seemplicity

You Can See It. Can You Fix It? A RemOps eBook

Moving From Output to Outcome

EBOOK

Introduction

Dynamic attack surfaces and rapidly evolving threats mean the ability to effectively remediate vulnerabilities is more critical than ever. But, as risks grow in complexity and volume, so too does the challenge of managing and mitigating them efficiently. This eBook explores the full spectrum of the remediation lifecycle, from the initial overload of findings to the implementation of sustainable, scalable processes that prioritize risk reduction, to reporting on progress.

The importance of remediation cannot be overstated. It is not merely about identifying risks but about taking actionable steps to reduce them. However, many organizations find themselves overwhelmed by the sheer volume of findings generated by their security testing tools. This overload often leads to a focus on output - counting and cataloging risks - rather than on the outcomes that truly matter: reducing risk and enhancing security posture.

This eBook explores the steps necessary to evolve from a reactive, firefighting mode to a proactive, resilient security strategy by delving into the key themes that define the remediation lifecycle:

STEP ONE

Managing findings overload

STEP TWO

Shifting from risk visibility and analysis to risk reduction

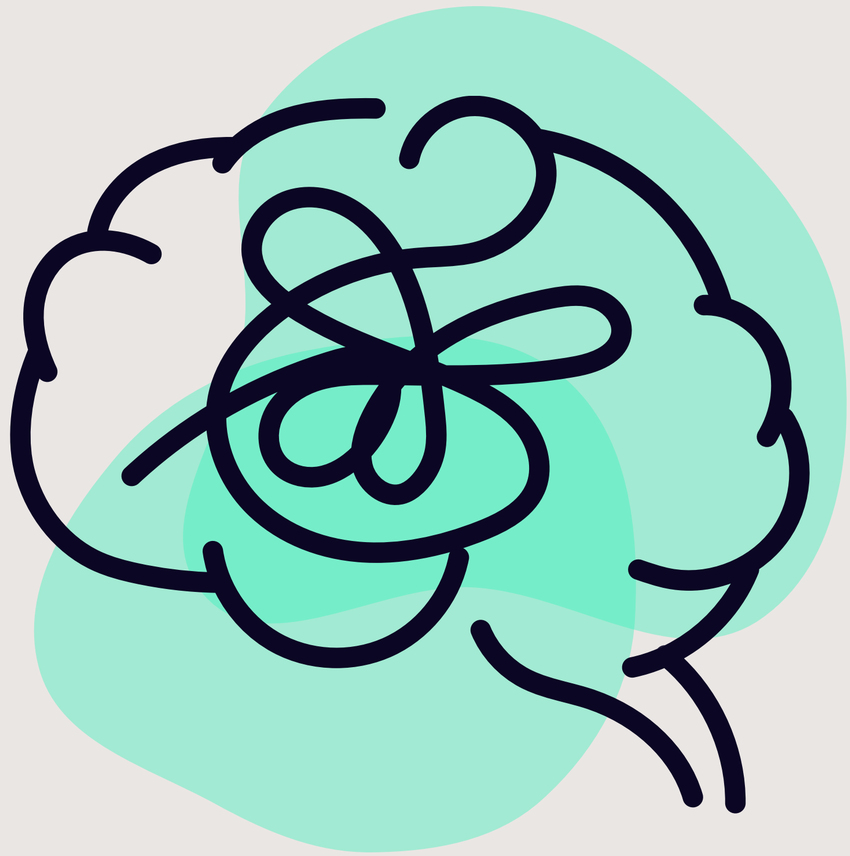
STEP THREE

Prioritizing remediation

01

NO-ONE WANTS FOMO

FINDINGS OVERLOAD, MIND OVERWHELMED



Understanding Findings Overload

In the cybersecurity industry, the effectiveness of testing tools is often paradoxically measured by the sheer volume of security-related findings they generate. This has led to a scenario where the loudest tools, those that generate the most findings, are perceived as the most effective. For example, if one vendor's tool uncovers 500 security findings while another identifies only 50, the natural inclination is to trust the tool with the higher number, and assume it provides more comprehensive coverage. However, this approach to evaluating security tools has created a significant challenge: findings overload.

