and straightforward.

The operations teams are now faced with the task of remediating the vulnerability without undermining their key mandate, which is maintaining business continuity. With modern applications being highly distributed and deployed across complex and dynamic infrastructures, it is up to the operations team to assess the risk that a vulnerability remediation process will cause unacceptable levels of downtime or—even worse—disrupt or break business-critical applications. Because the operational risk as assessed by the operations team usually overrides the security risk concerns of the security team, many known vulnerabilities are not remediated.
Yet another barrier to remediation is operational uncertainty about the solution to deploy. Among the different types of possible solutions, which will be the most effective while also being the least disruptive?

These tensions and uncertainties have been undermining enterprise security postures for a while now, with Gartner predicting a few years ago that 99% of the vulnerabilities exploited by the end of 2020 will be known by security and IT professionals at the time of the incident.

THE UNBEARABLE COST OF INEFFICIENT VULNERABILITY REMEDIATION

The average enterprise currently dedicates a total of around 413 weekly hours—equivalent to almost 10.5 full-time employees—to vulnerability detection and remediation (345 hours) and reporting (another 70 hours).
Yet many of those hours could be diverted elsewhere if vulnerability remediation processes were more efficient; companies would then also benefit from lower cybersecurity risk and a higher security posture.

Vulnerability remediation inefficiency is due in part to the disconnect described above between operations and security teams. Attempts to balance the two types of risk often result in the vulnerability remediation process becoming cumbersome and disjointed, with poor communications across the relevant stakeholders.

Another root cause of inefficiency is that current vulnerability remediation processes are still largely manual. In the August 2020 Ponemon report on "The state of vulnerability management in the cloud and on-premises," 51% of respondents admitted that manual processes were an obstacle to timely vulnerability remediation. With the number of vulnerabilities to be remediated constantly growing, manual processes are not only inefficient, they are also error-prone and not scalable.

In order to address these issues that significantly undermine the effectiveness and efficiency of their vulnerability remediation programs, this business case shows how enterprises can get a high return on investment from platforms that:

- **Precisely pinpoint which vulnerabilities pose a high risk to the organization**
- **Promote streamlined and collaborative remediation processes**
- **Automate remediation processes to the greatest extent possible**

Our Hypothetical Enterprise

Although enterprises vary dramatically in size, scope, IT requirements, vulnerability exposure, and so on, this business case is based on a hypothetical enterprise that meets the following description:

- The enterprise manages ~50,000 assets, of which 40,000 are servers (hosts, web servers, etc.) and 10,000 are endpoints (desktops, laptops, etc.). It has 20 code repositories under management as well as 20 public-facing websites.
- The enterprise encounters 1,000 new vulnerability instances per week.
- The average fully loaded FTE cost for a security engineer is ~$140,000/year.
- The enterprise spends 413 hours/week (i.e., 10.3 FTEs) on vulnerability detection and remediation.
- Based on a 2019 Symantec study across thousands of enterprises:
  - It takes this enterprise an average of 6+ months to patch 90% of endpoints against vulnerabilities in 12 enterprise applications.
  - It takes over 9 months for 90% of the enterprise server population to be patched and, on average, its server applications remain vulnerable for 7.5 months.

Fewer Critical Vulnerabilities to Remediate

As noted above, the hypothetical enterprise encounters 1,000 new vulnerability instances per week. Attempting to remediate all of these vulnerabilities would be prohibitively expensive (and most likely impossible). However, from the cybersecurity perspective, it is unacceptable to overlook a vulnerability that poses a high risk to business-critical assets.

Hence, the enterprise's cybersecurity team initially uses CVSS scores to differentiate between low- and high-level vulnerability alerts; they then use threat intelligence to further analyze and prioritize the new vulnerabilities.

Typically, this prioritization process identifies ~15% of the new vulnerabilities as critical and requiring immediate remediation.

Although dealing with 150 critical new vulnerability instances per week is better than trying to manage 1,000, it still presents a significant load on the enterprise's vulnerability remediation process. If prioritization, however, were both automated and contextual, it would not only streamline manual processes but also achieve much higher levels of precision by pinpointing the vulnerabilities that pose the highest business risk.

Vulcan Cyber, for example, automatically enriches CVSS scores with the organization's internal business data from the likes of asset inventories and CMDBs, as well as with threat intelligence gathered from external sources. As a result, the Vulcan Cyber platform can typically pinpoint automatically the ~2% of new vulnerabilities that are critical to the enterprise and therefore require immediate remediation.

