SECPOD

THE EXPERT'S GUIDE TO RISK-BASED VULNERABILITY MANAGEMENT IN 2021

www.secpod.com

Vulnerability scanners gather and return loads of data from their scans and report multiple vulnerabilities in the environment. Let's say you are in the process of remediating a specific risk. Meanwhile, another open vulnerability gets exploited by a hacker before you get to it. How can you save yourself from the resentment and remorse of thinking "mitigating that vulnerability first would've prevented the attack altogether"?

With growing vulnerabilities, exploits, and ransomware attacks, your vulnerability remediation process needs to be more strategic and goal-driven towards remediating the severe risks first to prevent common attacks.

What is risk-based vulnerability management?

Vulnerability scans report many vulnerabilities at once. Not all of them carry the same amount of risk. Your assessment efforts should be focused on measuring the risk levels of each vulnerability and remediating the bigger risks first. When the severe risks are out of the way, your environment's risk posture is reduced by a great extent.

Risk-based vulnerability management is a strategic process to assess the exact risk levels of vulnerabilities, prioritize the vulnerabilities based on calculated risk levels, and remediate vulnerabilities with higher risks to reduce the probability of an exploit.

The risk levels are calculated by combining multiple factors such as threat intelligence feeds, public risk ratings of the vulnerability, assets in the enterprise, current exploit activities, and many more factors.

Why does your organization need it now?

Gartner asserts that by 2022, organizations using risk-based vulnerability management will suffer 80% fewer breaches.

Conversely, organizations utilizing CVSS (common vulnerability scoring system), CWE (common weakness enumeration), and scanner vulnerability scoring suffer from alert overload and threat fatigue.

With a risk-based approach, your vulnerability management evolves into a smarter and more efficient risk remediation process that actually strengthens security instead of just being an eyewash for compliance purposes.

Increasing vulnerabilities and data breaches

The National Vulnerability Database (NVD) recorded the highest number of publicly disclosed vulnerabilities (18,353) in 2020 alone. Records leaked in data breaches were at an all-time high in 2020 at 37,186 million, which is 140 percent higher than 2019.

The number of vulnerabilities disclosed is growing at a rapid pace every day. A higher number of vulnerabilities mean more ways for hackers to attack and lower time for security teams to protect their organizations.

Growing ties between ransomware & vulnerabilities

Ransomware attacks, for the most part, rely on vulnerabilities to penetrate the environment for the first point of contact and then move laterally between devices. The **WannaCry attack** of 2017 is one such disaster. Nowadays, a good number of moderately old vulnerabilities are closely associated with ransomware groups. Ransomware groups weaponize a set of vulnerabilities and make it publicly available. Any threat actor who wants to readily execute an attack can do so easier than before.

Increasing size of organizations

As the size of an organization increases, the number of vulnerabilities exceeds the practical bandwidth of risks that the security team can handle. You practically cannot fix every vulnerability. Instead of standing in a pool of vulnerabilities and playing whack-a-mole, the more scalable approach is to have a standardized vulnerability prioritization process.

Race against time

The speed of vulnerability detection and remediation plays an important role in preventing attacks.

According to a recent study, once an exploitable vulnerability has been found, the time to develop a fully functioning exploit is relatively fast, with a median time of 22 days.

Only when you have a standard process to measure the risk levels of vulnerabilities consistently can you prioritize and respond to the right risks at the right time.

Heterogeneity of assets

The number of devices used by an average employee is on the rise. The heterogeneity of the devices, such as the device type (desktop, laptop, mobile), operating systems, applications installed, and several other factors, is diversifying an organization's IT asset portfolio. Naturally, the volume and complexity of vulnerabilities in the environment will go up. Risk-based vulnerability management is almost the only practical way to ensure risks are at a minimum.

Terminology for classification of vulnerabilities based on risk

After risk assessment, the vulnerabilities are included in one of the four categories based on their risk levels. The purpose of classifying vulnerabilities is to prioritize them and make it easier to take action. All vulnerabilities are classified according to the terminology in the below table.

🟥	Critical	The most severe vulnerabilities which need immediate remediation. Vulnerabilities in this range might be under extreme risk of exploitation or are currently actively exploited.
🟧	High	The second most severe stage which needs careful attention. Vulnerabilities in this range have severe implications but are currently not under a serious risk of exploitation.
🟨	Medium	These vulnerabilities carry a moderate level of risk that is not highly exploitable. They can be remediated after the critical and high severity vulnerabilities are out of the way.
🟦	Low	The vulnerabilities in this range pose very low risks to the environment and can be remediated at a later point in time.

