WHITE PAPER

Remediation 101

Common Pitfalls and Best Practices to Succeed at Vulnerability Management

NOPSEC

nopsec.com | hello@nopsec.com

Table of Contents

Introduction

Vulnerability risk management (VRM) can sound simple enough. In today's security-conscious environment, powerful vulnerability scanners are capable of identifying and generating detailed reports about numerous vulnerabilities across your environment. Your business may already have invested in the latest scanning technology (even if you use it less frequently than you should). Or you may be in the midst of deciding which scanner will generate the greatest return on investment.

Simply scanning, however, is not enough. By itself, the scan report does little to help most businesses quickly achieve the VRM goal that ultimately keeps the company secure: remediation. It takes the average organization more than three months to remediate vulnerabilities. If this sounds familiar, it's probably not because the information security (infosec) team is unaware of the risks posed to corporate and customer data or to critical operations from unremediated threats. Most likely, the infosec team is keenly aware of the need for effective remediation, and they are working harder than ever. But data overload produced by the scanner, as well as other common hurdles, may be getting in the way, slowing down remediation and keeping the team from scanning as often as best practice dictates.

Despite these challenges, there are ways to get your company's VRM program back on the path of keeping your business secure. In this paper, we explain common remediation pitfalls as well as

solutions to simplify remediation, reduce the average time it takes to close a remediation ticket, and keep your business running smoothly and securely.

Remediation Pitfalls

The number one remediation challenge reported by infosec professionals is data overload.

Pitfall #1: Data Overload

The number one remediation challenge reported by infosec professionals is data overload[1]. Most scanners make finding vulnerabilities relatively easy. The scanners fall short when it comes to adequately validating those vulnerabilities, ranking them, prioritizing them, and getting them to remediation. Typically, this means that the scanners produce lengthy vulnerability reports that overwhelm the infosec team with information. The staff doesn't know where to begin, so the burden is on them to evaluate and prioritize the data manually. This leads to frustration and communication breakdowns within the organization. In the meantime, un-remediated vulnerabilities put the company at risk despite the amount of effort put forth by the infosec team.

Pitfall #2: False Positives and Other Bad Data

Up to 60% of raw vulnerability scan data is "dirty" data like false positives, duplicates and mismatched endpoints. The average scanner does not do enough to eliminate this "noise" from its

[1] NopSec. "2016 Outlook: Vulnerability Risk Management and Remediation Trends." November 2015.

report output. Team members cannot trust the reporting as-is, so they must manually sift and sleuth through to determine what is a real threat and what is not. With time and resources already scarce (see Pitfall #4), the additional workload is something most infosec teams can ill afford.

Pitfall #3: Scanners that Don't Incorporate Enough Context

A scanner is made to find vulnerabilities, but it does not have the critical thinking skills to take contextual factors into account when ranking and prioritizing them. Most will attempt to prioritize vulnerabilities to some degree using the Common Vulnerability Scoring System (CVSS) and asset classification. However, these criteria are insufficient. For example, they do not take into account:

- Whether the vulnerability is known to be exploitable
- If there are active malware attacks against the vulnerability
- Whether the vulnerability will allow malware or phishing attacks to spread
- Other external data relevant to the risk score

Since the scanner doesn't weigh in these factors, the infosec staff has to do it through time-consuming manual research and analysis. Otherwise, the team may be chasing after small-time threats first, while the bigger ones go unaddressed and damage the business.

Pitfall #4: Lack of People, Time, and Expertise

Among small and medium-sized enterprises, dedicated infosec staff are rare. The IT staff is constantly juggling competing demands on their time and skills. Usually, they must balance responsibility for security along with other functions needed to run a business day-to-day, including operations, support, and development. Budgets are small, so the IT headcount is, too. Minimal resources contribute not only to a lack of time, but frequently a lack of expertise on the bench as well.

With everyone pulled in different directions, communication breakdown may also result, even if the organization is small. Combine these demands with the other typical remediation pitfalls, and it is no wonder that getting to remediation can take months even in a highly risk-aware company.

