tenable

PREDICTIVE PRIORITIZATION: HOW TO FOCUS ON THE VULNERABILITIES THAT MATTER MOST

Contents

Executive Summary

Effective cybersecurity requires more time and resources than cybersecurity and IT teams have. To make effective use of limited resources, they need to prioritize vulnerabilities and avoid wasting time on superfluous activities.

Identifying the subset of vulnerabilities that matter most is tough when most publicly disclosed vulnerabilities have been rated High or Critical. More precise information enables better use of time, money and people. Using **Predictive Prioritization** – a process for re-prioritizing vulnerabilities based on the probability that they will be leveraged in a cyberattack – organizations can dramatically improve their remediation efficiency and effectiveness by focusing on the vulnerabilities that matter most.

As the sheer number of technology assets increases, securing them all becomes more difficult. This growing complexity creates vulnerabilities that are difficult to identify and fix because security professionals often lack fundamental visibility into all assets in the organization's attack surface. Even if they did have the visibility they need, patching all vulnerabilities with finite resources would be extremely challenging – if not impossible.

The numbers are daunting: 15,038 new vulnerabilities were published in 2017 versus 9,837 in 2016 – a 53% increase in a single year[1]. In 2018, 16,500 new vulnerabilities were published.[2] On average, enterprises find 870 vulnerabilities per day across 960 IT assets.[3] Cybersecurity and IT teams don't have the time or resources to handle all vulnerabilities, so the need to prioritize is obvious.

This white paper explains why traditional vulnerability prioritization efforts fall short and how Predictive Prioritization can help. Using Predictive Prioritization, organizations can expect a 97% reduction in the number of High and Critical vulnerabilities they need to patch or remediate. And, they can concentrate their efforts on the issues that pose the greatest risk to their organization – while improving the efficiency of scarce security personnel and budget resources.

1 Vulnerability Intelligence Report, Tenable Research, 2018

2 National Vulnerability Database (NVD)

3 Tenable Research

Cyber Risk Creates Real Business Risk

Patching all the vulnerabilities present in an organization is difficult because:

- Businesses lack the visibility they need into and across all their technology assets
- Some assets have multiple associated vulnerabilities, so the total number of vulnerabilities is too numerous to manage
- There are too few cybersecurity and IT resources available to identify and patch all vulnerabilities

The inability to patch all vulnerabilities creates exploit opportunities. According to a study by the Ponemon Institute[4], 91% of organizations have experienced at least one damaging cyberattack over the past two years. 60% have had two or more cyberattacks.

91%

of organizations experienced one cyberattack in the last two years

Why Traditional Vulnerability Management Efforts Fall Short

In a perfect world, organizations would patch all vulnerabilities. But, the number of patches required across all assets exceeds cybersecurity and IT resources including budget and human capital. More than 110,000 vulnerabilities have been published in NIST's National Vulnerability Database (NVD), some of which date as far back as 1999. However, not all those vulnerabilities have been or will be exploited. In fact, very few vulnerabilities will ever be actively exploited.

According to the NVD, 16,500 new vulnerabilities were disclosed in 2018. Yet only 7% of these vulnerabilities had a public exploit available. Even fewer were actually leveraged by attackers – meaning the vast majority of these vulnerabilities posed only a theoretical risk.

For most organizations, the difference between the vulnerabilities that could be exploited and those likely to be exploited is measured in the thousands, making it extremely difficult to prioritize which vulnerabilities to remediate first, if at all.

CVSS is not an effective prioritization metric because it:

- Lacks the granularity to provide an accurate measure of criticality based on actual vs theoretical risk
- Provides a relatively static number that does not reflect real-time activity in the threat landscape
- Scores the majority of vulnerabilities as High or Critical

4 Measuring & Managing the Cyber Risks to Business Operations, Ponemon Institute, December 2018

Important Things to Know About CVSS Scores

CVSS is an industry-standard means of assessing the severity of security vulnerabilities. The scoring system ranges from 0-10, with 10 representing the highest level of criticality.

