A COMPARISON OF TENABLE AND RAPID7 APPROACHES TO VULNERABILITY PRIORITIZATION

Contents

Introduction

Organizations today struggle with a staggering number of vulnerabilities, and prioritizing which vulnerabilities to remediate first can be overwhelming. In this white paper, we compare Tenable's and Rapid7's methods for prioritizing vulnerabilities for remediation. With Tenable's Predictive Prioritization, security and IT teams can finally begin working smarter, not harder.

Tenable's Approach to Vulnerability Prioritization: Predictive Prioritization

Predictive Prioritization is Tenable's risk-based approach to vulnerability prioritization. This machine learning-enabled process prioritizes vulnerabilities based on the probability that they will be leveraged in an actual attack in the near future and the loss impact if they are attacked.

Predictive Prioritization starts with Tenable's Vulnerability Priority Rating (VPR), which combines over 150 different data aspects, including Tenable and third-party vulnerability and threat data, leveraging a proprietary machine learning algorithm to identify the vulnerabilities with the highest likelihood of exploitation in the near-term future (28 days). The algorithm analyzes every vulnerability in the National Vulnerability Database (plus many that have been announced by the vendor but not yet published in NVD) to predict the likelihood of an exploit being used against each. With this new insight, cybersecurity and IT professionals can focus first on the 3% of vulnerabilities that have been – or will likely be – exploited.

Traditional CVSS approach: overview and weaknesses

Traditionally, organizations have used the industry standard CVSS for measuring how easy it is to exploit a vulnerability and how damaging the exploit can be. Scores range from 0 to 10, with 10 being the most severe. CVSS is a great starting point for evaluating the potential impact of a vulnerability. Unfortunately, almost two-thirds (61%) of the vulnerabilities that enterprises find in their environments have a CVSSv2 score of “critical” or “high,” according to the Vulnerability Intelligence Report from Tenable Research. According to a recent Carnegie Mellon University’s paper on CVSS, “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.” Therefore, CVSS does not help identify the vulnerabilities requiring the most urgent attention – nor was it intended to do so.

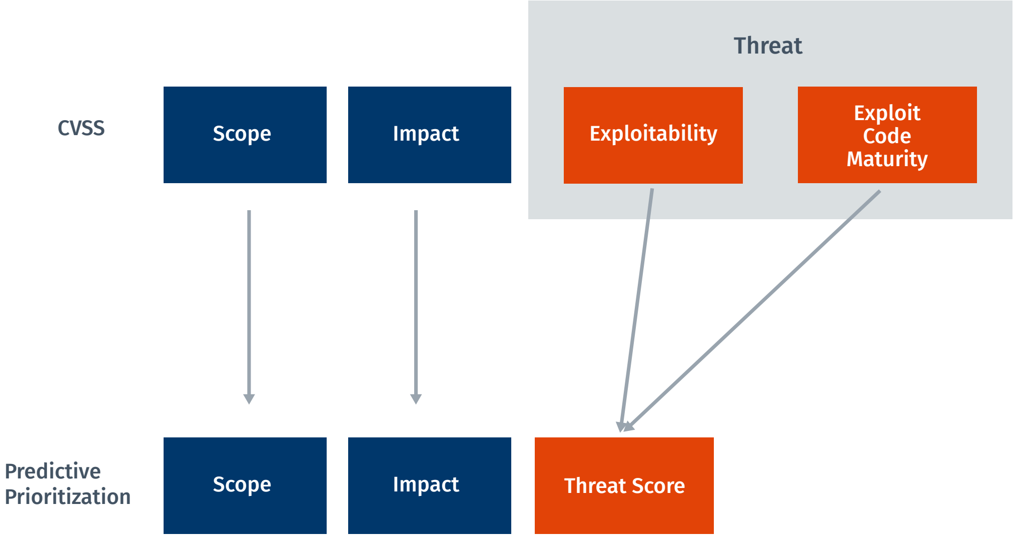
This leaves organizations with a mountain of vulnerabilities and insufficient context to prioritize them. In a healthcare context, it would be like prioritizing research on an ultra-rare but severe disease above research on slightly less severe but much more common diseases. Without understanding how widespread and actively spreading each disease is, health organizations might focus primarily on the first disease, even though others are much more likely to spread and could still be fatal. This would likely be a misallocation of resources. The same is true for cybersecurity teams who should take a risk-based approach to managing vulnerabilities within the context of their business environment.

