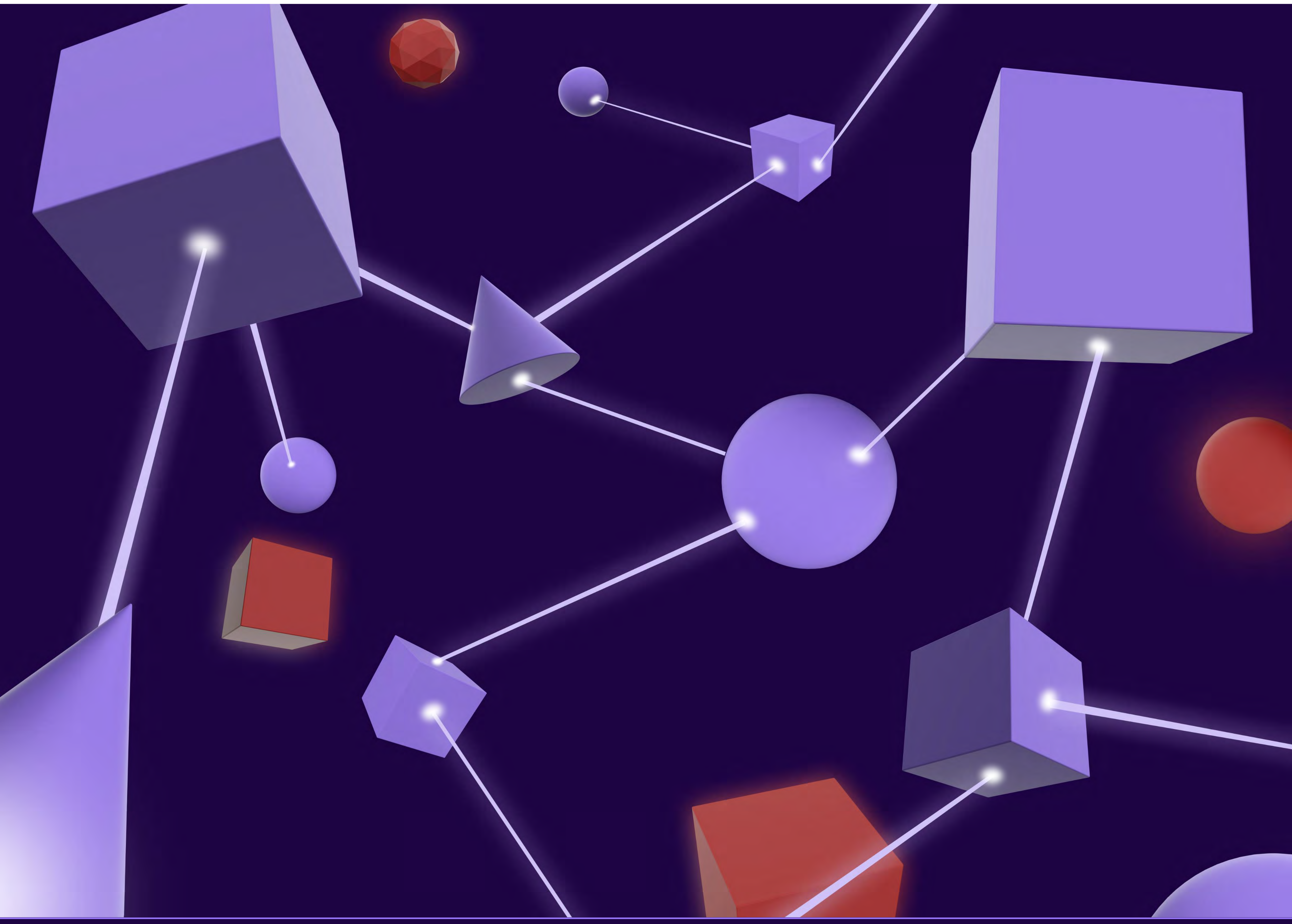
/ hackuity

Dear Security Teams:
Why Your RBVM Strategy Isn't Working



By the Hackuity Microsoft MVP Team

Vulnerability Management (VM) has been a security pillar for the past 20 years. While the foundation of VM has gone unchanged, efforts to make it more efficient and effective have been relentless. And why not?

The root issues requiring Vulnerability Management have not only endured two decades of cybersecurity innovations – they have outpaced our cyber defenses exponentially. It's time to break down what VM means today and where it's headed next.