CVSS scoring criteria changed from CVSSv2 to CVSSv3, which significantly impacted the distribution of severity ratings. According to CVSSv3 ratings, 60% of vulnerabilities are considered High or Critical compared to 31% in CVSSv2 as shown in Figure 1.

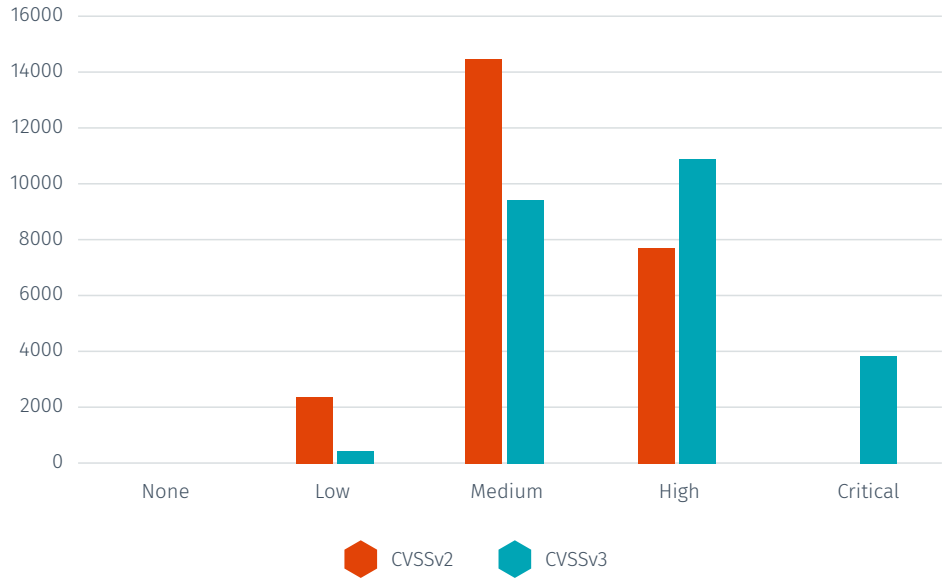


Figure 1. CVEs Overall - CVSSv2 to CVSSv3 Classification

The Attack Surface Is Expanding

An organization's attack surface is all the points where an attacker could possibly infiltrate. With digital transformation, the attack surface has expanded past traditional IT assets to include mobile devices, cloud, containers, IoT and Industrial Control Systems (ICSs). See Figure 2. Put simply, more devices result in more vulnerabilities.

