SECPOD

The Challenges of Traditional Vulnerability Management

& How to Solve Them

www.secpod.com

INTRODUCTION

It's the weekly scrum meeting at The_Teckies, and John, the CISO, and his two senior sysadmins are discussing a new vulnerability assessment solution. The sysadmins are happy they were getting a new piece of tech that can, hopefully, lessen their burden. But something was amiss. The CISO wasn't pleased.

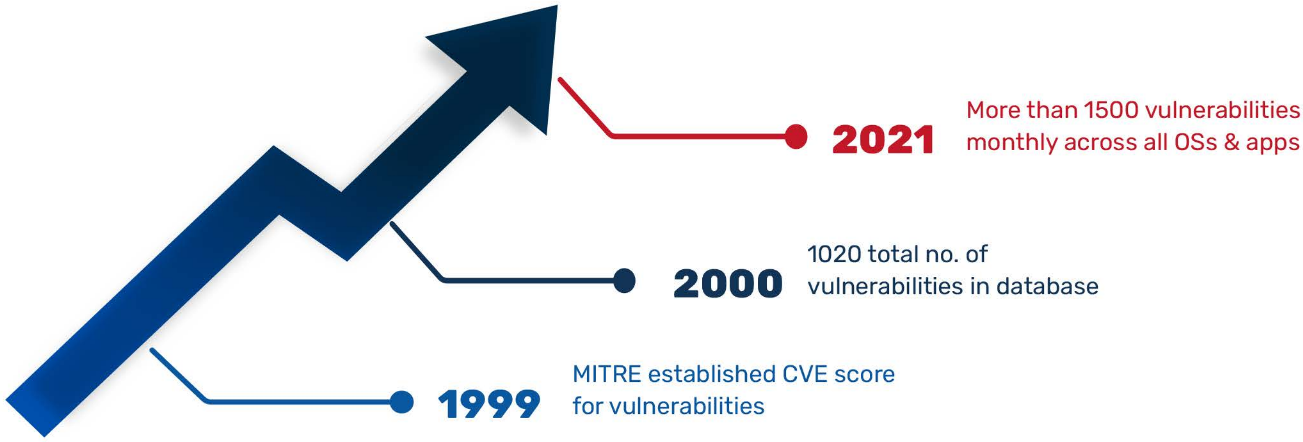
Sarah, the senior sysadmin, discussed the upcoming security audit for NIST 800-171 compliance, which was a priority. She was also updating the status of the network on patching the log4j vulnerability in their systems. Tom, the enthusiastic among the group, was excited about the new tool. It promised comprehensive and quick scans, which would make a part of his work a lot easier.

But the CISO was skeptical. He had seen the vulnerability assessment product before. It is what he had been buying for the past 20 years, just in a new package every single time from a new company. It was solving a part of his problem, no doubt, but not entirely. And unfortunately, he didn't have many options to choose from.

EVOLUTION OF VULNERABILITY MANAGEMENT (OR VULNERABILITY ASSESSMENT ?)

In 1999 MITRE established the CVE score for vulnerabilities, and 1020 was the total number of vulnerabilities in its database in the year 2000. Not much has changed since then, except for the quantity and the severity of vulnerabilities. On average more than 1500 vulnerabilities were discovered MONTHLY across all OSs and apps by security researchers in 2021 alone !

Vulnerability management in the 2000s was completely manual. Scans were lengthy and manual, and the vulnerabilities discovered had to be checked to ensure no false positives existed. IT admins had to manually patch the discovered vulnerability and verify if it was remediated by scanning again. This procedure gradually became impractical as the number of devices and vulnerabilities increased. The system needed a desperate change, and it also created an opportunity.


2021
More than 1500 vulnerabilities monthly across all OSs & apps
2000
1020 total no. of vulnerabilities in database
1999
MITRE established CVE score for vulnerabilities

THE EVOLUTION LEADING TO CHAOS IN THE VULNERABILITY MANAGEMENT SPACE

Vulnerability management broke into TWO major parts, vulnerability assessment and remediation. Well-established players in the scanning/assessment space wanted to strengthen their hold on the same. As for the remediation space, patch management solutions that were fulfilling the IT need slowly transformed into a security need as well. And the rat race began. Industry leaders and vendors were solving the problem at hand, not the problem at large. Assessment and remediation vendors were helping sysadmins do a part of their job, but vulnerability management as a whole was the problem at large that no one was thinking about.

