Cymulate

Understanding Vulnerability Prioritization Technologies

From Generic VM to Contextual Impactful VPT Programs

Table of Contents

01 | Abstract 3

02 | From Vulnerability Management to Vulnerability Prioritization Technologies 4

- The number of CVEs kept increasing 4
- The emergence of agile development led to a new set of requirements 5
- The growing reliance on open-source pieces of code as a development accelerator 5
- Effect of Backlog 6
  - IT teamwork overload 6
  - Not knowing where to start 6
  - Decreased security 6

03 | What Are Vulnerability Prioritization Technologies? 7

04 | Vulnerability Prioritization Technology Options 7

- Why is there more than one type of Vulnerability Prioritization Technology? 7
- What Are the Core Constitutive Elements of Vulnerability Prioritization Technology? 8
- What Are the Vulnerability Prioritization Technology Main Types? 10
  - VPT Type 1 – Detection-Based Vulnerability Management 10
  - VPT Type 2 – Risk-Based Vulnerability Management (RBVM) 10
  - VPT Type 3 – Attack-Based Vulnerability Management (ABVM) 11

05 | Appendix A - Sources 12

01 | Abstract

One of the core issues of vulnerability management is the need to free the resources required to patch the ever-growing number of CVEs. The second one is to cause the IT team in charge of the patching to view patching as a critical mission instead of a chore that they can move down the priority list. The combination of a fast-evolving threat landscape and acceleration of deployment pushes due to agile development has resulted in unmanageable vulnerability patching backlogs that put entire organizations at risk.

Vulnerability Prioritization Technologies' main goal is to reduce the vulnerability patching workload while improving the positive patching impact on the overall security posture. They achieve that goal by sorting through the detected vulnerabilities, pinpointing those that pose the highest risk, and creating a prioritized patching list designed to minimize exposure.

Though that seems simple enough on paper, the actual sorting method directly influences the end result. To avoid inaccurate or unnecessarily broad-ranging sorting systems that cause unmanageable backlogs, the new prioritization technologies have to adapt. Their priority moves from the exclusive goal of catching all vulnerabilities to listing only those posing an actual risk. The precision of the identification of the risk extent is in direct correlation with the scope of the data input the VPT can access and process, anging from CVSS score to business risk evaluation and, most importantly, technological context.

This paper focuses on the different types of VPTs, the upstream requirements involved, and the efficacy of the end results.

02 | From Vulnerability Management to Vulnerability Prioritization Technologies

Initially, software vulnerability patching management was entirely separate from cybersecurity until the computer worm Code Red attacked Microsoft's IIS web server in July 2001. This led Microsoft to start issuing patches to plug the software vulnerabilities it spotted.

The Code Red worm opened the door to many more worms and malware, and by the end of 2010, patching management became widespread across enterprises and organizations. In parallel, NIST's original "Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme" from 2002 evolved into the first National Vulnerability Database (NVD) in 2011.
The first-ever comprehensive cybersecurity vulnerability database, NVD, integrated all publicly available US government vulnerability resources with its own CVE (Common Vulnerability & Exposure) list to include severity scores and the availability of patches.
Since 2011, managing vulnerability patching and running regular patching cycles based on the NVD became recommended cybersecurity best practices.
Yet, in the last decade, three things happened that complicated vulnerability patching management:

01

The number of CVEs kept increasing
Since the beginning of the 20th century, concerns about the need to protect infrastructures from external attacks leveraging vulnerabilities have led to the creation of a vulnerability public database. In 2002, NIST published the "Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme" which was replaced in 2011 by the first National Vulnerability Database (NVD).

Since 2017, the yearly number of vulnerabilities has jumped from mid-digit to ever higher four-digit numbers. In 2021, as the ransomware epidemic led to ransomware being declared a National Security Priority, the Cybersecurity and Infrastructure Security Agency (CISA), a branch of the US Department of Homeland Security (DHS), released Binding Operational Directive (BOD) 22-01. In parallel to this directive, CISA created a list of Known Exploited Vulnerabilities (KEV), that filters the NVD list to focus on vulnerabilities carrying a significant risk for federal enterprises.

This federal requirement to focus on a subset of vulnerabilities is a direct consequence of the acknowledgment that it is unrealistic to expect anyone, including the federal, executive branch, departments, and agencies, to patch all vulnerabilities, or even all vulnerabilities with a high CVSS score.