Optimizing vulnerability prioritization, therefore, has two quantifiable benefits: automation of the largely manual prioritization process and fewer critical vulnerabilities to remediate. As shown in Figure 1, automated prioritization saves 90% of the cost of one FTE, i.e., just under $126,000/year. As shown in Figure 2, having fewer critical vulnerabilities to remediate saves about 85% of the cost of 3.4 FTEs, i.e., $404,600/year. **Together these benefits represent an annual savings of $530,600.**

LEGACY VULNERABILITY REMEDIATION PROCESSES AND TOOLS

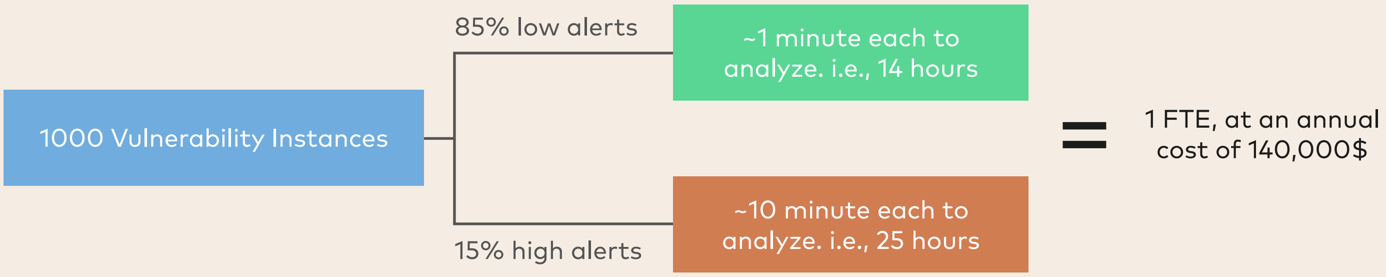

1000 Vulnerability Instances
85% low alerts
~1 minute each to analyze. i.e., 14 hours
15% high alerts
~10 minute each to analyze. i.e., 25 hours
=
1 FTE, at an annual cost of 140,000$

Figure 1: Traditional prioritization weekly effort versus minutes with Vulcan Cyber

VULCAN CYBER

Automated, smart prioretization requires virtually no analyst intervention, saving at least 90% of the FTE costs, i.e., **a savings of just under $126,000/year.**

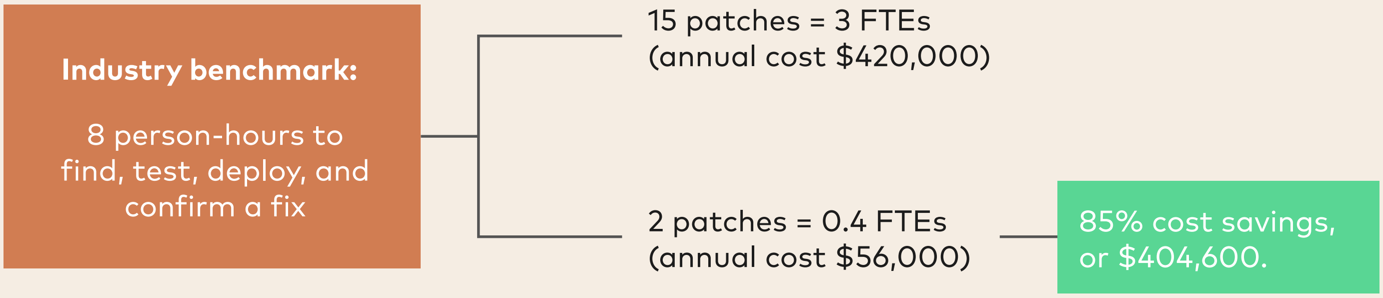

Industry benchmark:
8 person-hours to find, test, deploy, and confirm a fix
15 patches = 3 FTEs (annual cost $420,000)
2 patches = 0.4 FTEs (annual cost $56,000)
85% cost savings, or $404,600.

Figure 2: Cost savings by significantly reducing the number of vulnerabilities to be remediated

It should also be noted that reducing the number of critical vulnerabilities to be remediated on an urgent basis also has significant value for the enterprise. Remediation campaigns with a high sense of urgency are typically conducted in a war-room-like atmosphere, with all hands on deck. This kind of campaign disrupts not only IT staff and activities, but wide circles of people and activities throughout the organization. In fact, the industry benchmark for the deployment of emergency patches is 12 person-hours, or 50% higher than for non-urgent patches.

