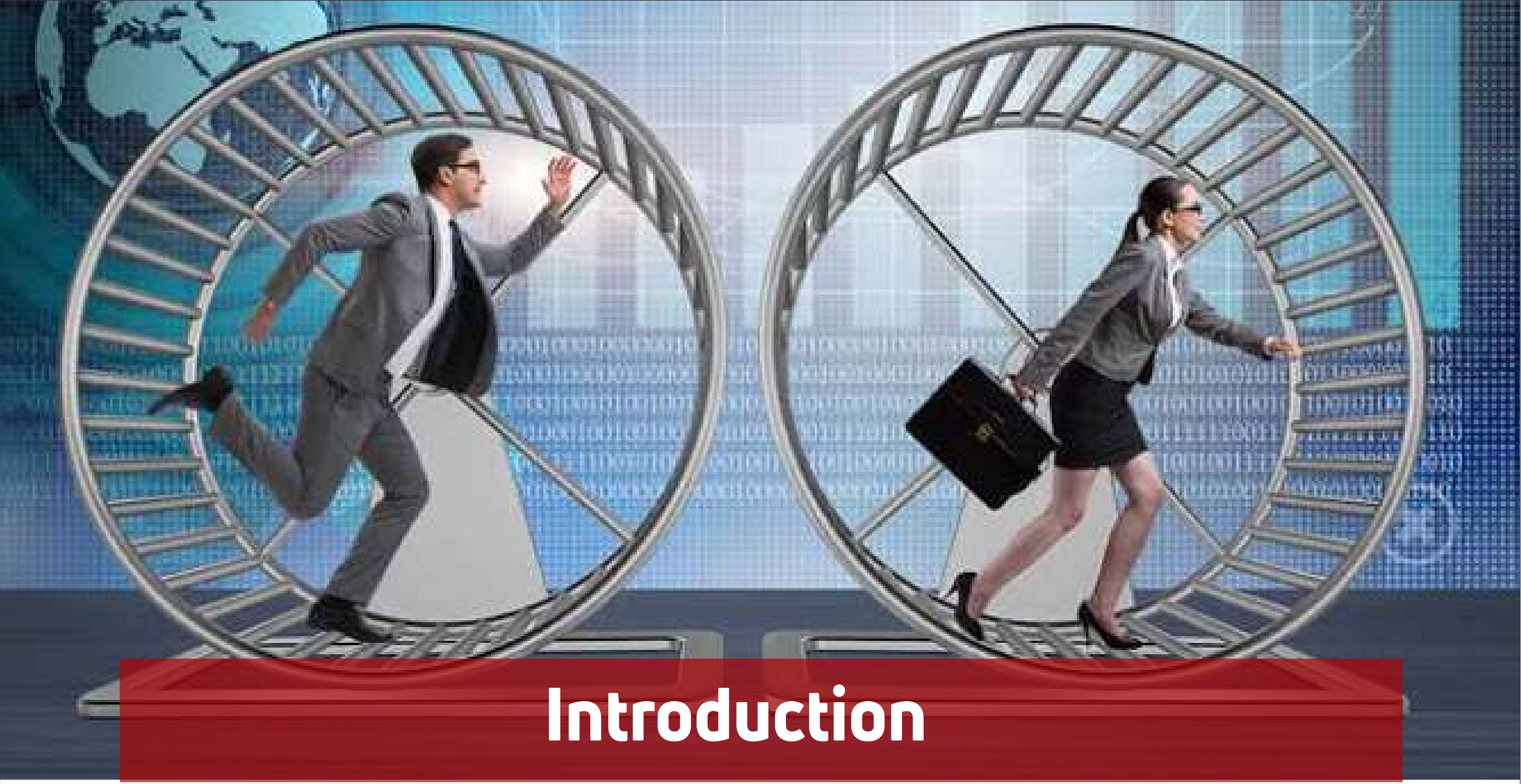
SIGNAL ALLIANCE CONSULTING

THE REMEDIATION RAT RACE: WHY YOU NEED RISK-BASED VULNERABILITY MANAGEMENT (RBVM)



Introduction

The task of protecting technology infrastructure from cyber threats remains most daunting and challenging for most businesses. Cybercrime went up 600% due to COVID-19 pandemic, Google has registered **2,145,013 phishing sites** as of Jan 17, 2021 and malware increased by 358% in 2020. One key element of achieving enterprise security is vulnerability management (VM). Through vulnerability management, cybersecurity and IT teams race to patch vulnerabilities discovered in their systems and applications, in order to prevent an exploit (vulnerabilities are simply weaknesses in a computer system which can be exploited during a cyber-attack).

