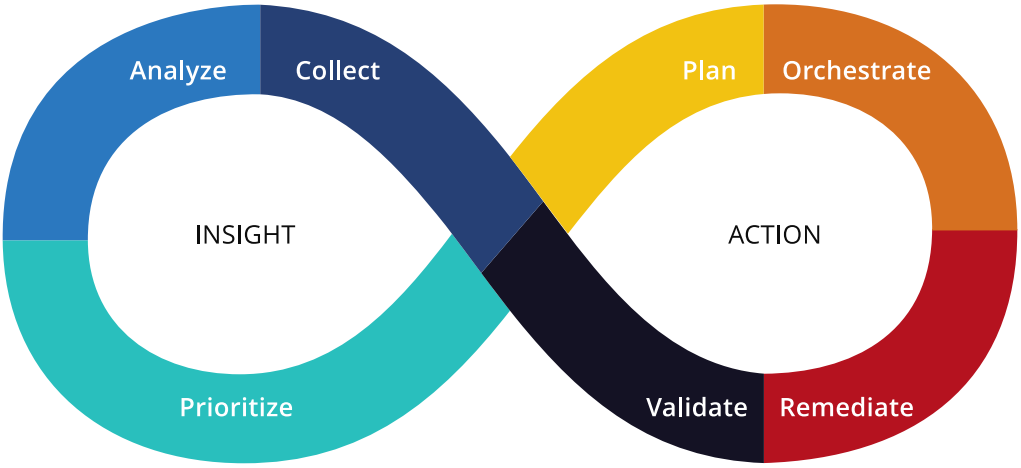
Why Continuous Software Exposure Demands Continuous Remediation

Three steps to fix what's broken in modern software vulnerability management



A Vulcan E-Book • May 2018

VULCAN
mind the gap

Contents

A New World of Software Stack Vulnerabilities

Organizations depend on software stacks to run their business, compete, and innovate.
With the dramatic change in digital dependence and the adoption of agile development and DevOps methodologies - the stakes have risen dramatically in the past decade. Organizations are now continuously exposed to threats from vulnerabilities, whereas in previous years the danger was more intermittent.

What's contributed to this spike in vulnerability exposure?
Consider that:

Less than a decade ago, Saas and cloud-based development and deployment were in its infancy. Software assets and tools were all either on-premise or in remote data centers with dedicated communications. Today, all enterprises are at least partially cloud-based, many are fully so - leaving exploitable assets exposed to anyone, rather than hiding safely behind corporate security perimeters. Moreover, the shift in development paradigms means that mission-critical software is continuously changing, with less inspection and testing - allowing vulnerabilities to easily slip into production.

The software ecosystem has exploded. Software environments used to consist of solutions from a severely limited number of vendors - literally fewer than 10. Today, enterprises are open to working with smaller vendors and multi-platform solutions, which has led to dramatic growth in the number of vendors. These vendors are more likely to be enterprise-ready, and to conduct comprehensive vulnerability research on their software. Thus, more and more vulnerabilities of all types are being disclosed and must be addressed.

Vulnerability assessment and patch management has taken off.
Ten years ago, you would have found one or two vulnerability assessment and patch management tools in an organization.
Today, there are up to 20. The sad fact is that because enterprise software is interconnected, patching one component can break an entire system.

Lastly, the growth in digital complexity has brought a corresponding growth in the number of disclosed vulnerabilities:

