tenable

HOW SECURITY LEADERS

WIN SUPPORT FOR RISK-BASED VULNERABILITY MANAGEMENT

Faced with an onslaught of vulnerabilities, security leaders recognize that a new approach is needed. Now, you just need to convince the rest of your organization.

An expanding attack surface demands new security objectives

Even the most well-resourced teams can't keep up with the thousands of new security flaws popping up each month. From cloud to mobile to IoT, the modern attack surface is expanding at a rapid clip, and legacy methods of vulnerability management are no longer cutting it.

Defending your attack surface requires effective prioritization. That means assessing the business risk behind each vulnerability and focusing your resources on the few that pose actual threats. Time and again, security leaders who embrace a risk-based approach to VM succeed in reducing their cyber exposure, while saving time and money in the process.

But, convincing the rest of your organization that "less is more" requires a paradigm shift from traditional objectives based on volume—of vulns remediated, or systems patched—to goals that reflect the impact of your team's efforts.

"Simply reordering security initiatives... according to the risk-based approach increased projected risk reduction **7.5 times above the original program at no added cost**."

– McKinsey on Risk[1]

[1] McKinsey & Company, "*McKinsey on Risk: Number 8*," November 2019

"By 2022, organizations that use the risk-based vulnerability management method will suffer 80% fewer breaches."

– Gartner[2]

Assessing your current security posture reveals quick wins

Before pitching your risk-based strategy, you'll first want to develop a thorough understanding of your security program's current maturity level. This can be an uncomfortable exercise, but it's important to ask yourself the hard questions about where your team is today and what gaps need to be addressed.

Remember that what's commonplace to you may not be for others – even within your own organization. Many high-ranking security leaders still hold a legacy view of vulnerability management, believing that antivirus software negates the need for vulnerability assessments, or that monthly scans are sufficient to defend against emerging threats.

A risk-based approach to VM cannot be achieved through siloed efforts or a single software deployment. It requires multiple tools, technologies and processes working in concert to continually assess and mitigate the threats that matter most (see Figure 1).

The Path Towards VM Maturity

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
NON-EXISTENT	**SCANNING**	**ASSESSMENT & COMPLIANCE**	**ANALYSIS & PRIORITIZATION**	**ATTACK MANAGEMENT**	**BUSINESS-RISK MANAGEMENT**
No Vulnerability Scanning	Vulnerability Assessment Solution in place	Driven by Regulatory Framework	Risk-focused	Attacker and Threat focused	Threat and risk aligned with business goals
Manual Vulnerability assessments	Ad-hoc Vulnerability Scanning	Scheduled Vulnerability Scanning	Scan Data Prioritized through analytics	Multiple threat-vectors scanned & prioritized	All threat-vectors scanned & prioritized
Haphazard Patching	Rudimentary Patching	Scan to Patch Lifecycle	Patching data-driven by priority	Patching based on risk to critical assets	Continuous patching
No Processes Exist	Basic Processes	Emerging Processes	Measurable Processes	Efficient, metrics-based processes	Unified business and IT Processes
No Metrics	Basic Metrics	Little Measurability busy metrics	Emerging Metrics and Trends	Threat-driven metrics and trends	Measurement integrated to enterprise risk management
Blissful Ignorance Phase		**Awareness & Early Maturity Phase**		**Business Risk & Context**	

Figure 1. Vulnerability management maturity model developed by Core Security.[3]

[2] Gartner, "*A Guide to Choosing a Vulnerability Assessment Solution*," April 2019

[3] Core Security, "*Growing Up: A Roadmap to Vulnerability Management Maturity*," 2015

Mapping your program against a VM maturity model will help determine what near-term benefits you should bring to the table, and ensure that your risk-based VM program is built on a solid foundation as you climb the maturity ladder.

If that prospect sounds intimidating, know that you're not alone. In a recent Tenable webinar, over 100 security professionals were polled about the current state of their VM program (as illustrated in Figure 2). The vast majority ranked themselves in the range of Level 1 to Level 3, revealing a broad movement towards risk-based prioritization with much ground still to cover.