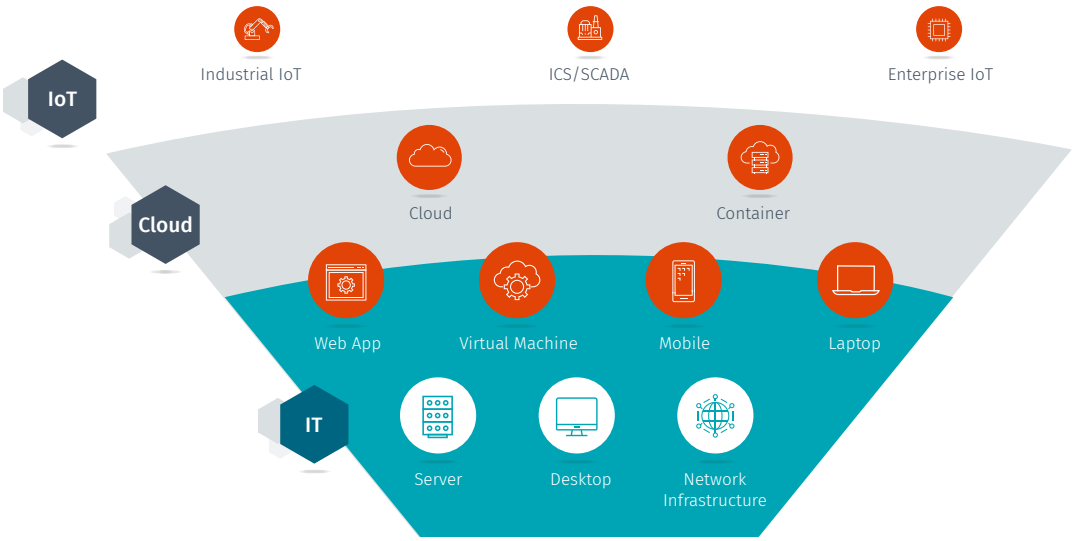


Figure 2. Digital transformation has resulted in new attack vectors

Businesses are most adept at handling the traditional vulnerabilities involving servers, desktops and network infrastructure because the tools are the most mature and familiar. Mobile security remains challenging given the device, operating system and browser diversity; infrastructure complexity; poor app security design; and end users' general lack of cyber hygiene. Cloud assets, including virtual machines and containers, tend to be ephemeral, making them hard to see. ICSs predate the Internet, so they weren't built with cybersecurity in mind. And IoT and IIoT are designed for Internet connectivity, but not necessarily cybersecurity.

A Single IT Asset May Have Multiple Vulnerabilities

Beyond that, each IT asset may have multiple vulnerabilities associated with it. For example, 5,255 CVEs are associated with the Windows 10 operating system in the NVD at the time this document was written.

Introducing Predictive Prioritization

WHERE SHOULD WE PRIORITIZE?

Predictive Prioritization addresses the critical question every organization faces: "Where should we prioritize?" This new, machine learning–enabled process re-prioritizes vulnerabilities based on the probability that they will be leveraged in an attack.

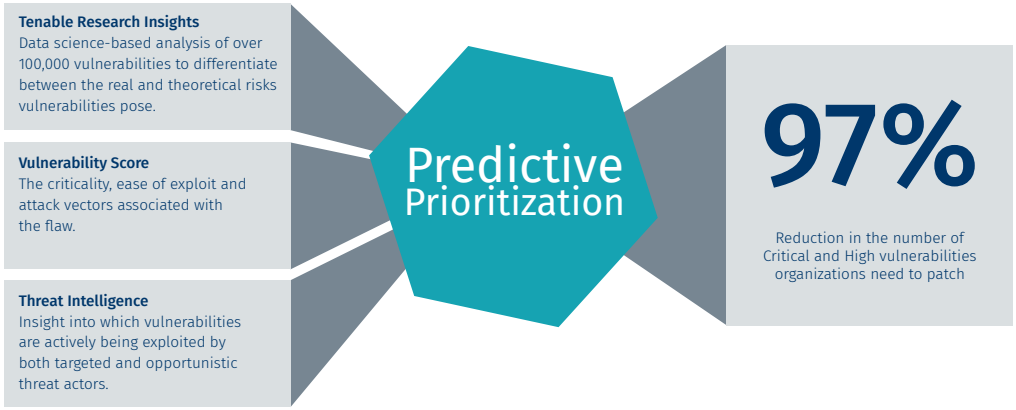


Figure 3. Predictive Prioritization provides a predictive, threat-based process for vulnerability remediation

Specifically, Predictive Prioritization combines over 150 data sources, including Tenable® vulnerability data and third-party vulnerability and threat data, leveraging a proprietary machine learning algorithm to identify the vulnerabilities with the highest likelihood of exploitability in the near-term future.

The algorithm analyzes every vulnerability in the NVD to predict the likelihood of an exploit for each. That way, cybersecurity and IT professionals can focus first on the 3% of vulnerabilities that have been – or will likely be – exploited.

Predictive Prioritization aligns with Gartner's prioritization approach as part of risk-based vulnerability management (see Figure 4).