Typically, the process flows like this- the cybersecurity team scans for vulnerabilities using a vulnerability scanning (VM) tool, the tool generates a report with vulnerabilities numbering between hundreds to thousands. The VM tool also indicates a severity level for each vulnerability based on the Common Vulnerability Scoring System(CVSS) , a standardized score which captures the principal characteristics of a vulnerability. The security team then exports these thousands of vulnerabilities to a giant excel sheet and begins engaging IT teams to remediate them, prioritizing the 'most severe'. On the surface, this traditional VM process seems straightforward and effective, except it isn't.

This whitepaper points out weaknesses in traditional approach to vulnerability management predominant in many of today's enterprises. The paper then introduces the industry-leading concept of risk-based vulnerability management (RBVM), an orderly, systematic, and data-driven approach to vulnerability management, outlines its superior value to enterprises and provides actionable steps needed to achieve RBVM.

> “One key element of achieving enterprise security is vulnerability management (VM)”

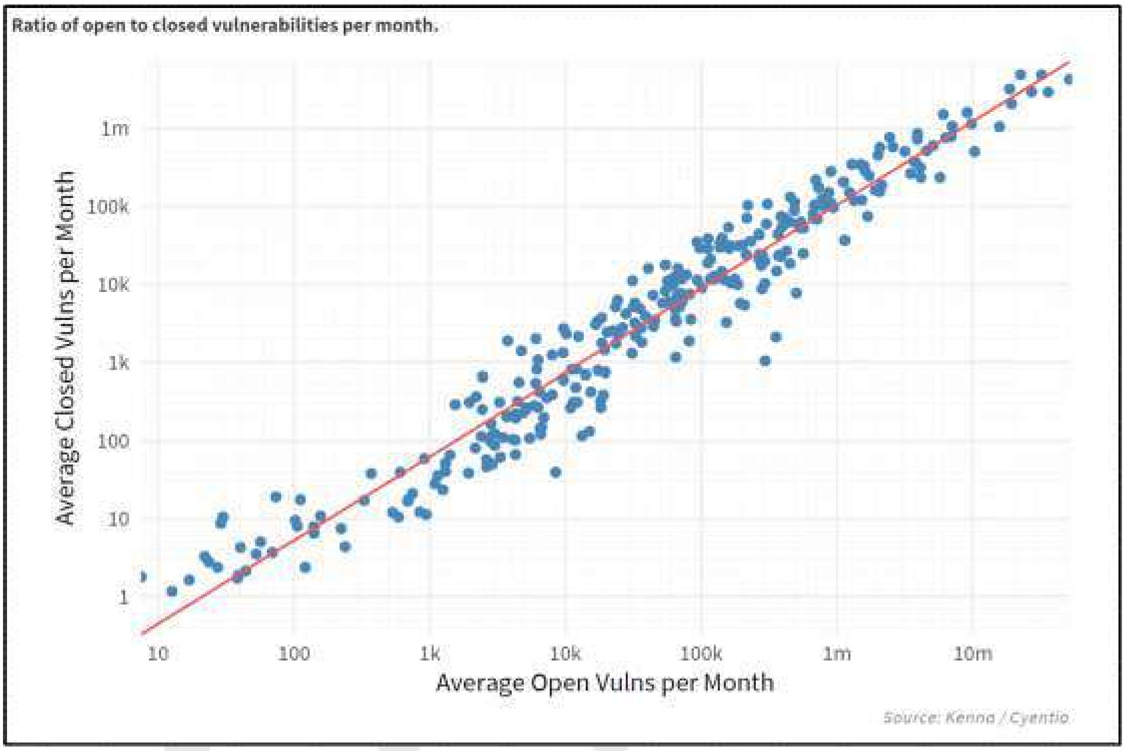
Photo credit: Unsplash

Traditional Vulnerability Management: A Futile Rat Race

We all know what the metaphorical rat race connotes, an endless, self-defeating, or pointless pursuit. The phrase equates humans to rats attempting to earn a reward such as cheese, in vain. Most organizations facing millions of vulnerabilities, erroneously believe that any one of them could be the entry point for a cyberattack. One word underlines the traditional vulnerability management approach, chaos. It is a revolving cycle that yields little benefits for 3 reasons.