02

The emergence of agile development led to a new set of requirements

The advent of container technology and, in parallel, of the availability of cloud computing, has revolutionized the entire software development. Business and organizational requirements quickly onboarded the new possibilities brought on by technologies, which led to the wide-ranging adoption of agile development and CI/CD (Continuous Integration/Continuous Development) practices.

One of the defining aspects of agile development is that it implies frequent deployment. From a vulnerability management perspective, this poses new challenges. Each deployment might include vulnerabilities, and even shifting security left and scanning for vulnerabilities during development stages is insufficient to eliminate all exposures that might result from incorrectly configured Privileged Access Management (PAM) policies or other faulty security control configurations in a production environment, especially in an increasingly connected infrastructure. To further complicate vulnerability management, prioritizing vulnerability patching in such a rapidly evolving landscape requires not only keeping track of the ever-growing list of vulnerabilities but also of the rapid code obsolescence and replacement.

03

The growing reliance on open-source pieces of code as a development accelerator

As one of the critical underpinning goals of agile development is to increase speed, it is no surprise that DevOps massively rely on open-source software to accelerate development cycles.
As a result, open-source pieces of code have become ubiquitous, but the level of code review for security implications runs from stellar to non-existent. Vulnerability scanners and other security solutions increasingly included during the development stage are detecting most of the CVEs listed on NVD or MITRE, but, as demonstrated by the 2021 Log4j debacle that resulted in millions of devices being affected, they are helpless at detecting unlisted vulnerabilities.

Today, simply listing all uncovered vulnerabilities, even if listing them by order of criticality to prioritize patching according to generic risk scores, still places too heavy a load on the IT teams. The patching process can, and does, break things for any number of reasons. The main culprits for patching-related issues are unforeseen patch compatibility issues that risk disrupting operability and make part or all systems unavailable for indefinite periods. There are other issues, such as, for example, not having access to third-party systems where the vulnerabilities are located or using versions too old to receive security updates.

Effects of Backlog

Unmanageably long and ineffectively prioritized vulnerability patching lists create a series of issues:

IT teamwork overload

Each required patch needs to be treated individually and requires not only obtaining the patch but also checking how implementing it will affect other systems' functionalities. Some patches also require complete system reboots, which might interrupt business for the necessary time, adding painful debates with the board to establish priorities and schedule the patch to minimize the impact on business. Shifting left and including security during the CI/CD process is only solving part of the issue, as, whether newly discovered or included in integrated open-source or third-party services, new vulnerabilities keep being uncovered after deployment.

When the patching schedule includes dozens or even hundreds of required patches, the tendency to relegate patching to the bottom of the to-do list is significant. It often leads to postponing for a time that tends to never comes.

Not knowing where to start

Even when detected patches are correlated with the vulnerabilities CVSS scores, long lists with ineffective or no prioritization at all tend to increase the feeling of unmanageability. The mere idea of having to wade through the mass of requirements to extract those that will have an actual impact on the security posture already seems unsurmountable.

This has snowballing effects as unaddressed vulnerability patching lists tend to get longer as more requested patches are added.

Decreased security

With ineffective vulnerability patching prioritization, every unpatched vulnerability holds the potential of leading to a catastrophic breach. Lacking proper context and prioritization leads to an unorganized patching backlog, increasing the risk that it includes vulnerabilities endangering critical organization systems or crown jewels.

Yet, even if the number of new CVEs published annually has tripled since 2011, the proportion of exploited vulnerabilities is falling.

Despite the exponentially growing number of known vulnerabilities, only a fraction result in actual breaches. Even critical vulnerabilities are infrequently exploited. Focusing your remediation efforts on high-impact mitigations is the most efficient way to ensure the resources dedicated to patching vulnerabilities actually harden your security posture.

03 | What Are Vulnerability Prioritization Technologies?

Also known as VPT, Vulnerability Prioritization Technology is a term coined by Gartner in 2019 to define a new class of solutions focused on the prioritization stage of the vulnerability management lifecycle. By July 2021, VPT reached the peak of Gartner's Hype Cycle for Security operations "Inflated Expectations" curve. At the same time, external Attack Surface Management (ASM) and the combination of Autonomous Penetration Testing and Red Teaming, made their appearance at the inception of the Innovation Trigger curve.

These two emergent technologies are integrated with the most advanced VPT solution, Attack Based Vulnerability Management (ABVM).

Before getting into the different types of VPTs, both those based on legacy and emerging technologies, it is vital to better understand the elements leading to the vulnerability patching backlog that plagues the digital world today.