Avoiding the Pitfalls: Measure, Automate, Validate, Communicate

Measure

The first step to avoiding common pitfalls and making your remediation process a success is to create measurable remediation goals. Without goal-setting, the infosec team is trying to hit a target that it can't see. You may have a vague sense that the time to remediation is longer than it could be, or you may lack confidence in your prioritization methods. Setting goals and

tracking your progress will give you the evidence needed to address any issues.

Start by getting a baseline understanding of where your organization is with these metrics, and then set measurable goals for improvement where needed.

Each of the measures in this list may also be observed by application or charted and compared over a given timeframe (month-over-month, per quarter, etc.) to provide additional insight on opportunities to improve the company's risk posture, resource planning, or operational processes.

In addition, it is necessary to assess your organization's risk tolerance when it comes to certain remediation goals and situations. The reality is that even advanced and well-funded infosec departments cannot reasonably mitigate every threat in real time. Knowing both what is an optimal remediation goal and where to draw the line will help the IT team know when they can – and when they must – exchange their operational hats for their infosec hat and focus on remediation.

Risk tolerance will be different for every organization. If you are in a heavily-regulated industry, compliance may be the biggest determinant, making your tolerance lower than that of a similarly structured business in another industry. Part of your risk tolerance assessment will also be to establish, document, and communicate the process for escalating remediation and risk acceptance decisions if necessary. Members of the infosec team

at all levels should know when to escalate a remediation issue

REMEDIATION METRICS				
	Scan Frequency	Average Vulnerability Aging	Days to Patch Critical Systems	Number of Security Incidents
	Days From Discovery to Resolution	Number of Unresolved vulnerabilities in a Given Time Period	Change in Number of Vulnerabilities Over Yime	Compliance with Industry Regulatory Measures

and through what channels.

Automate

SaaS can take the burden of manual data-cleansing, verification, risk ranking, and prioritization activities off of the infosec staff, and help get to remediation faster.

A lot of remediation pitfalls can be avoided by investing in the right VRM technology. This means implementing a solution that effectively automates as many processes as possible. A popular myth is that automation is not feasible for some of the most time-consuming VRM tasks. This false assumption does not take into account technological leaps made in the VRM landscape, including the rise of software-as-a-service (SaaS) solutions. SaaS can take the burden of manual data-cleansing, verification, risk ranking, and prioritization activities off of the infosec staff, and help get to remediation faster. This sample technology selection checklist outlines benefits of choosing the right VRM technology and areas in which SaaS solutions tend to stand out.

Vulnerability Risk Management Solution Cheat Sheet

Business Need	VRM Selection Criteria	Enables Us To	Metrics
Risk Reduction	❑ Risk scoring uses threat intelligence data beyond CVSS scores and asset classification***	• Prioritize vulnerabilities in the context of our unique business environment	• Number of reported vulnerabilities by priority before and after implementation
	❑ Forecasts probability of exploitation of identified vulnerabilities***	• Reduce risk by addressing most exploitable vulnerabilities first	• Percentage of risk reduction in the environment • Number of security incidents
	❑ Offers continuous monitoring***	• Identify vulnerabilities in real time rather than through annual pen testing or infrequent scanning	• Scan frequency • Days from vulnerability discovery to resolution Average remediation ticket aging • Number of unresolved remediation tickets • Days to patch critical systems
	❑ Removes false positives and dirty data***	• Reduce time to remediation	
	❑ Facilitates communication between teams		
Cost Control	❑ Can be customized to your business needs***	• Avoid paying for unneeded features	• Cost of VRM technology • ROI of VRM technology
	❑ Automates processes that staff has been doing manually***	• Save on overtime or additional head count	• Cost of employee time dedicated to VRM • Cost of employee overtime
Resource Efficiency	❑ Automates workflow***	• Efficiently manage ticketing systems and communication	• Number of employee hours dedicated to VRM • Number of overtime hours • Percentage improvement in productivity
	❑ Automates risk scoring, vulnerability verification and threat correlation***	• Avoid manually researching, tracking and correlating threat intelligence	
	❑ Integrates with existing ticketing systems and patching platforms***	• Operate using single comprehensive platform • Eliminate unproductive time switching between systems	
Strategic Fit	❑ Integrates with multiple scanners, ticketing systems and patching platforms	• Maximize value of existing investments	• ROI of VRM technology
	❑ Single dashboard view of risk status, applications, processes and workload in progress	• Manage and monitor risk status and key measurements	• Change in number of vulnerabilities • Change in number of security incidents • Change in compliance with regulatory requirements
	❑ Complete reporting tool	• Improve accountability • Improve accountability • Benchmark and track continuous improvements • Communicate relevant information with key stakeholders • Demonstrate compliance with regulatory requirements	