Newer assessment and patching tools were faster, more efficient, and better than their previous iteration. But the tools weren't integrated, automated, or comprehensive. The newer tools did the same job, but better and nothing more.

The vendors were running the wrong race while John's (the CISO in our story) problem remained unsolved...

A Veteran’s Perspective on the Chaos

Ever since the Cybersecurity/Infosec market started formulating as a proper function, hundreds of vendors have been in the vulnerability assessment & remediation space. Yet the security effectiveness and attack surface reduction have been chaotic and a far-away goal for IT security teams.

Operating in siloes has been a major pitfall for these conventional solutions. Most organizations are left to invest in 5-6 different tools to implement end-to-end vulnerability management yet stay unsatisfied with the outcome.

THE OWNERSHIP DILEMMA OF WHO OWNS SECURITY

John, & every other CISO in the world, also had another problem. The ownership dilemma.

With the number of vulnerabilities rising, assessing and prioritizing them became necessary. And with the creation of security teams to design and implement security systems, they also took up the task of assessment and prioritization. The IT teams, already maintaining the devices, were tasked with applying patches for remediation.

So, who is responsible for vulnerability management ? IT or security teams ?

Vulnerability management broke into assessment and remediation. While the vendors in both spaces were improving their products, the bigger problem of the CISOs (or preventing cyberattacks using a single solution) remained unsolved.

The friction between IT and Security teams on the ownership confusion started off with the dilemma the vendors faced.

If assessment vendors owned vulnerability detection and patching vendors owned remediation, who owns vulnerability management as a whole?

WHAT IS THE PROBLEM WITH TRADITIONAL VULNERABILITY MANAGEMENT?

PROBLEM 01

Herky-Jerky Vulnerability Management Process with Siloed Solutions:

Traditional vulnerability management with siloed solutions was and still is a herky-jerky process. Different tools for different steps lead to a break in the vulnerability management cycle. And juggling between 3-5 products to finish a round of vulnerability management becomes ridiculously

The sysadmins and the CISOs have to manually correlate the results of the vulnerability scans with respective patches while eliminating false positives, which becomes progressively difficult as the number of vulnerabilities increases. They had to learn how to use multiple products; a new solution had to be learned if a vendor changed.

PROBLEM 02

Lack of REAL Visibility into IT Infrastructure:

Traditional vulnerability management provides only superficial visibility into an IT network. A list of IT and software assets isn't enough to effectively combat modern cyberattacks, especially modern ones. You can't take any meaningful measures or actions with just basic insights.

Dangerous deviations and outliers in your IT infrastructure, like poorly configured Wi-fi settings, unapproved and unnecessary apps, bypassed user access control, and other risk exposures, go under the radar and can be disastrous. Holistic and comprehensive visibility into the IT environment is sorely missed.

PROBLEM 03

No Clarity or Quantification of Attack Surface:

Organizations and their IT security teams often don't know where they stand in terms of their attack surface or cyber hygiene in general. Without any clarity or quantification of the attack surface and how effective the remediation efforts are, IT security teams are clueless on how to fine-tune and improve the process.

Additionally, without a single measure of the attack surface, quantifying and communicating the changes in it becomes difficult. Risk communication between stakeholders is another significant issue that comes up without a hygiene/risk score.

PROBLEM 04
Risk Beyond Software Vulnerabilities:

Traditional Vulnerability Assessment tools have a few limitations that severely affect an organization's ability to establish a proper prevention posture. They only scan for software vulnerabilities, limiting the security risk landscape's scope. What about other security risks like IT asset exposures, misconfigurations, deviation in security controls, and security The risk beyond software vulnerabilities isn't considered.

PROBLEM 05
Manual Correlation and the Lack of Product Integration:

Multiple solutions from multiple vendors meant there was (and still is) no product integration to eliminate the manual correlation process between scanning and remediation.

Detected vulnerabilities had to be matched with respective patches and were a time-consuming process. Furthermore, integrating two different platforms would take too much time and is not worth the effort. And if the vendor changes or goes out of business, all the efforts go to waste.

PROBLEM 06
Lack of Automation in Traditional Vulnerability Management:

Vulnerability management is a repetitive process that must be performed regularly. But with lengthy scans and manual remediation, organizations perform it once a month, leaving it at risk without automation. With automation, repeating the scanning, manual correlation, and remediation can become a smooth, single, and streamlined process.

SO, ARE VENDORS SOLVING THE PROBLEMS THAT CISOs & IT SECURITY TEAMS FACE ?

Unfortunately, no!