04 | Vulnerability Prioritization Technology Options

The goal of any vulnerability prioritization method is to emulate the Eisenhower Matrix. Also known as the Urgent-Important Matrix, the Eisenhower Matrix helps deciding on and prioritizing tasks by urgency and importance, filtering out less urgent and essential tasks that can be postponed or ignored altogether.
Each new vulnerability prioritization technology aims at fine-tuning such a matrix based on two main parameters:

- Ensuring optimal security and resilience
- Minimizing the number of vulnerabilities that require patching

There are, however, different paths to achieve that result, with varying degrees of success based on the accuracy and depth of the input data, the ability to integrate the context, and the resulting correlation options.

Why is there more than one type of Vulnerability Prioritization Technology?

At its core, vulnerability prioritization technology (VPT) consists of detecting and listing vulnerabilities present in systems and creating a list of those that should be patched in priority based on the risk they pose to the environment.
With the constant increase in the number of vulnerabilities, vulnerability assessment tools had to evolve from simply identifying and listing vulnerabilities to evaluating each vulnerability's actual risk.
The necessity to evolve was noticeably brought to attention in early March 2022 when CISA added 95 vulnerabilities to the Binding Operational Directive (BOD) 22-01, initially released in November 2021.

Aimed at reducing the significant risk of known exploited vulnerabilities, BOD 22-01 singles out particularly egregious vulnerabilities that federal agencies are required to patch within 100 days of publication. The mere fact that US federal agencies find it necessary to single out a substrate of high CVSS vulnerabilities on which to focus patching efforts clearly signals that the score is only indicative.

The first version of CVSS was released in 2005 by a research team from the US National Infrastructure Advisory Council (NIAC) as a standardized system designed to provide universally standard severity ratings of software vulnerabilities. Based on feedback from vendors, the second version was released in 2007 with a wider scope of measurement covering access vector and complexity, authentication, confidentiality, integrity, and availability metrics. By 2012, dissatisfaction stemming from the lack of metrics granularity led to modifications, released as the third version of CVSS in 2015. CVSS v3 introduced user interaction, privileges required metrics, a physical attack vector, and fine-tuned the formulas of CVSS v2.

CVSS scores, though an invaluable element to incorporate when establishing a vulnerability patching schedule, suffer from a number of limitations that, ideally, need to be compensated for by vulnerability prioritization technologies.

To name a few:

CVSS Scores Limitations

The assigned risk score is permanent

It gives no indication about the exploitability of the vulnerability

It is a generic score that does not factor in the effectiveness of already installed mitigating systems

It does not take into account the various ways a vulnerability can be leveraged by an attacker

These are all elements that need to be taken into consideration when selecting a vulnerability prioritization technology.

What Are the Core Constitutive Elements of Vulnerability Prioritization Technology?

All VPTs include two main elements:

- A detection element
- An analysis element

The differences between each VPT type and vendor rely on their capabilities for each of those two elements.
To understand whether a particular technology type or vendor's product answers your specific needs, it pays to understand which capabilities are needed and which are available in the target product. To do so, it helps to understand their capabilities and how to evaluate their potential efficacy.

VPT tools detection and analytical capabilities include all or some of the following aspects:

Asset discovery:

scouring the Internet to uncover all known and unknown, active and inactive exposed asset is critical to maintaining full visibility of all assets across a disparate network.

Scanning:

broadly speaking, here are two types of scans:

- **Non-authenticated scan:** akin to a surface level scan, it scans the unprivileged areas of the environment.
- **Authenticated scan:** performed by an authenticated user using authorized credentials of the highest level, it scans the entire environment, using the credentials to access the privileged areas.

Reporting:

at the risk of stating the obvious, they should be able to list all detected vulnerabilities. However, the type of listing capabilities is a crucial part of evaluating any VPT solution adequacy. These capabilities are listed below in a logical order where all previously listed capabilities should be included in a solution offering the last listed one:

- Listing vulnerabilities by CVE number (VPT type 1)
- Correlating each detected CVE with its corresponding location (VPT type 1)
- Prioritization according to CVSS score (VPT type 1)
- Prioritization according to business context and risks (VPT type 2)
- Prioritization according to risk in the environment context (VPT type 3 only)

The ultimate goal of VPTs is to optimize the patching effort/impact ratio. The underlying goal is to keep the patching workload to a minimum while maintaining security robustness. Every added capability can shave off two-digit percentages of the patching workload, so it pays to keep this cumulative effect in mind.
Prioritizing according to the environmental context is the latest addition to the VPT generation, but the context addition impact is the highest on the exponential curve of added prioritization capability impact.