How Predictive Prioritization works

Predictive Prioritization starts with the Vulnerability Priority Rating (VPR), which uses a point scale of 0 to 10, just like CVSS. However, VPR enables organizations to focus on the vulnerabilities that:

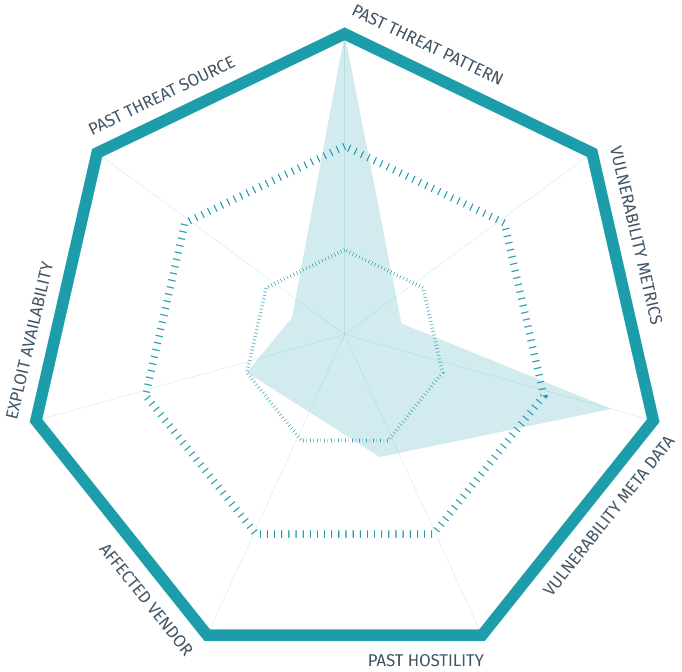
- Are most likely to be exploited
- Will have a major impact on the asset, if exploited

Predictive Prioritization combines data from various sources powered by machine learning and predictive analytics, including familiar CVSS scores. However Predictive Prioritization delivers a more relevant and timely view of vulnerability priority than CVSS, by replacing the CVSS exploitability and exploit code maturity components with a threat score produced by real-time threat intelligence and machine learning.



This threat score is powered by a diverse set of data sources, each of which is weighted based on its predictive capability. The threat model analyzes 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



Threat model development

Tenable ingests data from an ever-growing list of threat intelligence sources. An automated process analyzes all the raw data on each vulnerability – including its age, availability of exploits and exploit kits, presence in ExploitDB and Metasploit, and whether it's being actively discussed on the dark web, in forums and/or on social media, etc. Finally, multiple predictive, machine learning models work together to produce the threat score. These models use historical data to understand the relationship between the input features and the likelihood of threat activity, and thus can predict future threat activity.

With these dynamic models, vulnerabilities are scored daily, which means the score on any given day represents the real-time threat risk as the threat landscape changes. Additionally, the models build on the existing CVSS framework to produce a single score that reflects threat intelligence, exploit code maturity, and vulnerability characteristics – providing a complete view of the threat. Tenable's VPR uses the same scale as CVSS, easing migration to Predictive Prioritization and allowing the use of existing processes.

Using automated asset scoring to drive risk-based vulnerability prioritization in Lumin

In addition to rating the likelihood of each vulnerability being attacked in the near future, Tenable (available in Lumin) also provides automated asset criticality scoring that allows organizations to prioritize their remediation activities by asset value.

Tenable automatically calculates an Asset Criticality Rating (ACR) for each asset scanned, based on the rich data natively collected on each asset. The solution uses information such as asset type, running services/applications, and whether the asset is internet-facing to automatically score the value of the asset. This automated and intelligent approach is unique in the industry. Like CVSS and VPR, Asset Criticality Rating (ACR) uses a point scale of 0 to 10.

Tenable's automated asset scoring addresses the three greatest challenges most organizations face in assessing asset value:

- Lack of experience and knowledge about how to assign asset criticality scores
- Lack of time to manually score asset values in the first place
- Lack of time to continually update asset values as assets and networks change

Tenable gives users the flexibility to adjust ACR values, but doesn't put the burden on them to build an asset criticality framework from scratch, gather the necessary data inputs, or manually assign and update the asset values on thousands (or millions) of assets.

We use the combination of VPR and ACR data to calculate an Asset Exposure Score for each asset, reflecting the true cyber risk associated with that asset. We then provide a clear, prioritized list of vulnerabilities based on Asset Exposure Score that will reduce the most risk when remediated. This advanced, automated solution – analyzing vulnerability, threat, and asset data – is the only approach in the industry that delivers automated risk-based vulnerability prioritization.

