Whitepaper:

How to Prioritize Risk Across the Attack Surface.

REGARDLESS OF ORGANIZATION SIZE, YOU WILLNEVER HAVE ENOUGH RESOURCES TO FIX EVERY VULNERABILITY ACROSS YOUR ATTACK SURFACE. RISK PRIORITIZATION IS ESSENTIAL.

Security teams need to understand vulnerabilities in context

Businesses of all types and sizes are being overwhelmed by the sheer number of vulnerabilities already in their networks. And, that number is growing quickly, as modern networks become larger with the shift toward remote work and BYOD – leading to an ever-expanding, dynamic attack surface.

Security leaders need to understand vulnerabilities in context and use that data to prioritize their team's efforts.

But, there's a problem: We are dealing with more vulnerabilities today than ever before. In fact, the number of vulnerabilities has nearly tripled in the last couple of years[1].

Legacy methods are failing

According to US Cert in 2021 alone, 18,376 new vulnerabilities were disclosed. That means, on average, security teams are facing 50 new vulnerabilities every day. Already short on resources and time, security teams need an easy way to prioritize which vulnerabilities to fix first.

Many organizations are using legacy methods like the Common Vulnerability Scoring System (CVSS) to try to prioritize vulnerabilities for remediation. Most enterprises will attempt to remediate all the High and Critical vulnerabilities (CVSS score of 7 and higher). Some may opt instead to simply concentrate on the Critical vulnerabilities (CVSS score of 9 and higher).

> "CVSS is designed to identify the technical severity of a vulnerability. What people seem to want to know, instead, is the risk a vulnerability or flaw poses to them, or how quickly they should respond to a vulnerability." – Carnegie Mellon University[2]

[1]Tenable Research

[2]Towards Improving CVSS, Software Engineering Institute, Carnegie Mellon University, December 2018

CVSS classifies too many vulnerabilities as High or Critical

According to security research, 56 percent of vulnerabilities are assigned a CVSS score of 7 or higher – and are, therefore, considered High or Critical (see Figure 1). That means, for every 100,000 vulnerabilities, CVSS dictates that security teams would have to remediate 56,000 of them. So, it's not hard to see that using CVSS, workloads quickly spiral out of control, especially given that most large enterprises have millions of vulnerabilities.

Legacy Prioritization Methods Are Ineffective

- 56% of all vulns are rated High or Critical
- CVSS is risk-unaware
- Teams waste the majority of their time chazing after the wrong issues

Source: Tenable Research

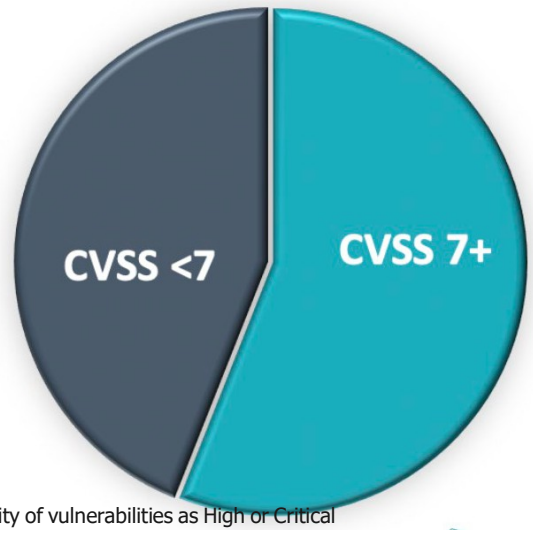

Figure 1. CVSS scores the majority of vulnerabilities as High or Critical

More importantly, CVSS is a completely ineffective method for prioritizing remediation efforts. That's because CVSS is risk-unaware. Since most CVSS scores are assigned within two weeks of vulnerability discovery, the score only employs a theoretical view of the risk a vulnerability could potentially introduce. That leads security teams to waste the majority of their time chasing after the wrong issues. Even worse, they're missing many critical vulnerabilities that pose immediate danger to the business.

CVSS is a poor indicator of actual security risk

Even if your team could tackle all the vulnerabilities that score 7 or higher, it turns out less than one-quarter (24 percent) of them currently have exploits available (see Figure 2). In other words, if you're using a CVSS 7+ strategy to prioritize remediation efforts, you're wasting 76 percent of your team's time fixing vulnerabilities that pose little to no near-term security risk.

Figure 2. Exploit availability for CVSS base scores

To make matters worse, nearly half of all vulnerabilities (44%) that have an exploit available – and therefore pose greater short-term risk – have a CVSS base score under 7 (see Figure 2). Yet, by policy based on a CVSS 7+ strategy, you'd be ignoring these high-risk vulnerabilities completely.

The attack surface is expanding

The attack surface is also expanding, creating a gap that's being exploited by attackers. In addition to traditional IT assets, the modern attack surface now requires you to consider vulnerabilities in your cloud and OT environments, as well. The problem is, while adversaries are scanning all these environments to find the easiest way in, legacy vulnerability management methods are limited to scanning traditional IT environments – so you'll never see any of the vulnerabilities residing in your cloud and OT assets.

A risk-based approach is needed

Risk-based vulnerability management helps government agencies put vulnerabilities in context. Instead of relying exclusively on CVSS, they can combine it with dozens of essential vulnerability characteristics to determine their severity. They can then correlate all this data with other key risk indicators, threat and exploit intelligence and an assessment of current and likely future attacker activity.

The result of this analysis enables agencies to focus on the vulnerabilities and assets that matter most. Instead of wasting time on vulnerabilities that have a low likelihood of being exploited, they can address the issues that pose the greatest risk to their organization.

Turning telemetry data into decisions

The amount of telemetry data and analysis required to effectively determine the level of risk each vulnerability poses to the organization can't be accomplished by human beings alone, so automation is required to scalethis process.

This automation can even include machine learning–based technologies that can predict the likelihood a vulnerability will be exploited in the nearfuture, based on past and current information about the vulnerability, the asset and attacker activity. This analysis results in a risk-based score for every one of the organization's vulnerabilities within seconds –enabling security teams to focus first on what matters most. With Predictive Prioritization, security teams can dramatically improve their remediation efficiency and effectivenessby focusing first on the 3% of vulnerabilities likely to be exploited.

With Predictive Prioritization, security teams can dramatically improve their remediation efficiency and effectivenessby focusing first on the 3% of vulnerabilities likely to be exploited.

Using data science and machine learning topredict vulnerability outcomes

Our risk based vulnerability management platform analyzed 110,000vulnerabilities to build the machine learning–based model called Predictive Prioritization, a capability which is cloud native.

Predictive Prioritization scores vulnerabilities based on theprobability they will be used in a cyberattack.

The data model takes more than 150 aspects of the vulnerability into account, including vulnerability characteristics from these sevendata sources:

- Past threat patterns
- CVSS
- U.S. NV Database
- Past hostility
- Vulnerability software
- Exploit code
- Past threat sources

Focus first on what matters most

Risk-based vulnerability management enables you to:

- Discover vulnerabilities across your entire attack surface, including cloud, OT, containers and IT assets.
- Conduct continuous in-depth assessments of the converged attack surface, rather than relying on occasional scans that are limited to a portion of your environment
- Focus on mitigating business risk, rather than measuring the number of vulnerabilities remediated or the number of assets freed from vulnerabilities
- Make the best use of your resources

Want to take the next step toward risk-based vulnerability management?

Get started with a free security workshop and trial.

Contact Us At:

Email: info@armoryze.co.uk

Tel: +44 – 0208 427 1131

Website: www.armoryze.co.uk