Industry Practices Leading to Findings Overload

The root of this problem lies in a combination of industry practices and psychological biases. First, there is a lack of standardized benchmarks for what constitutes a "good" number of findings. Without an expected result or target number of findings, security teams often assume that more is better, leading them to favor tools that produce a higher volume of results. This emphasis on quantity over quality is further exacerbated by a common industry bias: the preference for false positives over false negatives. The fear of missing even a single critical issue pushes security teams to tolerate a flood of false positives, creating an overwhelming amount of data that must be sifted through - often manually.

Moreover, the industry's demand for tools that generate more findings has driven vendors to expand their offerings beyond their core areas of expertise. This expansion often leads to duplicated findings, where different tools report the same vulnerabilities in slightly different ways. For instance, Extended Detection and Response (XDR) solutions, originally designed to detect and prevent malicious attacks, now often include features for testing vulnerabilities—areas traditionally outside their core focus. Similarly, web application security testing tools have expanded into external attack surface management, and Cloud Security Posture Management (CSPM) tools now often scan for cloud misconfigurations, leading to overlap and redundancy in findings.

Consequences of Findings Overload

The consequences of findings overload are far-reaching. As security teams become inundated with an ever-growing list of vulnerabilities, their focus shifts from the ultimate goal of reducing risk to merely managing the output of these tools. The process brakes, with teams spending more time counting and cataloging risks than actually fixing them. As such the focus on generating findings has overshadowed the true purpose of these tools: to reduce risk.

02

SHIFTING FROM RISK VISIBILITY AND ANALYSIS TO RISK REDUCTION

Findings Aren't Fixes

As the previous chapter made clear, the cybersecurity industry has been driven by the fundamental principle: "You can't protect what you don't see." The fixation with visibility birthed a risk analysis function into existence - albeit a passive one. The security scanning tools of today offer more accurate and contextualized findings, providing a clearer picture of the risk landscape than ever before. However, this mountain of data often lands squarely on the shoulders of CISOs and their teams, who are then tasked with the overwhelming job of deciding how to act on these findings.

So, while the focus remained on visibility, the industry neglected a more important question: "Can you protect what you do see?" To advance remediation operations, organizations must transition from a focus on visibility and analysis to an emphasis on risk reduction.

Making Visibility Actionable

The journey from risk visibility to risk reduction begins with transforming how organizations interpret and respond to security data. Merely having visibility into risks is no longer sufficient. To be effective, organizations need to translate this visibility into actionable insights that drive risk reduction. In other words, they need to shift their focus from output - the number of findings - to outcomes - the reduction of risk through effective remediation. This requires a fundamental shift in how risk analysis is perceived and utilized. Instead of viewing risk analysis as an end in itself - a way to assess the current state of security - it should be seen as a stepping stone toward active risk mitigation.

Transitioning to a Risk Reduction Focus

Shifting the focus from risk visibility to risk reduction involves redefining success metrics within cybersecurity programs. Traditionally, success has been measured by the number of risks identified and cataloged - a continuation of the visibility-centric mindset. However, to achieve meaningful improvements in security posture, organizations must adopt new key performance indicators (KPIs) that emphasize the reduction of risk through proactive remediation efforts.

These KPIs should measure not only how many vulnerabilities have been identified but also how many have been effectively mitigated. By setting clear, actionable goals tied to risk reduction, organizations can monitor their progress over time and make data-driven decisions about where to allocate resources and which technologies to implement. This approach also facilitates continuous process improvement, enabling teams to refine their strategies based on measurable outcomes.

Moreover, focusing on risk reduction allows for better communication across all levels of the organization. Effective risk reduction is a multi-team effort, involving stakeholders from across the organization. Each team - whether it's security, IT, or development - must understand their role in the remediation process and be held accountable for their part in reducing risk. When risk management efforts are tied to specific, quantifiable outcomes, it becomes easier to demonstrate progress to stakeholders. This transparency fosters accountability and ensures that all parties are aligned in their efforts to reduce risk.

