4 Steps to Achieving Risk-Based Vulnerability Management

Introduction

By 2022, organizations that use the risk-based vulnerability management method will suffer 80% fewer breaches.

-Gartner, "A Guide to Choosing a Vulnerability Assessment Solution," April 2019

Scanning network assets to identify security gaps and system vulnerabilities is a foundational element to any information security program. Beyond the security implications, there are sound business reasons for establishing a formal vulnerability scanning and remediation program. What many organizations do not realize is that 60% of all data breaches result from a software vulnerability.   Even more concerning in these instances is the vulnerability which caused the data breach had a known fix that was not applied. For organizations that do not want to be the next breach headline, establishing a risk-based vulnerability management program makes good business sense.

Despite all the business and risk benefits, vulnerability scanning is not without its own set of challenges. The good part about vulnerability scanning technologies is they collect lots of data for validating evolving risks…the bad part is that the volume of data returned can be extensive. With each scan generating 30-40 vulnerabilities per asset, the numbers can quickly become overwhelming. Consider the implications of a network with 1,000 assets. The mitigation team is faced with 30,000-40,000 data points each time a scan is run. So, it all comes down to resources and how much time is available to fix the widespread quantities of vulnerabilities they face.

Unfortunately, 77% of organizations lack sufficient patching resources, according to Ponemon Institute 2019, to address all vulnerabilities. Under these circumstances, the most daunting task is determining what vulnerabilities get patched.

Traditional Mitigation Strategy

> 77% of organizations lack sufficient patching resources to address all vulnerabilities.
>
> *-Ponemon Institute 2019*

In most cases, perceived risk is the driving factor that impacts patching behavior. While CVSS scoring is the prevalent approach for identifying and prioritizing which vulnerabilities get patched, it does have limitations. Most vulnerabilities are theoretical by nature (regardless of the CVSS score). With limited resources and escalating vulnerability counts, most organizations adopt a Traditional patching strategy that focuses on the Critical and High vulnerabilities. This approach usually delivers “do the best we can” results since the aggregate of these two categories (Critical and High) are on average 25% of the vulnerabilities generated with each scan.

If a monthly scan on a 1,000-asset network generates 30,000-40,000 vulnerabilities, the Traditional mitigation strategy yields a mitigation scope of 7,500-10,000 vulnerabilities. Even with efficient patching tools, planning 15 minutes to patch each vulnerability requires 1,900-2,500 hours of mitigation support each month. These high numbers push organizations into a mode of starting at the top of the Critical list and working though the vulnerability list to “do the best they can.” With insufficient resources to meet patching demand, the vulnerability counts grow month after month while continuing to age. The longer a vulnerability exists, the more likely it can be leveraged to cause harm.

4 Steps to Achieving Risk-based Vulnerability Management

For organizations that are results-oriented…the real question is how to start “chipping away” at the ever-growing mass of accumulated vulnerabilities. And more importantly, how does an organization with limited resources prioritize vulnerability findings to maximize impact? The answer requires a blend of unified process and technology that are detailed in this section.

1. **Address Exploits**

2. **Identify Heavy Hitters**

3. **Subscribe to Threat Intelligence**

4. **Manage Accountability**

1. Address Exploits

An exploitable vulnerability has a defined approach for leveraging it to disrupt or gain unauthorized access to the infrastructure.   The threat each represents is based on several variables including:

- **Type of asset it impacts**
- **Skills of the entity leveraging it**
- **Criticality/value of the asset on which it resides**
- **Maturity and age of exploit**
- **Whether or not the exploit has been used in the real world**

Since exploitable vulnerabilities represent about 3% of those identified during a scan, organizations with limited resources should allocate them toward addressing them above any other priority. It is equally important to look at them across all the reported priority levels. Since most scanners categorize vulnerabilities based on a CVSS ranking, many organizations will focus resources exclusively on those ranked as Critical and High. Because exploitable vulnerabilities can (and often do) appear on non-mainstream equipment like printers and switches, they may appear as a Medium CVSS ranking. As such, an organization that focuses exclusively on mitigating Critical and High vulnerabilities would never investigate or mitigate an exploitable with a Medium CVSS ranking. This example illustrates how the even the best-intentioned approach can still leave organizations exposed to real threats.