The Traditional VM Approach...

Vulnerability Management must be comprehensive. It needs to cover every possible device on the network. Workstations run various operating systems, from Windows to Macintosh to variations of Unix, and servers must run the appropriate operating system to support the services and applications that depend on each server. Network equipment and devices such as routers, firewalls, intrusion detection appliances, printers, and more all run various operating systems, applications, services, and programs. Each of these is susceptible to vulnerabilities. And surprise: it is impossible to produce a perfectly secure device or program, so attackers take advantage to exploit those vulnerabilities that security teams are struggling to patch. Just how far behind are they?

> _Well, 80% of cyberattacks leverage a vulnerability known for the past half decade, so you tell us.

... And Where It Fails

Early on, organizations realized the overwhelming challenge of the raw number of vulnerabilities. Even smaller organizations with fewer devices, operating systems, services, programs, etc. found that it was impossible to wrestle control of every threat.

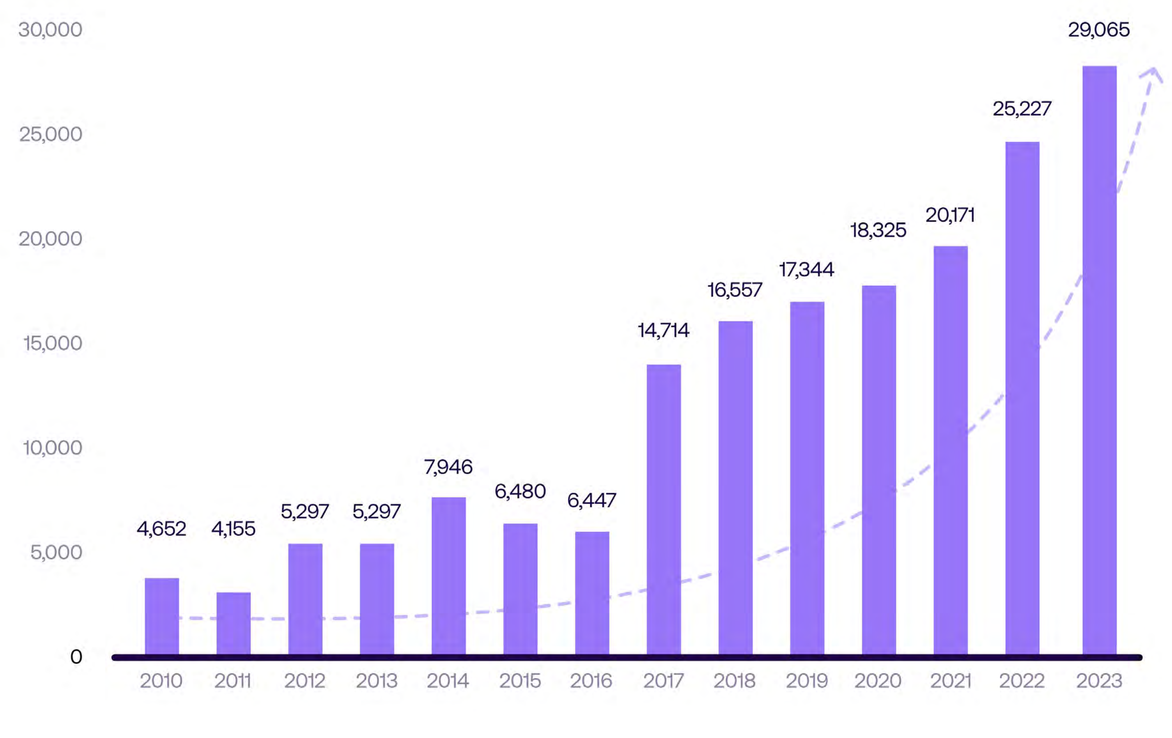


fig. 1: Hockey stick growth of Common Vulnerabilities & Exposures

To organize and develop an approach to resolving vulnerabilities, many organizations used manual tactics (i.e. spreadsheets) to attempt this analysis. As you can imagine, this was a feeble approach due to the volume of vulnerabilities, versions of software and platforms, and the constant introduction of new vulnerabilities across all platforms. The sheer number of platforms that needed to be patched, as well as the multitude of versions of each platform, proved that trying to patch every vulnerability was never going to happen. We lost that battle. So be it. More sophisticated and analytical solutions soon emerged to manage the vulnerability wave.