Twenty years ago, John manually mapped a vulnerability to its respective patch after a lengthy vulnerability scan. False positives had to be manually checked, patch availability verified, patch applied, and scans conducted again to confirm the vulnerability was patched.

Twenty years ago, the CISOs' and IT Security Teams' problems were a lack of automation of repetitive tasks, no single integrated solution that completely managed vulnerabilities from scanning to remediation, and lesser false positives.

The CISOs and the sysadmins' problems remain the same.

Vendors run the wrong race of trying to impress sysadmins and CISOs with flashy features while not solving the daily problems they face.
The present traditional vulnerability management solutions need a desperate overhaul — a REINVENTION to solve the real challenges faced by CISOs and the sysadmins.

REINVENTING VULNERABILITY MANAGEMENT WITH ADVANCED VULNERABILITY MANAGEMENT

Advanced Vulnerability Management (AVM) is the process of going beyond traditional vulnerability management with a broader approach to vulnerabilities by covering various other security risks.
It integrates vulnerability detection, assessment, and remediation into a unified, continuous, and automated process while increasing the scope of detection of various other security risks, such as misconfigurations, IT asset exposures, security control deviations, and security posture anomalies.

With increased scope in detection, AVM incorporates the remediation of the detected risks with relevant security measures along with other preventive measures to improve an organization's security posture even further.

AVM automates the vulnerability management process and prevents cyberattacks by aligning the organization with compliance policies and reducing the attack surface.

SO, HOW DOES ADVANCED VULNERABILITY MANAGEMENT SOLVE THE ORGANIZATION'S PROBLEMS ?

AVM is what vulnerability management should have been. We talked about the problems John faced 20 years ago and now. But how does AVM solve the CISO's & IT Security Team's problems?

SOLUTION 01

Providing Real Visibility into IT Infrastructure:

A list of IT assets isn't enough, and AVM's holistic visibility of your IT allows IT admins to detect posture anomalies and deviations and fix them. And only real visibility into all of your IT assets will ensure you don't miss out on devices with critical security risks.

Additionally, advanced vulnerability managementit also provides actionable insights into your IT, allowing you to declutter and eliminate unnecessary assets helping you reduce attack surface while saving costs.

SOLUTION 02

Unifying Siloed Solutions into One Complete Platform:

Working with 3-5 products is difficult, and Advanced Vulnerability Management, with its single integrated solution, becomes the answer. Using multiple products curtails the functioning of IT security teams, and the lack of a single solution causes confusion. Further, jumping through multiple hoops and dashboards to perform vulnerability management reduces efficacy and efficiency.

And as an added advantage, the IT security teams don't have to evaluate multiple products for each step of vulnerability management and don't have to quarrel with themselves about their individual roles.

SOLUTION 03

Quantifying Attack Surface with a Risk Score:

A standard measure of attack surface is a built-in feature of Advanced Vulnerability Management. It simplifies and solves the multiple challenges of a IT Security team and allows for smooth exchange of information between different teams.

Further, a single score accurately helps understand the security posture of an organization and allows teams to measure the impact of your mitigation efforts. Based on the collected data and changes in the score, teams can improve and fine-tune their remediation strategies and make the entire vulnerability management process smoother, faster and more efficient.

SOLUTION 04

Mitigating the Risks beyond Software Vulnerabilities:

Traditional vulnerability assessment tools typically scan for software vulnerabilities. But cyberattacks can happen from anywhere, and other risks like misconfigurations and security anomalies are becoming focal points of attacks in recent times. With AVM, other vulnerabilities are included in a large umbrella of defense to prevent cyberattacks.