Faster Time to Remediation

Another pain point for the aforementioned hypothetical enterprise is how long it takes them to implement a fix for all those non-critical vulnerabilities that didn't require immediate and urgent remediation. As noted above, on average, it takes them at least six months to remediate a client-side vulnerability and at least nine months to remediate a server-side vulnerability—as measured from the date when the vulnerability was first identified to the date when a scan shows that it was remediated. A typical remediation process, once initiated, takes about a month to complete on average. In cases where the vulnerability itself is complex or has a particularly high operational impact, the remediation process will take longer. For example, the vulnerability may involve an application that has many dependencies, and the fix has to be tested thoroughly to ensure that it does not degrade or disrupt system performance. Another example is when the vulnerability impacts a now-fragile legacy system or a system with high technical debt. A typical remediation process may look something like this:

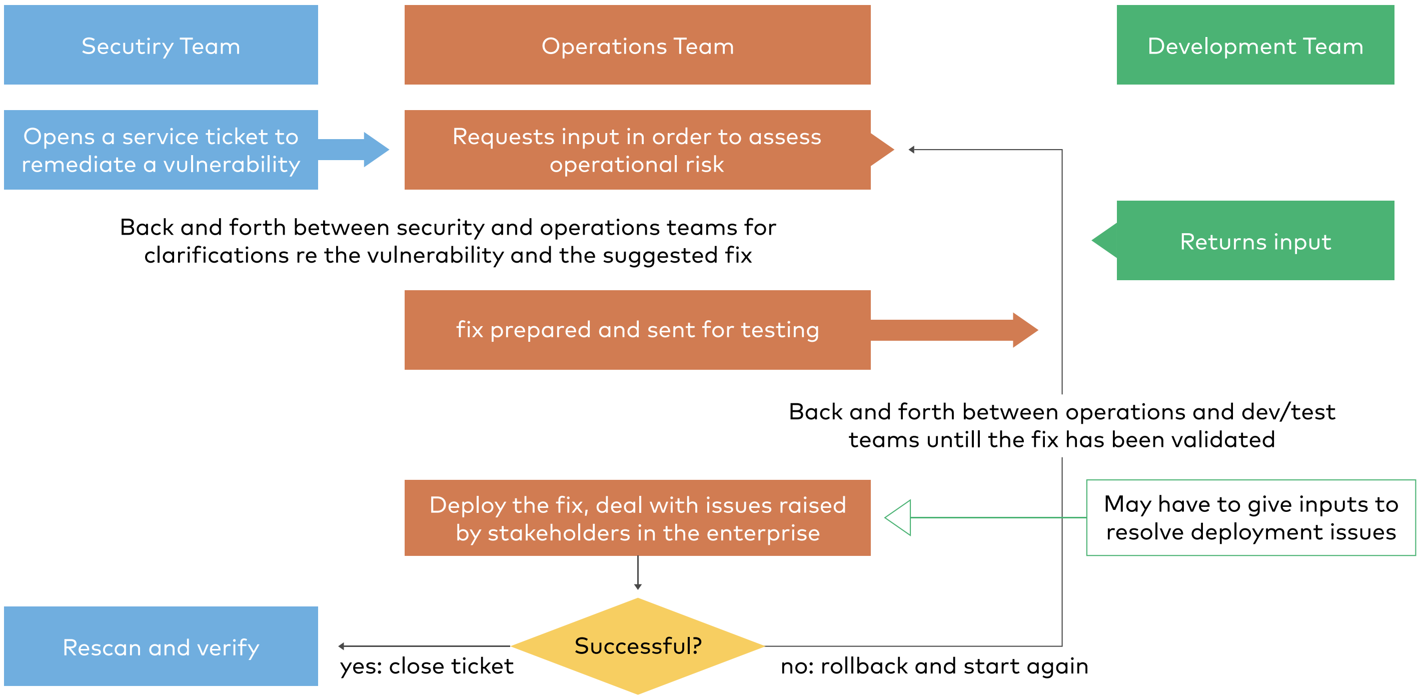

Secutiry Team
Operations Team
Development Team
Opens a service ticket to remediate a vulnerability
Requests input in order to assess operational risk
Returns input
Back and forth between security and operations teams for clarifications re the vulnerability and the suggested fix
fix prepared and sent for testing
Back and forth between operations and dev/test teams untill the fix has been validated
Deploy the fix, deal with issues raised by stakeholders in the enterprise
May have to give inputs to resolve deployment issues
Successful?
yes: close ticket
no: rollback and start again
Rescan and verify

Figure 3: Typical traditional remediation process

Some of the key inefficiencies built into the process shown schematically in Figure 3 are:

- Multiple teams are involved at different stages of the process, with many manual hand-offs from one team to another.
- The teams are siloed and often in the dark during long stretches of the process. Other than the service ticket, there is no single source of truth across which the teams can collaborate.
- Overall, there is poor end-to-end visibility and control across the process. In the Ponemon study on the state of vulnerability management noted earlier, close to 60% of the respondents reported that their organization could not effectively track the timeliness of their vulnerability patching process.