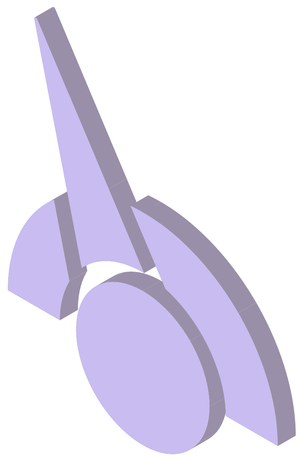
Risk-Based Vulnerability Management (RBVM)

RBVM was and remains a disruptive shift in the way we think about vulnerabilities. Maybe not every vulnerability needed rapid patching – or any patching – after all. With so many devices and platforms in even a medium-sized organization, there needed to be some alternative to deciding which vulnerabilities required immediate remediation and which vulnerabilities could be postponed or even ignored.

The *risk-based* approach to Vulnerability Management gave organizations breathing room to address the most important vulnerabilities, usually based on CVSS scoring, EPSS scoring, and other important criteria. As a refresher:

CVSS SCORE

The common vulnerability scoring system was introduced by NIST as a framework to communicate the characteristics and severity of software vulnerabilities.



EPSS SCORE

The exploit prediction scoring system is based on data that can estimate the probability that a software vulnerability will be exploited in the wild.

Where RBVM Comes Up Short

Although RBVM is a major step toward solving the volume and remediation issues that traditional Vulnerability Management failed to, RBVM has its own limitations that have proven to restrict effective patching and risk reduction.

RBVM does give an organization a prioritized list of vulnerabilities that need to be patched, but for most organizations the task of trying to patch the prioritized list remains overwhelming. To put it another way, they're facing the same, better organized vulnerability wave.

Many RBVM solutions have attempted to add more and more analytical measurements to their risk scoring, but they haven't significantly cut down the real threats to an actionable amount. Sec teams are left sweeping up the avalanche one snowflake at a time.

Moving Beyond “Another RBVM Solution”

Vulnerability Management is still essential. But just as 2024’s definition of AI carries vastly different expectations versus 2014’s interpretation of the same technology, the future of VM demands progress. It is a business imperative to implement solutions that will truly secure the enterprise, and that begins with enabling unprecedented efficiency for all security teams (CERT, CSIRT, SOC, etc.).

A centralized Vulnerability Management solution is essential to delivering those teams the full visibility and controls they require to secure an organization’s entire attack surface. These solutions include all the benefits of RBVM, but also automatic vulnerability scoring, threat intelligence, and improved remediation tactics and techniques – each tailored to the org’s own context. In effect, they bolster the bandwidth of security and operations teams far beyond their headcount would suggest.

Organizations that have a splintered Vulnerability Management approach find that juggling more than one VM platform is too confusing and complex, which knocks them back into the same state as when they had traditional or basic RBVM solutions in place. Too many tools can pose as much of a challenge to security as too many vulnerabilities. Remediating an entire enterprise-worth of vulnerabilities without advanced and centralized platforms is an inhuman task.

Why In-depth Cyber Exposure?

Patching vulnerabilities isn’t a question (only the “how” is). It’s also clear that solutions to date have been unable to overcome the complexity and volume of vulnerabilities that need to be patched. Moving to an advanced, centralized RBVM solution is a proven approach to finally resolve the vulnerabilities that lead to breach. Additional benefits of this approach include:

+ Automated remediation – manually attempting to install the myriad of patches is not reasonable. With connectors to all platforms and an automation engine, most patches can be automatically deployed.

+ Less time on VM – by considering advanced vulnerability scoring, including threat intelligence, and improving remediation techniques, Vulnerability Management costs will be reduced, as will time needed to remediate vulnerabilities. Not bad in a resource-strapped economic environment.

+ Fewer vulnerabilities – the inclusion of advanced vulnerability metrics, such as actual risk level, business context of assets, and exploitation scoring, gives a new look into which vulnerabilities need to be addressed immediately, over a generic priority list of all vulnerabilities.

Tying It All Together

Vulnerability Management is a key pillar that every organization must prioritize (pun intended). However, advances in attacks are forcing organizations to be more diligent and expansive on how they approach vulnerabilities and other areas of exploitation. Traditional VM and even most Risk-Based Vulnerability Management solutions do not go far enough in giving organizations the insights to efficiently and rapidly resolve essential issues throughout the network.