2. Identify Heavy Hitters

The number of vulnerabilities identified during each network scan can be seemingly overwhelming. The common question organizations face is where to start? Since a key goal is to reduce vulnerability counts, looking for vulnerabilities that appear on many assets is an effective way to address this challenge. A heavy hitter is a unique vulnerability that appears on many assets. If a single vulnerability appears on every asset in the enterprise…applying a single patch will have a big impact on reducing overall vulnerability counts. Depending on the scan toolset being used, a data sort or predefined report are the most effective way to identify these types of vulnerabilities. Once a list of heavy hitters is generated, it can be further refined to prioritize based on CVSS category and exploitability. Applying a structured approach of this type will maximize resource utilization to drive results.

3. Subscribe to Threat Intelligence

Another way to prioritize and identify the most important vulnerabilities to fix is with assistance from external threat intelligence resources. Scanning technologies work from a standardized set of criteria for referencing and categorizing vulnerabilities. This information is used by mitigation teams to evaluate, prioritize, and fix vulnerabilities. In essence, the mitigation teams know what they know about vulnerabilities; external threat intelligence will help them understand what they don't know.

There are several qualified vulnerability threat resources available in the market today. One example of a well-rounded threat intelligence resource is Cyr3con. Their firm does dark web research that looks at social media, chat rooms, forums, and other platforms where attack techniques are being discussed and developed. Their team does the research in multiple languages spanning more than 1000 hacker sources. Information collected is fed into artificial intelligence software that assigns risk scores to vulnerabilities. The resulting detail highlights vulnerabilities that are most likely to be the targets of attacks. The higher the score…the more likely it is to be attacked. This type of detail transcends the typical CVSS and exploitable classifications providing additional insight to help improve the process of prioritizing mitigation activities.

Each threat intelligence solution will have its own approach to qualify what vulnerabilities are the highest priority for patching. Taking the time to understand which one aligns best with the scanning tool, process, and resources used in the current program will reduce onboarding time and improve the return on investment.

4. Manage Accountability

Understanding what, when, and where vulnerabilities need to be patched is a foundational requirement for any program, but the story does not end there. Establishing and managing a process for assigning mitigation and tracking progress is just as important. Accountability is the other half of the equation for delivering results.

There are numerous technologies that support tracking results, ranging from simple (MS Excel worksheet) to complex (Workflow-based ticketing systems). Regardless of the platform used, a culture of accountability is founded on key principals:

Set Reasonable Goals

Track and Publish Results

Schedule Reviews

Ensure Management Support

Diligence is Critical

At first glance, these principals may seem like a simple statement of the obvious. The challenge is not in understanding why they are important; it's in following through and consistently adhering to them. Because vulnerabilities never stop, organizations can suffer from patching fatigue, which in turn can stall program progress. Adopting a cadence and sticking to it a foundational success factor that cannot be ignored.

The simple reality is that vulnerabilities provide a never-ending workload stream for mitigation resources. Some equate the process of vulnerability management to the arcade game called whack-a-mole. This analogy rings true as it seems like the moment one vulnerability is patched…three more pop up to replace it.

Beyond understanding what vulnerabilities must be fixed first, a documented and repeatable process is necessary for delivering consistent results. It takes diligence and focus…but success is attainable.

TARA

Developed by Security Vitals

Leverage predictive prioritization to deliver true risk-based vulnerability management with TARA. Developed by Security Vitals, TARA identifies and validates evolving risk in your company including work from home environments.

How TARA works:
Step 1 - Scans your environment for vulnerabilities
Step 2 - Feeds dark web research into AI to predict risk and map it to vulnerabilities
Step 3 - Prioritizes mitigation and tells you what to fix

Security Vitals has the broad experience of supporting enterprises large and small. Leveraging risk evaluation tools and process, we reveal the areas of greatest risk and help you effectively apply resources to mitigate it.   For organizations that need ongoing assistance, we also offer managed security programs that provide monthly support to address risk from both a process and technology perspective.

Request a Demo Today

svtara.com | (866) 802-9405 | sales@securityvitals.com

TARA