03

WHEN EVERYTHING IS TREATED AS A PRIORITY, NOTHING IS TRULY PRIORITIZED

Risk Reduction in Practice

Shifting from risk visibility to risk reduction is easier said than done. Even with improved visibility and a focus on actionable outcomes, organizations often face a significant challenge: prioritization. In an environment where resources are limited and the volume of security findings is vast, deciding which vulnerabilities to address first becomes crucial. Yet, these very factors mean that prioritization efforts are often reactive, limiting process efficacy and scalability.

The Pitfalls of Firefighting

Security teams find themselves trapped in a cycle of constant “firefighting,” reacting to the latest and loudest vulnerabilities and addressing critical issues as they emerge, rather than following a proactive and planned approach. This reactive posture is not only unsustainable but also prevents organizations from building scalable, long-term remediation strategies that can withstand future challenges.

Moreover, the ad hoc approach leads to inefficiencies, with security teams spread thin across a vast landscape of issues. The constant demand to address urgent vulnerabilities diverts attention and resources away from developing a more resilient, comprehensive security posture. Overwhelmed by the sheer number of findings, teams often resort to quick fixes for the most glaring issues, leaving other, potentially dangerous vulnerabilities unaddressed.

Operating in firefighting mode also introduces significant delays in remediation. Often, by the time a vulnerability is flagged as a priority - because an exploit is already in the wild - the window for effective mitigation may have already closed. This reactive stance is not only inefficient but also perilous, leaving organizations exposed to risks that could have been mitigated with a more proactive approach.

The Cost of Inefficiency

The reason for these reactive prioritization efforts is resource limitations; a central challenge in the remediation process. Addressing even a single security finding involves several costly and time-consuming steps: analyzing the finding, determining its relevance, opening a ticket, and coordinating with the appropriate team to implement the fix. These steps require significant manpower, and the administrative burden alone can be overwhelming, especially for security teams that are already operating at, or beyond, capacity.

These resource constraints often force security teams to focus solely on the most critical findings, neglecting other important vulnerabilities that could escalate into serious risks if left unaddressed. This limitation prevents organizations from adopting a proactive approach to remediation, instead locking them into a cycle of reacting to the latest crisis. This inefficiency not only heightens the risk of security incidents but also severely hampers the organization's ability to scale its remediation operations to meet growing demands.

Furthermore, the cost of inefficiency extends beyond the immediate security team. As vulnerabilities remain unaddressed due to prioritization challenges, the risk to the entire organization increases. This can result in costly breaches, regulatory fines, and damage to reputation—all of which could have been mitigated with more effective resource allocation.

Towards Effective Prioritization

To move beyond the limitations imposed by firefighting and resource constraints, organizations must develop a systematic approach to prioritization. This involves not only assessing the criticality of vulnerabilities but also making strategic decisions about how to allocate limited resources most effectively.

One key strategy is to automate the administrative processes associated with remediation. By reducing the time and effort required for tasks such as analysis, triage, and ticketing, organizations can free up valuable resources that can then be directed toward actual remediation efforts. This approach allows security teams to address a broader range of vulnerabilities, rather than being forced to focus solely on the most immediate risks. As a result, the security team is no longer a bottleneck in the remediation process.

Another essential strategy is to leverage parallel workflows wherever possible. Different types of findings - for example those identified by External Attack Surface Management (EASM) tools versus Static Application Security Testing (SAST) tools - often require remediation by different teams. By enabling these teams to work concurrently on separate streams of vulnerabilities, organizations can reduce bottlenecks, accelerate the remediation process, and make more efficient use of their limited resources.

Building a Scalable Remediation Process

Effective prioritization is the foundation of a scalable and efficient remediation process. By addressing the inefficiencies and resource constraints that plague many organizations, security teams can allocate their efforts more strategically, focusing on the vulnerabilities that pose the greatest risk. This not only improves the organization's ability to manage current risks but also prepares it for future challenges by ensuring that security processes can scale with the organization's needs.