Moving to an advanced and centralized RBVM platform is a proven solution that can improve the organization's overall security risk, while also saving bandwidth and budget on vulnerability remediation tasks.

The end result?

> _A fully enabled Vulnerability Operations Center (VOC) that can finally shoulder the security burden alongside your SOC.

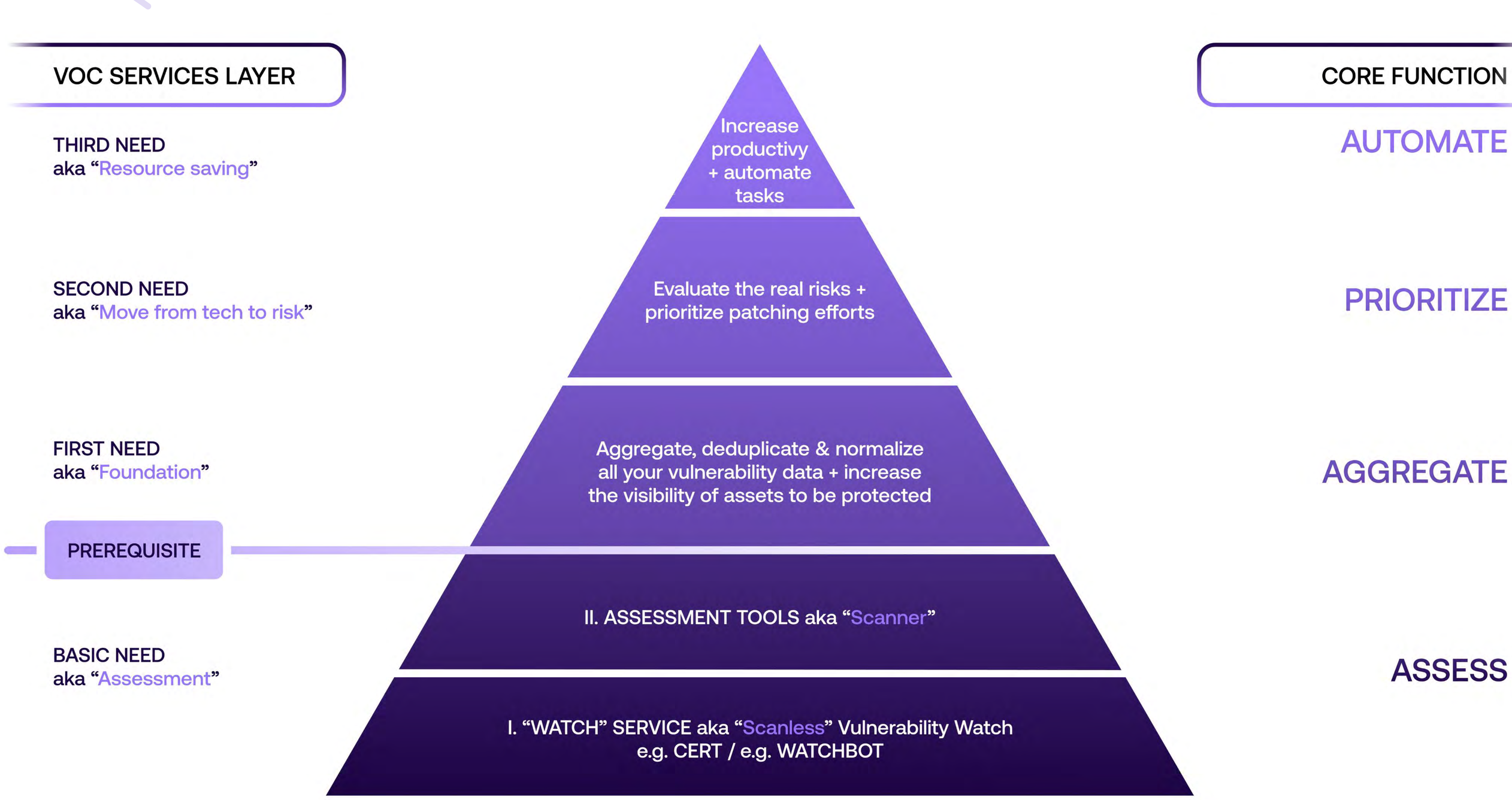


fig. 2: The different stages of th VOC pyramide