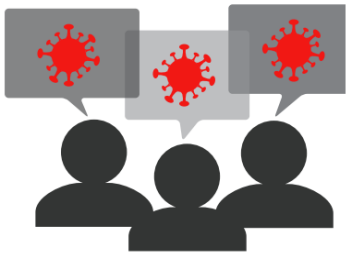
*** denotes critical criteria

Validate

Regular scanning and SaaS automation reduce your company's risk but do not eliminate the need for penetration testing (pen testing). Pen testing is still required to show whether your risk analysis and remediation are holding up to attacks coming from the real world – where real hackers possess not only sophisticated technology and creativity, but financial and other strong motivations to find their way around your security controls. Perform a pen test at least annually to validate the effectiveness of your risk analysis and remediation.

Communicate

Effective remediation requires cross-functional involvement. The infosec team needs the backing of the entire leadership team, including the CEO and CFO, in order to have the budget, resources, and business context to get to remediation efficiently. However, if IT is not the core function of your business, it's easy for the infosec team to feel as though they are on an island, or worse, competing to get the support they need. Z



Establish a regular rhythm for communicating the outcomes related to your remediation goals and pen testing.

Good reporting and communication systems can help. With a unified ticketing system, ticket status will be clear within and across departments, and visibility into open tickets will ensure the infosec team can address them in a timely manner. In addition, establish a regular rhythm for communicating the outcomes related to your remediation goals and pen testing. Keep leadership informed and involved in your wins as well as the

areas where you need their support to improve. After all, it's not just the infosec team that relies on remediation success to keep their jobs. The whole business depends on it.

Customized reports should be shared within the infosec team as well as with stakeholders outside of it. What the infosec people need to know and what outside stakeholders care about won't always be the same, so those who generate reports must take time to understand their audiences and tie their messages to the business outcomes that recipients care about most.

Stakeholders responsible for the big picture (board of directors, CEO, CFO) will not have time or need to hear about day-to-day measures important to the operational team like average ticket aging. What they do want is assurance of how secure and compliant the organization is and what the infosec team is doing to achieve those aims. Regulatory compliance measures, the overall number of security incidents, and reduction in number of vulnerabilities over time will help them understand the big picture trends they need to know about. Chances are good that they will also be hearing about high-profile threats and breaches in the news. Board and c-level reports should address these and demonstrate the infosec team's ability to keep up with news and trends.

Again, a quality SaaS VRM solution can streamline the reporting process to provide a customized, digestible, real-time view of where you are when it comes to meeting your remediation goals.

The usual pitfalls don't have to slow down your time to remediation and keep your business at risk. By setting measurable remediation goals and automating time-consuming processes like data cleansing, risk ranking, verification, and workflow, your team will get to remediation faster. Combined with annual pen test validation, you will have a clear picture of the effectiveness of your remediation efforts. Finally, regular communication with key stakeholders will give you the support and backing you need to continually improve remediation and keep the business secure.

Find Out How Spring Bank Used These Tips to Succeed at Remediation

Learn how using the right VRM technology allowed Spring Bank to simplify VRM, reduce time to remediation, improve reporting, and – most importantly – make their business more secure. Check out this 2-minute video.

Find out how NopSec's Unified VRM can help you think like a hacker and stay ahead of the trends. Visit www.nopsec.com or email hello@nopsec.com for additional information or to request a demo.

About NopSec

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.