Important note:

The inclusion of a vulnerability in a particular class is temporary and is subject to change over time. As the risk levels change due to real-world scenarios, their priority levels keep changing. For example, a two-year old 'Medium' severity vulnerability may get bumped up to 'Critical' today due to its age and suddenly increasing exploit activity.

Factors to calculate and analyze the risk levels of vulnerabilities

Multiple factors contribute to the measurement, analysis, and prioritization of vulnerabilities. A combination of all risk factors is used to classify each vulnerability and categorize them based on severity. The risk levels of vulnerabilities are always dynamic.

01 CVSS score

CVSS (common vulnerability scoring system) is a scoring system and framework for rating software vulnerabilities based on their severity levels, maintained by the NVD (National Vulnerability Database). The latest version CVSSv3, has a scoring and rating system, as shown in the table below. Security researchers enter the technical details of the discovered vulnerability and arrive at a standardized score as dictated by the **NVD's CVSS score calculator**.

Note:

The severity ratings of CVSS scores are different from the overall classification of vulnerabilities discussed in the previous section.

Severity Rating	CVSSv3 Scores
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Many professionals make the mistake of using CVSS scores as the only factor for risk assessment. This is a serious flaw because CVSS scores are published at the time of vulnerability disclosure and do not account the current state of the vulnerability in the real-world after a few months or years. CVSS scores are a good starting point, but they should not be the beginning and end of your risk assessment process.

02 Type of application and business criticality

Each application and device occupy different levels of operational importance in different companies. When vulnerabilities are found in mission-critical applications and devices, admins have to take more care and precaution. They cannot afford excessive downtime and, at the same time, cannot leave the asset exposed to the risk of an exploit. Examples are web servers of e-commerce websites, database servers, etc., where downtime would have an impact on the revenue and reputation of the business.

When critical applications or devices have vulnerabilities, they should be considered critical no matter the level of severity of the vulnerabilities. Follow standard change management principles in these cases. Get the buy-in from the business users and educate them about the necessary downtime to save the systems from grave dangers in the future.

03 Exploit activity and availability

Zero-day exploits are attacks where a vulnerability was discovered and exploited before the vendor has provided a patch to fix the vulnerability. By default, zero-day vulnerabilities occupy a critical level priority. Sometimes, even a critical vulnerability may not be actively exploited. There might be other constraints like the ease of developing an exploit and other factors.

A study found that exploit development time is usually relatively short. In their data, 71 percent of the exploits were developed in a month (31 days or less), almost a third (31.44 percent) were developed in a week or less, and only 10 percent took more than 90 days to exploit.

Published proofs of concept (PoC) from security researchers or attackers worldwide make the technical work easier for other attackers since the exploit is readily available to weaponize and deploy. When the exploit is available and actively preferred by attackers, its priority level increases.

04 Impact of a potential exploit

The impact of a potential exploit is what effects or damage it can cause to the exploited device, the environment, and ultimately the business. An attacker chooses to exploit a vulnerability based on the ease of developing exploit, publicly available proofs of concept (PoC), vulnerabilities that can help with lateral movement, etc.

Technical impact of exploits may cause one or more of the following:	Business impacts due to an exploit can be:
Denial-of-service (DoS)	Loss of revenue
Remote code execution (RCE)	Damage to the reputation
Memory corruption	Theft or compromise of data
Privilege elevation	Interruption of business operations
Cross-site scripting	Damage to customer trust and business
Sensitive data disclosure	Legal consequences due to compliance violations

More daunting technical impacts are the wormable vulnerabilities, which allow any future malware exploiting them to propagate from one vulnerable computer to another without user interference. In most cases, a remote code execution vulnerability is preferred by attackers. Consider the impact a vulnerability could have in your environment and business and prioritize the serious impacts.

05 Age of the vulnerability

Contrary to what you may think, older and less severe vulnerabilities have a higher risk of causing widespread ransomware attacks than the new ones.

Of the 223 ransomware attacks that involved vulnerability exploits, 213 (96 percent) vulnerabilities were reported in the US National Vulnerability Database (NVD) before 2019.

Hackers take time to develop exploits for many vulnerabilities. When the exploit is finally developed and available, they weaponize the vulnerability and start attacking organizations.

The worst mistake is to sweep the old and low severity vulnerabilities under the rug and call it a win. At any point in time, security teams should be aware of all vulnerabilities in their environment. Any vulnerability can be weaponized and leveraged in an attack. Security teams should be aware of the current exploit activity of all vulnerabilities in their security risk profile and be ready to mitigate them when the situation demands.

06 Number of affected assets

The more assets affected with a particular vulnerability, the higher the probability of an exploit and ransomware attack. A hacker will find it easier to use the same attack mechanism a hundred times to penetrate a hundred devices than use ten different mechanisms to penetrate one device at a time.