In **2000** there were 1020

In **2010** there were 4652

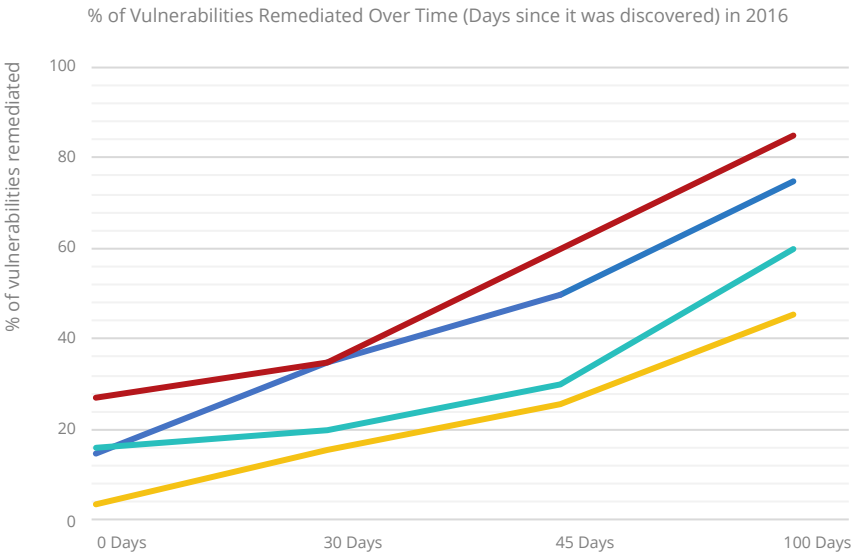
In **2016** there were 6447

In **2017** there were 14704

What's worse, the gap between the discovery of a given vulnerability and its remediation has grown drastically too: Vulnerability Remediation Gap at Verizon

Verizon Data Breach Report, 2017

- % of Vulnerability Remidiatied in **Servers**
- % of Vulnerability Remidiatied in **Network Devices**
- % of Vulnerability Remidiatied in **User Devices**
- % of Vulnerability Remidiatied in **Embedded Devices**



2017- Just When You Thought It Couldn't Get Worse

2017 was a watershed in vulnerability remediation. It was the year in which everything changed, and the benchmark by which we should measure vulnerability assessment and vulnerability management going forward. Why?

In the years leading up to 2017, the vulnerability mindset was **Stuxnet-oriented**.

The Stuxnet worm brought the potential physical-world consequences of vulnerabilities into the public consciousness. Zero-day, or unknown, vulnerabilities were often closely-held by state-actors like the NSA and FSB, and massive and expensive remediation efforts were focused on solving each vulnerability, using sophisticated tools like machine learning.

Yet in their focus on identifying the next jumbo-size zero-day vulnerability, security stakeholders and vendors neglected to address the ever-growing list of known vulnerabilities. This strategic mistake led to the one-two knockout punch in 2017, from which the vulnerability world is just now starting to recover. The **Equifax** breach and the **Eternal Blue** vulnerability were, without exaggeration, earth-shattering:

Equifax's **failure to patch** a known two-month-old vulnerability led to a massive breach that exposed the details of some 145 million people - arguably the largest vulnerability-related **PII** breach to date.

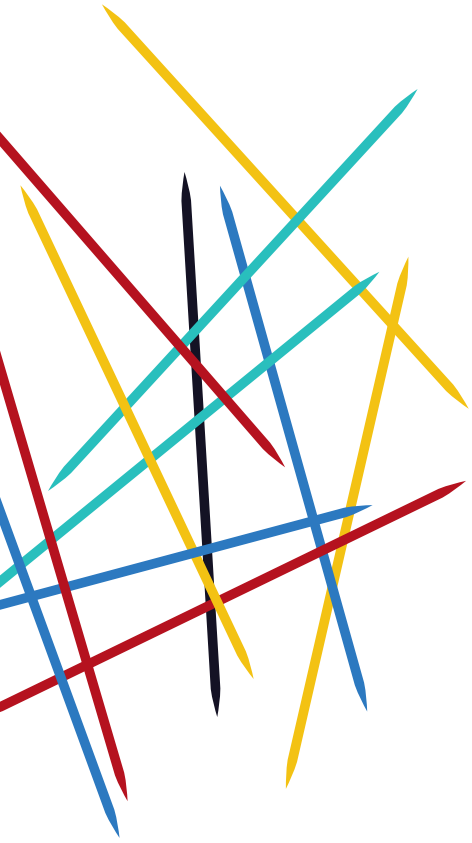
Eternal Blue was the basis for the **WannaCry and Petya** ransomware attacks - two of the largest in history, which massively impacted company finances across the globe