Predictive Prioritization along with Lumin differentiates between real and theoretical risks so well that organizations can expect to reduce the number of vulnerabilities they need to focus on first by 97%.

Rapid7's Approach to Vulnerability Prioritization

4 scoring models: overview and limitations

In contrast to Tenable's single, clear model for risk-based prioritization, Rapid7 offers 4 different methods of scoring vulnerabilities. In general, InsightVM bases its scoring on factors like CVSS, "threat exposure", existence and ease of use of exploits, and vulnerability age. The use of 4 models leads security teams to puzzle over which one should they use in their specific environment.

Let's dive into each method to gain a better understanding of them.

> **"InsightVM's Risk Score takes in CVSS scores, malware exposure, exploit exposure and ease of use, and vulnerability age..."**
>
> **– Rapid7**

Method 1 - Real Risk

On the surface, Rapid7's "Real Risk" method sounds valuable. However, exploring further reveals that the way it scores vulnerabilities is based on CVSS base metrics (access vector, access complexity, and authentication requirements) and what Rapid7 calls "threat exposure." "Threat exposure" or "exposure" is simplistic and only a slight improvement over CVSS. The threat exposure factors include Rapid7's own data collection efforts like Metasploit data, honeypot network (Heisenberg Project), internet-wide survey (Project Sonar), threat intel from Rapid7 researchers, vulnerability age, and existence of exploits and exploit kits. This approach may produce some current data but provides limited intelligence. It relies instead on a few threat factors and on limited past static information – like the existence of exploit kits – which generally does not change over time for most vulnerabilities, and does not predict the current chance of exploitation.

Weaknesses:

- Not predictive
- "Threat exposure" factors provide only slight improvement over CVSS scoring
- Limited advanced real-time threat intelligence to prioritize and predict based on current threat activity
- Does not differentiate between real and theoretical risk
- Requires manual prioritization of assets to provide business context – no automated asset scoring
- No scoring available prior to NVD release

Method 2 - Temporal

“The Temporal risk strategy aggregates proximity-based impact of the vulnerability, using confidentiality impact, integrity impact, and availability impact in conjunction with access vector. The impact is tempered by dividing by an aggregation of the exploit difficulty metrics, which are access complexity and authentication requirement. The risk then grows over time with the vulnerability age.” – Rapid7

Similar to the “Real Risk” model, Rapid7’s Temporal model again assumes that older vulnerabilities are more likely to be exploited because attackers have known about them longer. And like the Real Risk method, it considers “exposure” and exploit difficulty, which is part of CVSS. This is another simplistic model that does not effectively predict the likelihood of a vulnerability being exploited today. While vulnerability age and exploitability can affect the likelihood of attack, these are just some of many factors that must be considered to predict the chance of attack.

The Temporal model score can also provide a very large number - above 100,000. Such large numbers are difficult to interpret (“What does the score really mean?” is a common question), and can give the impression that the VM program is performing poorly – even when it’s not.

Weaknesses:

- Not predictive
- Very little tangible difference from “Real Risk” model
- Causes more confusion by providing a very large number that lacks context
- Requires manual prioritization of assets – no automated asset scoring

Method 3 - TemporalPlus

Rapid7’s TemporalPlus adds more sophistication, but does not meaningfully improve prioritization effectiveness. It is based on the Temporal model, which again focuses on the vulnerability age, and it uses the same variables as the Temporal model. The difference is that “more granular analysis” is done on the vulnerabilities – specifically distinguishing vulnerabilities with “partial” impact values from those with “none” impact values for the same vectors.

This is only a slight improvement over the Temporal model and simply creates more confusion about which model to use. According to Rapid7, it will also cause the vulnerability scores to increase even more. Aggregate scores can reach hundreds of thousands and are difficult to interpret. (“What does this score mean? Are we doing well or poorly?” are common questions.)

Weaknesses:

- Not predictive
- Nearly identical to Temporal model, creating confusion about which model to use
- Little tangible difference from “Real Risk” model
- More granular analysis without meaningful improvement in determining which vulnerabilities to focus on first
- Requires manual prioritization of assets – no automated asset scoring

> **“TemporalPlus emphasizes the length of time that the vulnerability has been known to exist. However, it provides a more granular analysis of vulnerability impact by expanding the risk contribution of partial impact vectors.”**
>
> **– Rapid7**

Method 4 - Weighted

“The strategy is based primarily on site importance, asset data, and vulnerability types.” – Rapid7

Rapid7’s Weighted model simply takes into account a manually assigned group of assets and their vulnerabilities. It then provides a weighted score that is based primarily on the location importance (set manually), asset data (set manually), and number and types of vulnerabilities. The higher the number of vulnerabilities, the greater the score.