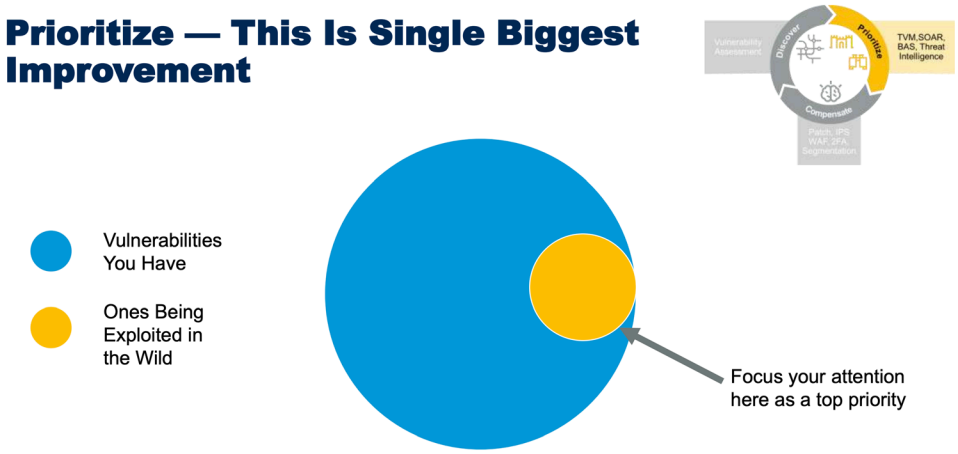


Figure 4. Prioritize — This Is The Single Biggest Improvement (Source: Gartner)[5]

5 "Gartner's Strategic Vision for Vulnerability Management," Craig Lawson; *Gartner Security & Risk Management Summit*, August 2019, Sydney, Australia

In fact, Predictive Prioritization differentiates between real and theoretical risks so well that organizations can expect to reduce the number of vulnerabilities they need to focus on by 97%. (Note: Predictive Prioritization helps you zero in on the vulnerabilities to fix first. However, that doesn't mean you should stop there. Continue working your way down the list to further reduce your organization's risk.)

How Predictive Prioritization Works

Predictive Prioritization enables organizations to focus their efforts based on the vulnerabilities that:

- Are most likely to be exploited
- Will have a major impact, if exploited

Predictive Prioritization combines data from various sources including familiar CVSS scores. Each data source is weighted based on its predictive capability. The output of Predictive Prioritization is a vulnerability priority rating (VPR), which is achieved by analyzing 150 distinct vulnerability characteristics in seven categories including:

- Past threat pattern
- Past threat source
- Vulnerability metrics
- Vulnerability metadata
- Past hostility
- Affected vendor
- Exploit availability using threat intelligence data

GARTNER RECOMMENDS:

"Start monitoring this as a key metric:

How many vulnerabilities, do you have, that are being exploited in the wild"[5]

5 "Gartner's Strategic Vision for Vulnerability Management," Craig Lawson; *Gartner Security & Risk Management Summit*, August 2019, Sydney, Australia

Predictive Prioritization assigns a VPR score to each vulnerability.

Predictive Prioritization assigns a VPR to every vulnerability and updates the score daily. The VPR represents the likelihood that a given vulnerability will be exploited in the near-term future. Like CVSS, VPR uses a point scale of 0 to 10.

In summary, Predictive Prioritization helps organizations reduce their cyber risk by helping them hone in on the issues to patch or remediate first:

- Predictive Prioritization adds sophisticated threat intelligence, so organizations can predict which vulnerabilities will be exploited in the near-term future.
- Predictive Prioritization rescores over 111,000 distinct vulnerabilities every 24 hours to constantly align VPRs with the shifting threat landscape.
- Predictive Prioritization reduces the number of the Critical and High vulnerabilities that organizations need to patch by 97%.

97%
reduction in Critical and High vulnerabilities

Conclusion

Vulnerability management has become more difficult as the number of enterprise IT assets and their associated vulnerabilities increase. Patching all vulnerabilities isn't practical given limited cybersecurity and IT resources, so organizations must prioritize their vulnerability remediation efforts to find the most dangerous needles in their haystack of vulnerabilities.