The Vulcan Cyber Remediation Orchestration Platform provides vulnerability remediation that can condense a month of fixing, tracking, and verifying into less than an hour. In addition to the smart prioritization already discussed above, some of the most relevant features are:

- Easy integration with the enterprise's existing tools (asset management, configuration management, deployment tools, and so on) allows for them all to be orchestrated into a seamless remediation stack.
- The platform features an extensive and proprietary Remediation Intelligence database containing millions of remediation actions in the form of patches, configuration changes, workarounds, or compensating controls. Through this database, the platform leverages machine learning and cybersecurity research to automatically recommend the most appropriate fix for any vulnerability. In many cases, the fix can also be deployed automatically. By reducing uncertainty and downtime through streamlined and highly focused remediation measures, Remediation Intelligence bridges the gap between security and operations teams.
- Pre-defined playbooks automatically drive the process forward and keep all teams aligned.
- Vulcan Cyber provides a single console and source of truth for the remediation in process, with all teams kept continuously updated as to the progress and status of the fix.

The first benefit of faster time to remediation is that vulnerable assets are protected faster, thus reducing the risk of costly successful exploits. Although it is hard to put a price tag on such a benefit, it is a strong proposition in any business case for more efficient vulnerability remediation. The second benefit is that streamlined, automated, and scalable vulnerability remediation processes can reduce FTE costs by as much as 85%. In the case of the hypothetical enterprise discussed herein, assuming that 75% of its 10.3 FTEs' time is spent on remediation per se, the potential annual cost saving is: ((10.3 x $140,000) x75%) x 85% = ~$919,000.

Enhanced Coverage

An enterprise's vulnerability remediation program is only as good as its scanning coverage and cadence. Every unscanned asset—whether a host, endpoint, code repository, or web application—is a weak link. However, enterprises tend not to scan 100% of their assets and not to scan continuously for two key reasons:

- They are overwhelmed by the sheer quantity of incoming data. Going back to the hypothetical enterprise, it is monitoring 50,000 assets, 20 code repositories, and 20 web applications. It's hard to imagine the quantity of scanning data such an environment would generate.

- They are overwhelmed by the diversity of the incoming data. This hypothetical enterprise is most likely operating dozens of scanning tools, each with its own unique output. How can it get actionable insights from such diverse data?

The bottom line is that the industry benchmark today is about 85% scan coverage, meaning that 15% of its assets are unscanned at any given point in time.

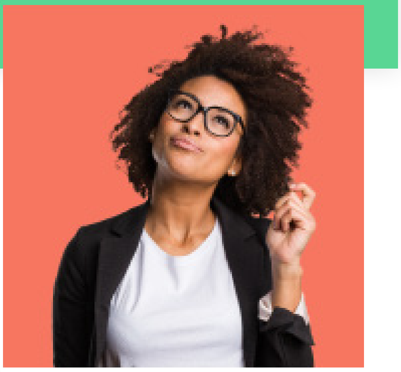
Vulcan Cyber, however, facilitates 100% and continuous scan coverage by thriving on big and diverse data. The more scan data and types of scan data that Vulcan Cyber receives from the enterprise's array of scanners, the smarter its prioritization and the more targeted its remediation recommendations.

The cost to an enterprise of a breach due to an unscanned host can be considerable. The Ponemon study found that 53% of companies have experienced such a breach over the last two years. In 2020, the average cost of a successful data breach was $3.86 million, or $146 per record lost. In the first half of 2020, a total of 16 billion records were exposed, which is 273% higher than the number of breaches in the first half of 2019.

Efficient Vulnerability Management Accelerates the Business

This business case has shown the direct and indirect cost savings that an enterprise can gain from investing in more efficient vulnerability management and remediation. Although these quantifiable benefits are important in and of themselves, there is also a compelling strategic gain. By spending less time on correlating tools, people, and processes, enterprise IT teams can focus with greater clarity on core operational and security issues that significantly impact overall business outcomes. This gives yet another example of how IT can and should be transformed from a supportive enabler into a full partner in moving the enterprise forward.

Optimize your vulnerability management processes, and overcome the conflicts between your operational and cybersecurity needs with the Vulcan Cyber Remediation Orchestration Platform today.



VULCAN.™