Figure 2. Results of April 2020 webinar poll on VM maturity.[4]

Adapting your message is key to gaining support beyond IT

While C-suite leadership may control the purse strings, the implementation of a successful risk-based VM program requires support from teams throughout the organization, from developers and accountants to engineers and systems administrators. It's important to recognize that your basic security message won't necessarily resonate with each of these stakeholders, especially non-technical colleagues.

[4] Tenable. "*Security Maturity Self-Assessment Poll*." Informal online survey of 107 security professionals to determine vulnerability management maturity. Conducted during an April 29, 2020 webinar.

Every Audience Has Different Needs: Sample Benefits to Emphasize

Security Engineers	Fewer tools and automation deliver operational efficiencies
System Admins	Shortlist of prioritized vulns that pose actual risk
Developers	Early detection of potential code vulnerabilities
CISO	Contextual metrics that show clear risk reduction
CFO	Tangible overall risk reduction without significant overhead costs
CIO	Increased efficiency reduces operational workload

Before offering your solution, take the time to ask each team about their view on risk and listen for the challenges that keep them up at night. You can even break the ice by admitting to the stigma around InfoSec as the "bad guys" who tell everyone what not to do. The more open and honest your conversation, the more likely it is you'll find common ground to weave into your risk-based story, allowing you to highlight the benefits that matter most to each particular audience.

By gaining broad support for your program, you can pave the way for approval from your CISO, who must ultimately sponsor and sell the program upstream. Since a risk-based approach requires new ways of measuring success, your CISO will need these department-specific challenges and benefits to address potential questions from the board, explain how better metrics can help every team work more effectively, and ultimately highlight how the risk-based VM method will reduce the organization's exposure to cyberattacks.

Measuring with context adds value to your vulnerability story

The next step in changing the conversation around VM is changing what you measure. For years, security operations (SecOps) have typically measured success based on the number of vulnerabilities assessed or systems patched. This philosophy continues to shape the management objectives for many security programs, which are evaluated on the volume of vulnerabilities remediated. Prioritizing the work using static scoring methodologies such as Common Vulnerability Scoring System (CVSS) scores has not only made the work completely unmanageable, but it also doesn't adequately reflect real-world risk and context for vulnerabilities.

As the attack surface expands, and new vulnerabilities are added to the existing workload that was already too large to be addressed, this approach no longer makes sense – it's an ever-growing problem. Instead, you'll want to position your remediation efforts within context that matters to other teams and the broader organization. This includes factors like time, risk and financial impact.

For example, you can highlight the amount of exploit risk that was reduced within a given quarter, or the average time to detect and mitigate vulnerabilities affecting key business assets. These metrics more accurately represent the progress and value of your team's efforts, and they'll begin to change the way your leadership thinks about cyber risk.

Methods for Measuring Your Security Team's Effectiveness

Legacy VM	Risk-Based VM
Total # of vulns in the environment	Length of time vulns are present
Number of patches deployed	Mean time to remediate
Total # of "high" and "critical" CVSS severity vulns identified	Average time to detect new vulns
	Average age of vulns detected
	Average risk score (including asset criticality)
	% of critical assets hardened from exploitable vulns
	Risk benchmarks compared to similar organizations

A new approach is the only way to combat emerging threats

Agility is key to running a successful cybersecurity operation. Ad-hoc scanning and manual analyses are no match for today's dynamic threat landscape. Once you've gained buy-in from various teams and outlined a maturity plan, you can use concrete data points to convey the urgency of acting now rather than later.

Simply put, legacy VM leaves your organization exposed to critical threats it can't afford to miss:

Few organizations have visibility across their entire attack surface, including just 10% of respondents surveyed in a recent Tenable webinar poll.[5] This leaves dangerous exposure gaps in modern assets such as web apps, DevOps and IoT devices where attackers are most likely to exploit weak security links.

Exploitable vulnerabilities currently fly under the radar. Despite their higher risk, exploitable vulnerabilities are as persistent in enterprise environments as vulnerabilities with no available exploit,[6] revealing the shortcomings of CVSS-based remediation in assessing and reducing risk.