What Are the Vulnerability Prioritization Technology Main Types?

VPT Type 1 – Detection-Based Vulnerability Management

The most basic type of VPT is vulnerability assessment (VA). Today, VA identifies vulnerabilities in a system and lists them in decreasing order of criticality based on CVSS scores. Advanced detection-based VPTs apply some correlation between those scores and baselines reflecting the organization's risk appetite and use the data to create a prioritized patching schedule.
However, detection-based vulnerability management suffers from major flaws:

- It is limited to traditional assets and blind to a large part of the attack surface
- It categorizes vulnerabilities by severity alone
- It lacks harmonization between technical metrics and business outcome metrics
- It is reactive, perpetuating the firefighting mode

VPT Type 2 – Risk-Based Vulnerability Management (RBVM)

Scanning the entire attack surface, which discovers and assesses previously uncatalogued exposed assets, rendering the vulnerability management process far more comprehensive.

Integrating the exploitability index ranging from DREAD risk assessment model types to vendor-specific scores such as Microsoft Exploitability Index or Red Hat Severity Ratings, or establishing proprietary indexes that evaluate the likelihood of a vulnerability being exploited.

- Factors considered when evaluating a vulnerability exploitability range from:
  - The known existence of one or more exploits leveraging it
  - The complexity required in coding capabilities to create an exploit
  - The potential versatility of an exploit
  - The potential exploit's stealthiness to cover its expected capabilities to remain undetected for extended periods or across escalation paths
  - The vulnerability reachability
  - Threat intelligence collected on the Darknet
  - Other

- Factors used to affect an exploitability score to the evaluated vulnerability calculate the risk based on:
  - The potential impact in terms of
    a. Potential damage extent
    b. Number of components potentially affected

- Ease of exploitation in terms of
  - Discoverability
  - Exploitability
  - Reproducibility

Reconciling technical and business priorities by continuously re-assessing exposed assets. This includes the last modifications to the environments effected by keeping with evolving business priorities and updating the vulnerability priorities to reflect those changes.

Undoubtedly, RBVM is a marked improvement on detection-based vulnerability management, but it still has some flaws:

- It only evaluates detected vulnerabilities – At its core, RBVM still relies on its capacity to reactively detect vulnerabilities. In other words, it looks for vulnerabilities from a defensive perspective that fails to integrate the attacker's views.
- It lacks the capability to evaluate the effectiveness of compensating measures such as security controls configuration.
- It lacks the capability to evaluate a vulnerability's actual risk when looking at how an attacker could leverage it to move laterally or escalate its attack.
- It lacks end-to-end visibility.

VPT Type 3 – Attack-Based Vulnerability Management (ABVM)

ABVM is the latest and most advanced vulnerability prioritization technology in existence. As opposed to the reactive detection and risk-based vulnerability management approaches, it takes a proactive approach by analyzing the results of simulated or emulated attacks. It then prioritizes the required patching criticality based on the environment's actual exposure by scoring the vulnerability not only based on CVSS scores and DREAD-type methods but also by deprioritizing vulnerabilities that are effectively compensated by the security controls in place.
ABVM includes all the analytics tools of RBVM, such as Attack Surface Management, and incorporates a variety of risk scoring methods. But instead of relying on guesstimating the actual risk posed by vulnerabilities, it correlates that risk with precise, documented exposure data.

To summarize, in addition to RBVM, ABVM:

- Proactively covers all Tactics, Techniques, and Procedures (TTPs) listed by MITRE ATT&CK and NIST 800-53 Revision 5
- Prioritizes vulnerability patching based on local context exploitability - Streamlines the required patching schedule by downgrading high CVSS vulnerability risk scores when security controls demonstrated their ability to stop or deflect attacks leveraging them
- Documents the effectiveness of existing security controls
- Provides data to rationalize and optimize defensive tools
- Data-backed prioritization through collecting specific, comprehensive, and precise exposure data

About Cymulate

05 Appendix A - Sources

Some of the sources are hyperlinked within the text and some are not as it would hamper readability. All the documents referred to below have been used as information sources to create this White Paper.