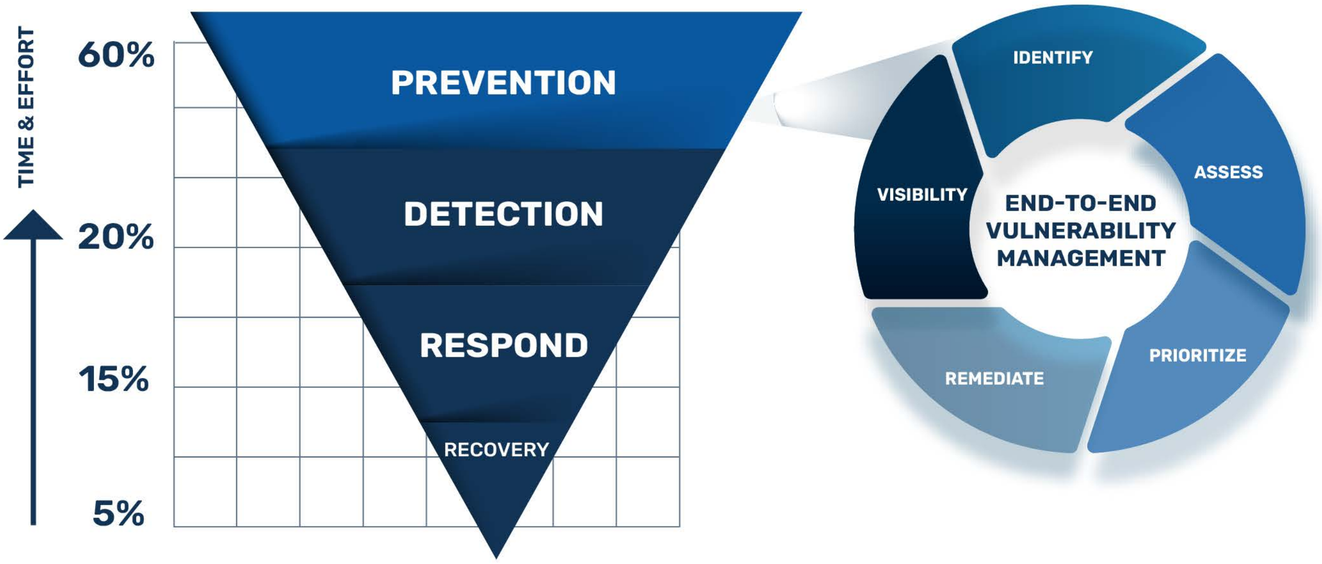
Other security risks like asset exposures and more are also the leading cause of cyberattacks, and effectively detecting and mitigating them can only be performed with advanced vulnerability management.

SOLUTION 05

Prevention over Reaction with Attack Surface Management:

By virtue of mitigating risks beyond software vulnerabilities and reducing attack surface, AVM ensures prevention is key over response. Taking action after cyberattacks occur usually leads to a significant loss in capital, reputation, and data. But with prevention in the foreground, the pitfalls of responding to attacks will become non-existent.

As the old adage goes, 'Prevention is better than cure'. So instead of reacting to a cyberattack and fixing the issue after it has occurred, prevention allows you to stop the attack before it occurs and before it is too late.



SOLUTION 06

Harnessing the Power of Automation:

Vulnerability management is a lengthy step-by-step process with repetitive tasks that might be mundane but necessary. Long ago, manually doing it might've worked, but in the modern digital age, AVM provides a much-needed helping hand by automating the entire vulnerability management process. As a result, newly detected vulnerabilities will not go under the radar.

Automation also helps you effectively use your resources and focus on mitigating risks that matter. Further, it also makes the entire process smoother, allowing you to fine-tune and improve it as you go.

CONCLUSION

With traditional vulnerability management reaching a breaking point in the cybersecurity world due to the lack of innovation in the marketplace, a dire need for its 'REINVENTION' was called for. Adapting to advanced vulnerability management is the only way forward for CISOs and sysadmins to relieve their pain points and for organizations to keep up with attackers.