Most organizations prioritize vulnerabilities using CVSS scores. However, more than 60% of vulnerabilities are rated as Critical or High. Prioritization needs to become more precise.

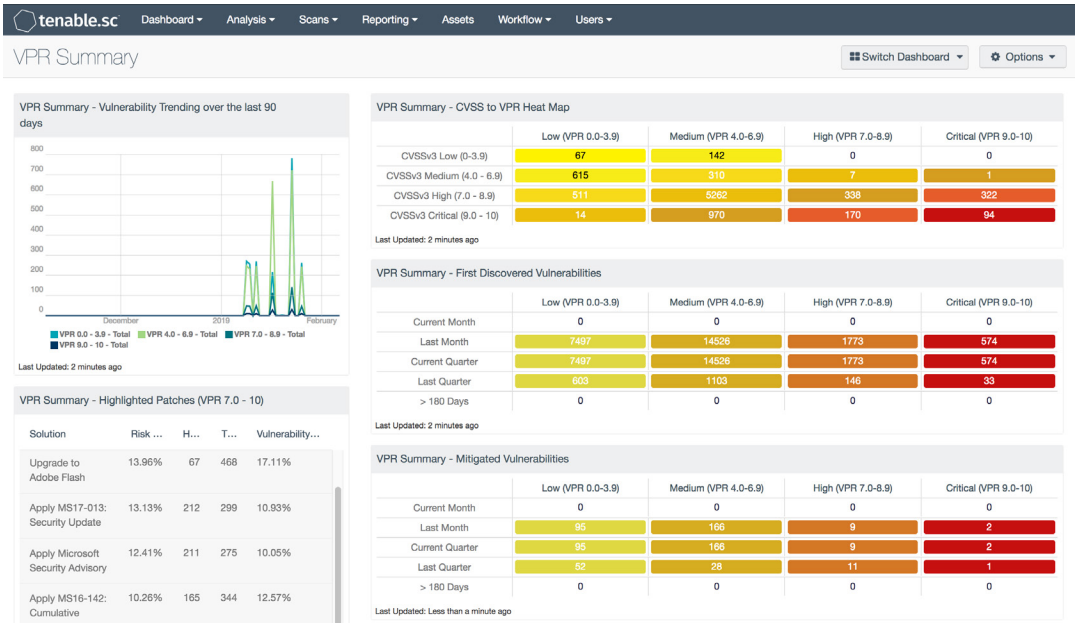
Predictive Prioritization builds on CVSS scores, adding threat intelligence and machine learning to render VPRs that are more accurate than CVSS scores alone. Using Predictive Prioritization, organizations can ensure they're focusing on the vulnerabilities that are both dangerous and likely to be exploited, making the best use of their resources and increasing the return on their risk management investments.

> **"As our organization grows organically and moves from legacy systems to cloud environments such as GCP, AWS and Microsoft Azure, our attack surface is rapidly expanding. We had a significant number of vulnerabilities. Around 250,000 vulnerabilities were detected initially, several of which were classified as being critical and exploitable due to some of the legacy applications. It is essential that my team efficiently prioritize our vulnerabilities to reduce our cyber risk, and stay one step ahead of the threats. I'm enthusiastic about Tenable's product roadmap and the efficiency that Predictive Prioritization will bring to my team's prioritization efforts."**
>
> **- Mike Koss, Head of IT Security and Risk, NBrown Group**

Predictive Prioritization is a key capability within the Cyber Exposure platform, providing security teams with actionable insights to answer the critical question: Where should we prioritize?

Predictive Prioritization is avaliable now for cloud or on-premises deployment:

- Cloud: Start free trial of Tenable.io
- On-premises: Request demo of Tenable.sc



7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

North America +1 (410) 872-0555

www.tenable.com

09/05/19 V05