- Anton on Security - Role of Context in Threat Detection - Anton Chuvakin https://medium.com/anton-on-security/role-of-context-in-threat-detection-f7076e71f206 -Dec 2020
- Applied Sciences - Vulnerability Management Models Using a Common Vulnerability Scoring System - https://www.mdpi.com/2076-3417/11/18/8735 - Sep 2021
- Bloomberg - Apple and Meta Gave User Data to Hackers Who Used Forged Legal Requests - https://www.bloomberg.com/news/articles/2022-03-30/apple-meta-gave-user-data-to-hackers-who-forged-legal-requests?sref=xuVirdpv – Mar 2022
- CISA – Known Exploited Vulnerability Catalog - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CPO Magazine - Open Source Security Flaws Exist in 70% Of Applications, 80% Of Libraries Are Never Updated - https://www.cpomagazine.com/cyber-security/open-source-security-flaws-exist-in-70-of-applications-80-of-libraries-are-never-updated/ - June 2021
- Cyentia Information Risk Insights Study – IRIS Tsunami Following the Wake of Damages from Multi-Party Cyber Incidents - https://www.cyentia.com/wp-content/uploads/IRIS-Tsunami.pdf - 2021
- Dark Reading - The Evolution of Patch Management: How and When It Got So Complicated - https://www.darkreading.com/vulnerabilities-threats/the-evolution-of-patch-management-how-and-when-it-got-so-complicated - Jan 2022
- Dark Reading – Open Source Code: The Next Major Wave of Cyberattacks - https://www.darkreading.com/vulnerabilities-threats/open-source-code-the-next-major-wave-of-cyberattacks - Feb 2022
- Department of Homeland Security - Binding Operational Directive 22-01 - https://cyber.dhs.gov/bod/22-01/ - 2021
- Flashpoint-intel - CISA's BOD 22-01 Update: Revamping Vulnerability Management Capabilities for Federal Agencies - https://www.flashpoint-intel.com/blog/cisa-update-vulnerability-management-for-federal-agencies/ - March 2022
- Gartner - Hype Cycle for Security Operations 2021 - https://www.gartner.com/en/doc/security-operations - 2021
- Gartner - Ten Cyber and IT Risk Fundamentals You Must Get Right - https://www.gartner.com/en/conferences/hub/security-conferences/insights/cyber-risk-fundamentals - Oct 2021
- Gartner – IT Roadmap for Cybersecurity - https://emtemp.gcom.cloud/ngw/globalassets/en/information-technology/documents/insights/the-it-roadmap-for-cybersecurity-excerpt.pdf - 2021
- Infosecurity – Vulnerability Management With Applied context - https://www.infosecurity-magazine.com/next-gen-infosec/vulnerability-management-applied/ Oct 2021
- ISO - ISO/IEC 29147:2018 - Information technology — Security techniques — Vulnerability disclosure - https://www.iso.org/standard/72311.html - 2018
- ISO - ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls - https://www.iso.org/standard/75652.html - 2022
- ISO - ISO/IEC 27001:2013/COR 2:2015 - Information technology — Security techniques — Information security management systems — Requirements — Technical Corrigendum 2 - https://www.iso.org/standard/69378.html - 2015
- JupiterOne - The State of Cyber Assets Report - https://info.jupiterone.com/hubfs/J1%20Gated%20Content/Reports/JupiterOne%20State%20of%20Cyber%20Assets%20Report%20-%20SCAR%20-%202022.pdf - 2022

- Kenna Security - Gartner identifies VPT as a critical tool for your security arsenal - https://www.kennasecurity.com/blog/gartner-identifies-vpt-as-a-critical-tool-in-your-security-arsenal/ - 2022
- Kenna Security/ Cyentia Institute – Prioritization to Prediction - https://website.kennasecurity.com/wp-content/uploads/2020/12/Prioritization_to_Prediction_Volume_6___Attacker_Defender_Divide.pdf - 2020
- Microsoft - Microsoft Exploitability Index - https://www.microsoft.com/en-us/msrc/exploitability-index
- Neoticcyber - Using continuous, contextual insight to improve your vulnerability management program - https://noeticcyber.com/using-continuous-contextual-insight-to-improve-your-vulnerability-management-program/ - Sep 2021
- NIST- National Vulnerability Database - https://nvd.nist.gov/
- Ontario Government - Information Technology Standards - GO-ITS 42 Security Requirements for Enterprise Vulnerability Management - https://www.ontario.ca/page/go-its-42-security-requirements-enterprise-vulnerability-management
- OWASP – Threat Modeling - https://owasp.org/www-community/Threat_Modeling - and Threat Modeling Process - https://owasp.org/www-community/Threat_Modeling_Process