This sounds good in theory, but since the user has to manually enter the location importance and asset values, there is no way to utilize those capabilities at scale. This model ends up being largely a simple scoring of vulnerabilities, based primarily on CVSS.

Weaknesses:

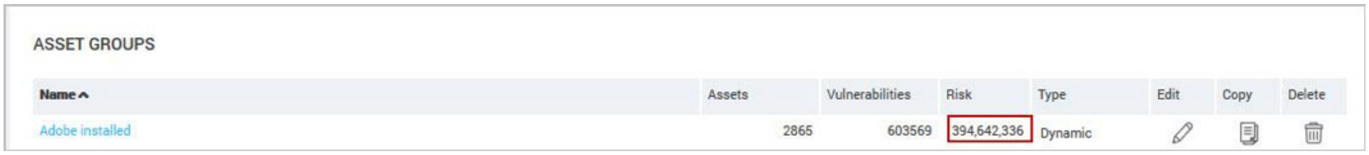
- Not predictive
- Unsophisticated approach focusing on the total number of vulnerabilities and their severity
- No threat context
- Requires manual prioritization of assets – no automated asset scoring

The use of multiple models creates confusion, not clarity

Instead of using a predictive approach that provides clear recommendations based on current threat activity and vulnerability and asset data, Rapid7 provides 4 models, which leads to confusion and questions about which model should be used and when.

According to Rapid7's own customers, the different methods of scoring vulnerabilities are mystifying. Common questions include:

- Is a score of over 100,000 for just a few assets good or bad?
- Can I report to my senior management that my risk is moderate if Rapid7 reports a "risk" score of 300 million (as shown in the example highlighted below, taken from rapid7.com)?
- Which scoring method should I choose for my organization? What are the implications of choosing one method over another?



ASSET GROUPS

Name ^	Assets	Vulnerabilities	Risk	Type	Edit	Copy	Delete
Adobe installed	2865	603569	394,642,336	Dynamic	✎	⧉	🗑

There can be value in choice, but at Tenable we believe in providing the most accurate and modern approach to predicting which vulnerabilities are likely to be attacked in the near term – instead of providing multiple legacy models.

Comparing the Tenable and Rapid7 approaches

Information overload – a chronic problem in information security – becomes even worse when too many choices are presented and guidance is lacking. This is one of the problems with Rapid7's four models. In contrast, Tenable provides a single model and a clear set of recommended solutions to reduce the most cyber exposure (cyber risk). We present it in an easy to understand way, while still providing flexibility through customization.

In addition, Rapid7's primary scoring method is based on limited "threat exposure" and historical data like CVSS scores and availability of exploits and exploit kits. This is a good start, but unlike Tenable's Predictive Prioritization, it does not actually forecast the likelihood of exploit in the near future. As an analogy, think about how you decide whether to take an umbrella to work each day. Just looking at historical climate trends might help a little, but it's not nearly as valuable as a current weather forecast based on real-time conditions and recent trends. Tenable's Predictive Prioritization uses both historical data and real-time intelligence with cutting-edge machine learning to prioritize the vulnerabilities requiring the most urgent attention today.

Asset scoring – an integral component of measuring risk and prioritizing vulnerabilities – is another area where Tenable provides greater value. Rapid7 simply leaves the task of scoring assets to the customer. You will need to develop an enterprise-wide scoring system from scratch, decide how to identify and group assets for scoring, and then manually perform the work of assigning asset scores to each asset in your environment. Then you will need to continually and manually update those asset values when assets change, appear, or get retired across your dynamic environment. It's just not feasible. Tenable's Asset Criticality Rating (ACR) automatically calculates and assigns asset values, and updates them continuously, while giving you the flexibility to adjust scores as needed.

Conclusion

In the modern era where the number of vulnerabilities has exploded, resources are scarce, and the impact of missing significant vulnerabilities can be severe, no organization can afford to focus on remediating the wrong vulnerabilities.

Most organizations still rely on CVSS for prioritization, and Rapid7's multiple scoring models are not much better. With Predictive Prioritization, Tenable is helping organizations dramatically improve their vulnerability remediation efficiency and effectiveness, using real-time threat intelligence, automated asset criticality scoring, and machine learning.

Contact us today to learn how we can help you address your specific challenges tenable®

7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

North America +1 (410) 872-0555

www.tenable.com

11/12/19 V01