1. You Can't Remediate Everything

Traditional VM tries to remediate everything (prioritizing using CVSS). But this is just not possible. You just can't remediate everything, so the entire venture is an attempt in futility. According to Cisco Kenna Security, the average enterprise has 39 million vulnerabilities and can only address about 1 out of every 10 vulnerabilities.



Source: Kenna / Cyentio

Photo credit: Unsplash

The reason for this is not far-fetched, because today's technology and cybersecurity teams are heavily overworked and understaffed. In fact, nearly two-thirds (62%) of cybersecurity teams are understaffed. The idea of an understaffed Security team emailing spreadsheets with thousands of vulnerabilities to an overworked tech team seems very inefficient. Throw in other stakeholders such as business owners worried that their servers might experience downtime due to the patching, or product managers asking for more security on their product, the outcome from this engagement is often series of haggling, email back and forth and ultimately, minimal risk reduction achieved.

> "The average enterprise has 39 million vulnerabilities and can only address about 1 out of every 10 vulnerabilities."

2. CVSS Score is not Enough

CVSS alone is no longer sufficient to rank which vulnerabilities are severe or needs priority. In fact, the CVSS was never intended to be an all-in-all enterprise risk calculator. It is a static score and lacks context, that is, the score is derived without considering how prevalent the vulnerability

Photo credit: Freepik

is in real network environments, how many systems globally have been exploited already, the importance of the asset it affects or any other environmental context.

To reiterate, many vulnerabilities with high CVSS scores pose little or no risk of exploitation. One research by Cyentia Institute that only 5 percent of enterprise vulnerabilities have known exploitation events. Hence, patching a vulnerability that is not likely to be exploited represents a waste of scarce resources.

> “CVSS alone is no longer sufficient to rank which vulnerabilities are severe or needs priority”

Photo credit: Unsplash

3. Very Manual and Lacks Automation

In 2021, The National Institute of Standards and Technology (NIST) reported that up 18,378 new vulnerabilities were reported that year. In 2020, 18,351 were reported and in 2022 already, 12,317 new vulnerabilities have been reported. The sheer volume of vulnerabilities to 'chase' is massive and the process used in chasing them is very manual- running periodic VM scans, exporting and emailing excel sheets, following up with IT over emails and meetings. This manual process guarantees that no meaningful dent can be made in remediating important vulnerabilities and reducing the enterprise risk.

> “5 percent of enterprise vulnerabilities have known exploitation events.”