Today, it's not just CISOs who have to worry about vulnerabilities and patching. Company board and C-level executives are now also responsible for ensuring processes are in place that minimize risk. The potential for personal criminal and civil liability, damage to brand equity, and negative impact on revenues is keeping stakeholders of all levels awake at night - and with good reason. Because despite best efforts, it's still estimated that by 2020, 99% of exploited vulnerabilities will have been known for at least a year.

Vulnerability Remediation: Key Challenges

The transition to the cloud and an agile development paradigm has presented the opportunity for agile vulnerability management. Yet two key stumbling blocks to continuous and effective vulnerability remediation remain:

Prioritization



It's not always readily apparent which vulnerabilities are the most important to fix and will have the most significant impact on an enterprise. In years past when total numbers of vulnerabilities were few and far between - prioritization of vulnerabilities based on technical severity was a far less problematic systematic approach. Today, however, prioritization needs to be based on the correctly-weighted fusion of:

Technical severity

Generally reflected in each vulnerability's **CVSS** score, this is the sole aspect that the majority of vulnerability assessment tools focus on today.

Exploitability

How is a given vulnerability being used in the real world? Are there known public exploits, like scripts that anyone can download to use the vulnerability? Are there active campaigns exploiting this vulnerability, and if so what type (ransomware, DDoS, malware, etc.)? In which vertical markets (financial enterprises, SaaS companies) are we seeing greater exploitation of the vulnerability?

Business impact

How does a given vulnerability impact my own network? The ultimate business impact of every vulnerability - no matter how technically severe or exploitable - is measured by how it affects business.

Responsibility

Even when a vulnerability remediation plan exists, most application and infrastructure security teams do not have hands-on implementation capabilities. Rather, these teams work with other teams: R&D to plan, write and fix code, QA to check bugs and authorize patch deployment, IT to actually deploy, DevOps to change architecture or replace packages. Coordinating between teams to orchestrate remediation is always complex – and all the more so when security may not be their top priority, and the primary tools are Excel and email.

What's Broken in Vulnerability Remediation Today?

With vulnerabilities so firmly on the executive radar, organizations realize they need to take action. The problem is that most organizations still focus on **patching** and a **tiered vulnerability management processes:**

Patching

Taken in a vacuum, patches solve vulnerabilities. The problem is, in IT nothing exists in a vacuum. Patches are usually bundled with features or updates, which may have a wildly unpredictable impact. Moreover, automatic or single-component patching can often break the entire systems - causing downtime and interrupting business processes. Finally, though patching specific software on PCs is not challenging for most organizations, patching servers and networks is far more complex - they break more than they fix, and should be applied selectively, intelligently and strategically.

Organizations need to keep in mind that patching is not necessarily the only solution; there are other options that are as effective, less disruptive, and ultimately faster - including updating signatures in Web Application Firewalls (WAF), IPSs, or configuration changes of the vulnerable software.

Tiered Vulnerability Management Processes

Cross-organizational teams composed of IT, security, DevOps, and R&D use complex vulnerability management processes operating dozens of detection tools to discover thousands of potential vulnerabilities. Each of these needs to be analyzed, categorized, and remediated if relevant. This generates a lot of data that needs to be manually reviewed - but provides few insights into the business impact of vulnerabilities, how remediation should happen, and who should do the remediating. Thus, existing processes often create far more work and interdepartmental friction than they identify and resolve vulnerabilities.

And this is what's broken in vulnerability management. Because neither patching nor existing processes can provide a timely and focused response to vulnerabilities, organizations have given up on prevention and rely, by default, on incident response and forensics. This traditional methodology addresses malicious vulnerability exploitation by identifying an ongoing incident as quickly as possible, responding in an attempt to mitigate damage, and then dissecting how the event unfolded in the hope of ensuring that future, similar attacks don't occur. The ex post facto wisdom gained from this process is valuable from a security perspective. Yet with the rapidly-evolving threat environment, the potential costs of even a single incident are prohibitively high.