When a particular vulnerability is found in too many devices, the vulnerability gains the Critical severity rating by default. For example, let's say a specific Medium severity vulnerability is found in a hundred assets. This vulnerability should be prioritized over a Critical vulnerability present in 10 assets.

Hitting the bullseye when choosing a risk-based vulnerability management tool

Vulnerability assessment should always be the fastest stage of your program. When the exact risk levels are determined, the decision-making process on remediation is also faster. If you are stuck assessing vulnerabilities with manual research, security teams will commit errors during the assessment and develop alert fatigue in the long run. Your attack surface will suffer the consequences.

The ideal risk-based vulnerability management tool is an all-rounder in all crucial functions. Multiple factors chip-in to make it suitable for fighting risks in today's environment. The main characteristics are:

Size of the vulnerability database

The effectiveness of a scanner lies in how many publicly disclosed vulnerabilities it can detect. If it does not have enough vulnerabilities in its database of research intelligence, you are in a dangerous situation that you don't even realize. A fewer number of security checks fail to identify all vulnerabilities and give you a false sense of security. For a scanning tool to grab all the vulnerabilities, it needs to read from a large vulnerability database with research intelligence for almost all vulnerabilities disclosed until today.

Wide asset coverage

Some scanners support only one or a few platforms like Windows or Linux. To implement vulnerability scanners for all your devices, you will be forced to configure and maintain many other open-source scanners for your heterogeneous environment. You may think you're saving costs, but you lose a lot of time and resources making upgrades and maintaining custom code. Invest in a proper scanner that covers all your core assets (desktops, laptops, servers) in all the core platforms you use.

Advanced, customizable scanning techniques

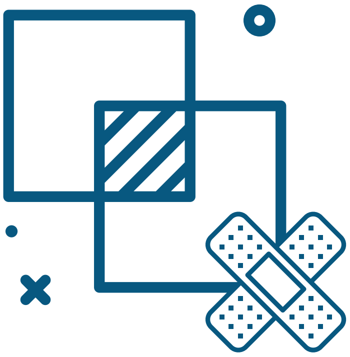
Vulnerability scans should be under your control at all times. The bandwidth should be configurable along with the scope and asset groups of the scan. Advanced scanning techniques such as continuous vulnerability scans monitor your endpoints constantly for any signs of new vulnerabilities and report them to you immediately.

Automatic, predictive prioritization

The scanner should be smart enough to prioritize vulnerabilities for you and not leave you with buttons and switches to manually mark priority levels and confuse your team even more. Automatic prioritization based on all the factors discussed previously, such as exploit activity, availability, age, leverage to ransomware, etc., should be a default feature to make a real difference in your vulnerability management.

Integrated remediation controls (patching)

The point of scanning and prioritizing vulnerabilities is to mitigate them and run operations in a safe environment. Patching is the top remediation measure to mitigate vulnerabilities. A vulnerability scanning and assessment tool should have integrated patching controls. In fact, the security industry should look at vulnerability management and patching as one integrated process. Having both in the same tool is the path to smarter and faster remediation.



Handy and practical reporting

Since vulnerability scanning and assessment are security measures, security teams need to collaborate and demonstrate their goals to top management and between themselves. They are also a compliance requirement that requires security teams to generate reports for audits. Having easy and simple reporting features go a long way to help security teams. Readily downloadable or e-mailable PDFs/CSVs and customizable report views add to the practicality of the tool.

Strengthen your defense with SanerNow Risk-based Vulnerability Management

SanerNow Vulnerability Management is a cloud-based tool that calculates the exact risk levels of every vulnerability in your environment by measuring and analyzing all the risk factors discussed in the above sections. The threat intelligence feed of SanerNow is continuously updated every day to provide its customers with the latest data and research about new and ongoing threats.

- Prioritize vulnerabilities accurately based on the exact risk levels they pose in your environment
- Automate vulnerability scans to run on specific time intervals based on rules
- Leverage our own homegrown, world's largest vulnerability intelligence feed of 100,000+ security checks to detect risks with the highest rate of accuracy
- Perform ultra-fast vulnerability scans in under 5 minutes with specially designed scanning algorithms
- Run real-time and continuous vulnerability scans to detect critical risks immediately
- Take the extra step by mitigating risks with integrated and automated patch management capabilities

Thirty days is the right amount of time to make a live and real-life evaluation of a vulnerability management tool. New vulnerabilities come and go. Your security risk profile undergoes slight changes. Schedule a demo with us. We'll give you a quick overview and a free 30-day trial with the full house of features, no restrictions.

Schedule a Demo

Contact Us

Email us on: info@secpod.com

Call us at: India - (+91) 80 4121 4020 / USA - (+1) 918 625 3023

secpod