Policy-based prioritization ignores critical threats. Organizations that remediate based on policy, addressing only vulnerabilities with a "high" or "critical" (or 7+) CVSS score, are ignoring a large portion of the actual threats facing their organization. Roughly half (44%) of common vulnerabilities with an available exploit have a CVSS base score of less than 7.0. These known vulnerabilities are exactly the kinds of low-hanging fruit by which cybercriminals prefer to launch their attacks.

[5] Tenable. "*VM Practices Poll*." Informal online survey of 78 security professionals to determine vulnerability management maturity. Conducted during a January 22, 2020 webinar.

[6] Tenable Research, "*Persistent Vulnerabilities: Their Causes and the Path Forward*," June 2020

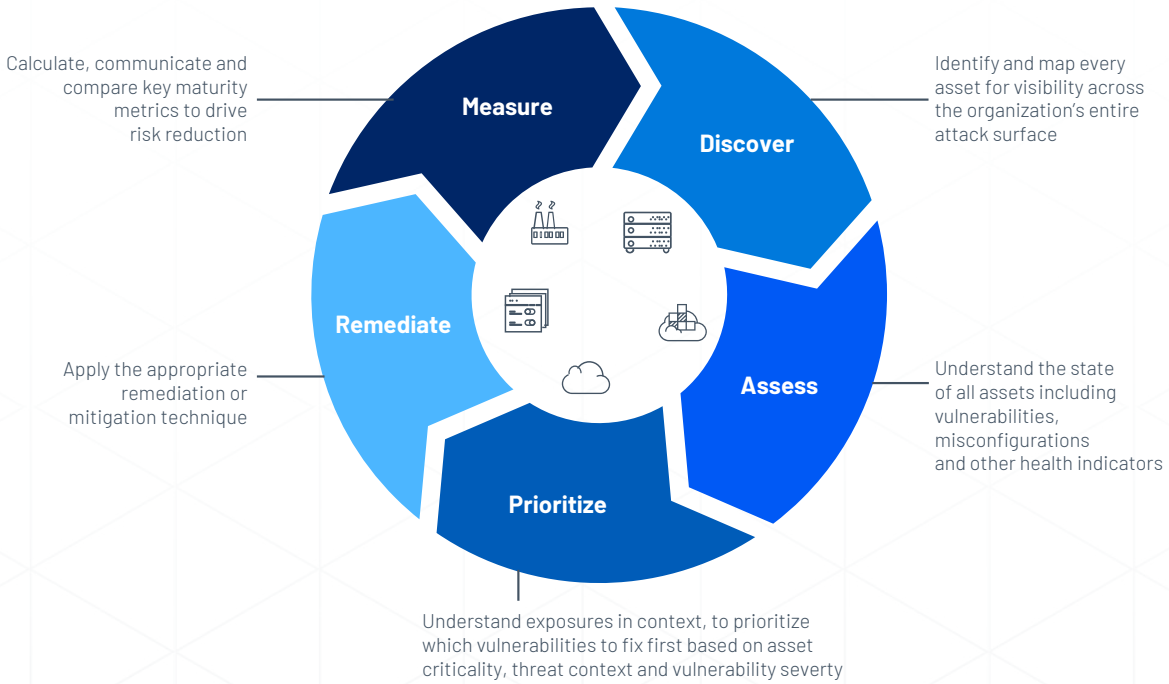
If your security process has been in place for several years, it's only a matter of time before its defenses will break down amid these emerging cyberthreats. The sooner you act, and win support for a risk-based approach, the better your chances of avoiding an unforced and possibly catastrophic error.

Putting your risk-based VM strategy into action

Evolving to a risk-based VM strategy doesn't happen overnight. But once you've forged the necessary trust and confidence between teams, it's important to make progress as soon as possible.

A true risk-based VM program includes a broad range of tactics, and choosing the right technology partners is key to equipping your team with the tools for success. To defend your attack surface, you'll want to make sure your risk-based security stack is capable of supporting every stage of the RBVM lifecycle:

Lifecycle for Risk-Based Vulnerability Management



To learn more about concrete steps you can take to execute your risk-based VM vision, check out our eBook on How to Implement Risk-Based Vulnerability Management.

7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

North America +1 (410) 872-0555

www.tenable.com

092120 V1