Three Steps to Fix It

The transition to the cloud and an agile development paradigm has presented the opportunity for agile vulnerability management. Yet two key stumbling blocks to continuous and effective vulnerability remediation remain:

Step 1

Improve Visibility

The fact that vulnerability detection systems are siloed and provide insights separately based on the platforms and infrastructures they scan - code, applications, production and more shouldn't force teams to look, act and prioritize them in a detached way.

A sound vulnerability remediation process should enable teams to view all vulnerabilities under the same parameters clearly, regardless of where they reside in the infrastructure. Remediation actions would then be based on their business impact and severity, and not their vulnerability type. This is especially critical for tech and SaaS companies, where the interdependency between code and production and their business is clear.

Step 2

Enrich Vulnerability Remediation With Intelligence and Smart Prioritization

Currently, vulnerabilities are detected and prioritized based on technical severity alone by vulnerability detection systems. Yet what determines actual vulnerability severity is threat intelligence, as well as the greater business, ecosystem, and technical context. Without context, a severe vulnerability on a little-used, low-value system would be remediated before a medium-severity vulnerability on a mission-critical system.

Effective vulnerability remediation should offer integrated, intelligent and weighted insights derived from multiple IT systems. The ultimate goal: precise, infrastructure-focused and context-sensitive prioritization of vulnerabilities. In prioritizing vulnerabilities in production, application, and code, security teams consider the overall status of the vulnerability within the larger landscape of vulnerabilities at that very snapshot in time - to determine a vulnerability's

technical severity and overall level of exploitability. For example, are there active campaigns and if so, which ones? Which asset is affected, and what is its importance vis-a-vis a company? What is the asset's level of exploitability within the network and its corresponding risk factor? Is the vulnerability highly protected, for example, at the core of a network - or otherwise minimally protected?

Smart prioritization of exposures and vulnerabilities uses intelligence and analysis of their parameters and context.

Step **3**

Create a Trans-Organizational Culture of Vulnerability Remediation

Security teams working in vulnerability detection and remediation should at once:

prioritize helping individual units continue to work on their own priorities (for example, IT employing patches, DevOps changing architecture and replacing packages, and R&D fixing code); and

ensure that vulnerabilities are addressed in newly defined processes and SLAs both quickly and with minimum levels of friction.

This way security teams become facilitators in this process - helping other teams determine how many resources to allocate, and with which urgency to utilize their tools and expertise in both defining said expectations and building solutions. It allows IT, DevOps and R&D to continue to work on their own systems, (IT team to employ patches, DevOps teams to change architecture or replace packages, and the R&D team to fix code) organically in their comfort zone and areas of expertise, while still enabling trans-organizational collaboration.

It is here that we can begin to create a more effective culture of vulnerability remediation - in sharing actionable insights and utilizing methodologies grounded in transparency - reflecting the complexity of unrelenting security risks.

About Vulcan

Vulcan Cyber is a Continuous Remediation platform that integrates vulnerability assessment, IT and DevOps tools, automating and orchestrating existing tools and processes, to eliminate the most critical risks caused by vulnerabilities - while at the same time avoiding any unexpected impact to business operations.

Vulcan Cyber understands that known vulnerabilities are truly where the rubber meets the road. Today, the only way to deal with the continuous risk of new vulnerabilities is through continuous remediation achieved by data collection, smart analytics, simple automation, and closed-loop remediation planning and orchestration.

Vulcan Cyber's comprehensive orchestration and validation deliver unprecedented insight, ability, and confidence - eliminating exposure and risk. Vulcan closes the vulnerability remediation gap and creates a trans-organizational culture of vulnerability remediation; continuous exposure demands continuous protection.

Vulcan Cyber - Insight to Action.