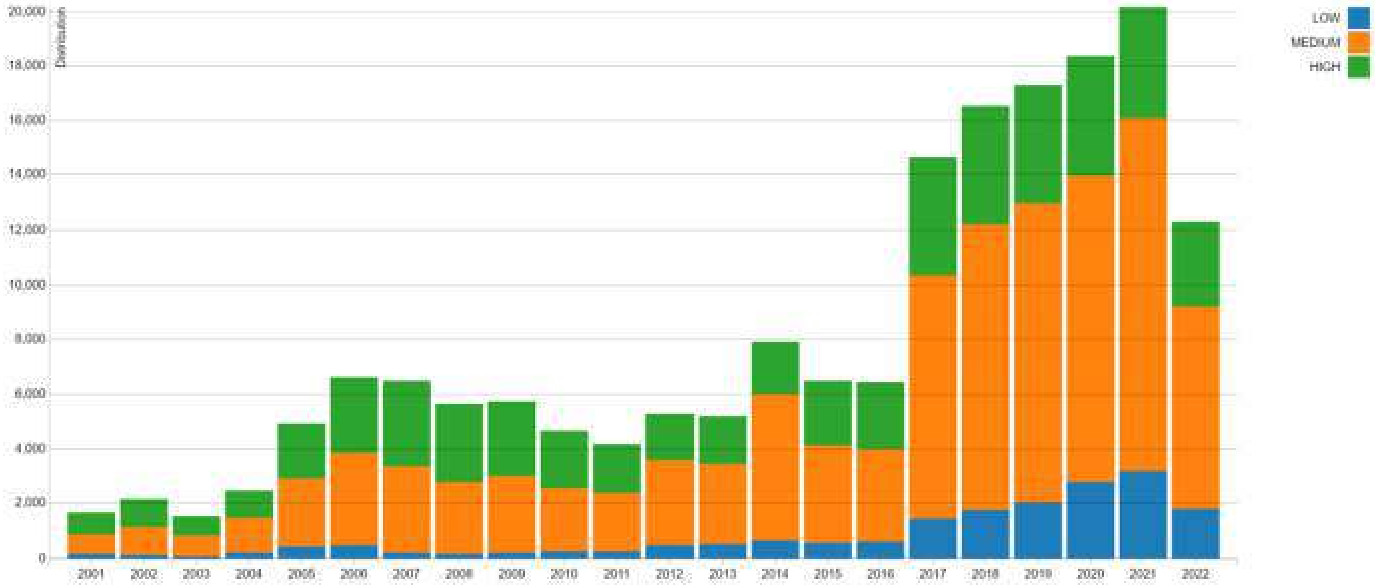


Fig. 2. Total number of vulnerabilities reported since 2001- NIST

Photo credit: Unsplash

A Better Way: Risk-based Vulnerability Management

To achieve comprehensive cybersecurity in today's hyperconnected world, an enterprise needs to get the full picture of risk from multiple feeds, tools and contexts, adequately rank vulnerabilities based on this consolidated view, and then prioritize remediation accordingly. All this is achieved via risk-based vulnerability management. Unlike traditional VM which is based on a tunnel vision of risk, RBVM considers multiple sources of data- threat intelligence, exploitability, attacker activity and internal asset criticality.

Key components of a risk-based vulnerability management approach include:

1. Integrated Threat Intelligence

Why limit yourself to the CVSS score when there are many more factors to consider in evaluating a vulnerability? By integrating threat intelligence into the VM decision-making, organizations give themselves a better chance at identifying what matters most.

By threat intelligence, we mean making use of data like, which vulnerabilities are being actively exploited, where are all the vulnerabilities from all your tools, on what assets do these vulnerabilities exist and what controls already exists on those assets.

This approach shifts the strategy away from trying to fix everything and instead, focusing on remediating the vulnerabilities which are most likely to cause a breach.

Photo credit: Unsplash

2. Comprehensive Risk Score

Traditional vulnerability management erroneously views the CVSS score as the risk score of a vulnerability, hence the severity. But we now know that this could not be further from the truth. In contrast, RBVM combines the CVSS with integrated threat intelligence, and other contextual data to provide a comprehensive risk score for each vulnerability. What is produced is an indication of risk that is based on contextual data like asset criticality, severity of risk, probability of attack, impact to the business and other important factors.

With better risk scoring, an organization can prioritize its remediation efforts on the 'truly critical' vulnerabilities, eliminate the friction between IT and Security teams and achieve a common objective—reducing risk.

3. Automation

The fact is, no vulnerability management program can be effectively driven by excel sheets. However, it is also not possible for humans to manually analyze and evaluate millions of intelligence sources to arrive at sound risk conclusions. Therefore, effective risk-based vulnerability management uses Artificial intelligence (AI) and machine learning (ML) to ingest these various threat and exploit intelligence feeds including scanners, penetration testing results, bug bounty programs, and databases of vulnerabilities, study and understand the volume of attacker activity regarding a vulnerability in the wild and then provide the context required to determine which vulnerabilities to remediate first.

> “However, it is also not possible for humans to manually analyze and evaluate millions of Intelligence sources to arrive at sound risk conclusions.”

In practice, RBVM is achieved using technology solutions. These modern vulnerability management solutions operationalize all the components stated above. They will take all internal security data, analyze it along with billions of pieces of external data, and then tell which vulnerabilities pose the most risk. With robust risk evaluation and remediation intelligence, organizations get the information they need to make truly data-driven remediation decisions.

Photo credit: Freepik

Conclusion

Enterprises must adopt a better approach to vulnerability management. This approach must make efficient use of lean IT and Security staff, and tackle the vulnerabilities that matter most, on the assets that matter most. This approach must also increase collaboration between all stakeholders involved, working towards the same goal which is to reduce technology enterprise risk. To be clear, a risk-based vulnerability strategy will leave some vulnerabilities unpatched, however it allows organizations to do so with confidence, knowing that these weaknesses pose an acceptably low level of risk to the overall security of the company. For enterprises that aim to advance their threat and vulnerability management strategy, RBVM is a no-brainer.

To find out more about RBVM and how we can help you remediate high-risk vulnerabilities with 94% accuracy, contact us or send an email to marketing@saconsulting.ai

Photo credit: Unsplash