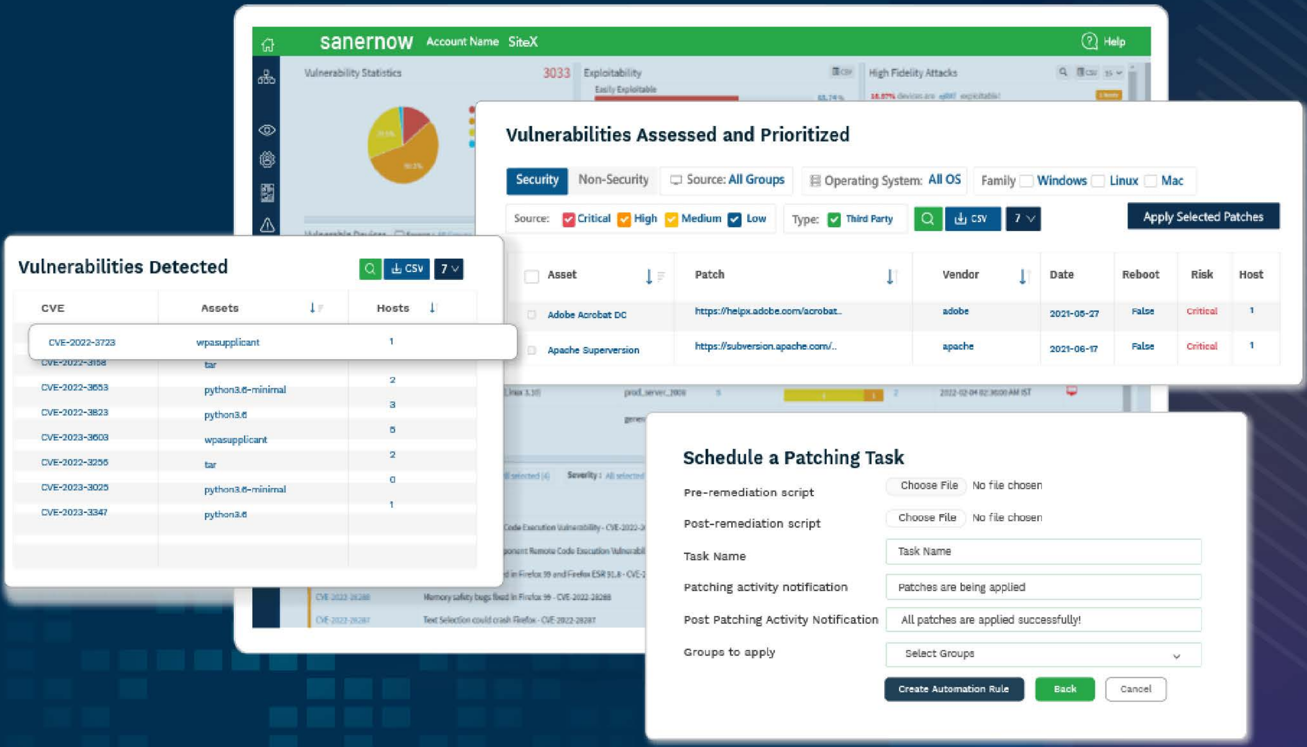
With the prevention of cyberattacks from attack surface reduction being the anchor on which the entire process sits, advanced vulnerability management subverts the limitations of a traditional vulnerability management process and transforms it to into its strengths.

SanerNow advanced vulnerability management platform integrates and automates each step of vulnerability management and, as a result, helps organizations eliminate attack surfaces and reduce cyber-attacks. It goes beyond traditional vulnerability management and provides an advanced single-pane-of-glass solution that replaces the siloed solutions of the old with a natively built and truly integrated vulnerability management platform.

SanerNow quantifies your attack surface with Cyber Hygiene Score, normalizes your IT by fixing deviations, automatically scans and remediates vulnerabilities and security risks, and allows you to take control and strengthen your cyber defense.

Vulnerabilities are rapidly evolving,
Hackers are continuously surrounding,
And new cyberattacks are dangerously alarming!

But, Advanced Vulnerability Management is the pathway to a safer organization.



Vulnerabilities Detected

CVE	Assets	Hosts
CVE-2022-3723	wpasupplicant	1
CVE-2022-3158	tar	
CVE-2022-3653	python3.6-minimal	2
CVE-2022-3823	python3.6	3
CVE-2023-3603	wpasupplicant	5
CVE-2022-3256	tar	2
CVE-2023-3025	python3.6-minimal	0
CVE-2023-3347	python3.6	1

Vulnerabilities Assessed and Prioritized

□ Asset	Patch	Vendor	Date	Reboot	Risk	Host
□ Adobe Acrobat DC	https://helpx.adobe.com/acrobat..	adobe	2021-06-27	False	Critical	1
□ Apache Superversion	https://subversion.apache.com/..	apache	2021-06-17	False	Critical	1

Schedule a Patching Task

Pre-remediation script	Choose File No file chosen
Post-remediation script	Choose File No file chosen
Task Name	Task Name
Patching activity notification	Patches are being applied
Post Patching Activity Notification	All patches are applied successfully!
Groups to apply	Select Groups

SCHEDULE A DEMO

◀◀◀◀◀ ▶▶▶▶▶

About SecPod

SecPod is a cyber security technology company. We prevent cyberattacks. We do everything to prevent attacks on computing environment. Our product helps implement cyber hygiene measures, so attackers have tough time piercing through.

Our SanerNow CyberHygiene platform provides continuous visibility to computing environment, identifies vulnerabilities and misconfigurations, mitigate loopholes to eliminate attack-surface, and helps automate these routines. Our product philosophy is offering simplicity and automation to make the job of security administrators slightly better.

☎ Contact Us

Email us on: info@secpod.com | Visit us at: www.secpod.com