A scalable process also requires continuous assessment and refinement. As organizations grow and their security environments become more complex, their prioritization strategies must evolve accordingly. By continuously improving and adapting their approach, organizations can ensure that their remediation processes remain both efficient and effective, even in the face of resource constraints.

04

FROM COLLECTING RISK DATA TO ACTUALLY REDUCING RISK

The Action Plan

In the previous chapters, we've explored the challenges of findings overload, the importance of shifting from risk visibility to risk reduction, and the critical role of prioritization in the remediation process. While these elements are essential for a robust cybersecurity strategy, the ultimate goal is to move beyond data collection and analysis to actually reducing risk. This chapter focuses on actionable steps to make that transition, enabling organizations to shift their key performance indicators (KPIs) from "risks found" to "risks remediated."

To achieve meaningful risk reduction at scale, organizations must move away from a reactive, firefighting approach and adopt a proactive strategy that integrates and optimizes their existing vulnerability and risk management processes. The following seven steps outline how to transition from simply collecting risk data to actively reducing risk in a structured and efficient manner.

STEP 1 | Collect – Create a Centralized Backlog

The first step in transitioning to a risk reduction-focused approach is to consolidate all findings into a single, centralized backlog. In the traditional, findings-based approach, security teams often start by logging into the dashboards of various security tools, each with its own functionality and terminology. This fragmented process makes it difficult to manage and prioritize findings effectively.

To overcome this, organizations should centralize all findings from their security testing tools into one location, whether that be a spreadsheet, database, or another system. This centralized backlog serves as the foundation for a fixing-based approach, allowing for more streamlined management and enabling the organization to transition from a focus on identifying risks to actively remediating them.

STEP 2 | Consolidate – Normalize, Deduplicate, and Enrich with Context

Once all findings are centralized, the next step is to consolidate this data by normalizing, deduplicating, and enriching it with relevant context. Normalization involves standardizing the formats used across different tools, creating a uniform dataset that can be consistently managed. This step is critical because uniformity allows the organization to execute remediation processes consistently across all findings.

After normalization, it's essential to remove duplicate findings. Deduplication streamlines the backlog by eliminating redundant entries, making it easier to focus on the most relevant and actionable items. Furthermore, by enriching the findings with additional context - such as ownership information gathered from a configuration management database (CMDB) - organizations can make more informed decisions about who should be responsible for remediation actions and how those actions should be prioritized.

STEP 3 | Choose – Decide What, Who, How, and Where to Remediate

With a consolidated and enriched backlog in place, the next step is to decide how to prioritize and assign remediation tasks. This involves a multi-dimensional approach to prioritization that takes into account several factors:

WHAT	Determine whether to prioritize findings based on external context, such as the presence of a known exploit, or internal context, such as the specific domain (cloud, code, etc.) affected by the vulnerability.
WHO	Identify the appropriate remediation team based on the resource ownership information collected in the previous step. This ensures that the right team is tasked with the right remediation actions.

HOW	Prioritize remediation actions over individual findings. If multiple findings can be addressed with the same solution, aggregate them into a single remediation task to streamline the process.
WHERE	Decide where to open the remediation ticket within the organization's workflow, whether in Jira, ServiceNow, or another system, ensuring that the task is seamlessly integrated into the existing processes of the remediation team.

This step is crucial for ensuring that remediation efforts are focused, efficient, and aligned with the organization's overall risk reduction goals.

STEP 4 | Route – Get Remediation Tasks to Remediation Owners

Once the remediation actions are prioritized and assigned, the next step is to route them to the appropriate teams. Effective routing ensures that remediation tasks are not only assigned correctly but also executed in parallel rather than sequentially. This approach prevents bottlenecks and makes better use of available resources.

For example, if Engineering and DevOps teams are responsible for different sets of findings, the remediation tasks can be routed simultaneously to both teams. This parallel processing enables the security team to address multiple issues at once, significantly speeding up the remediation process and reducing the overall risk exposure.

STEP 5 | Receive – Automate Backlog Management

To truly scale remediation operations, automation is key. Automation can be implemented by creating programmatic workflows that synchronize security data with other organizational processes, allowing security teams to focus on higher-level strategic tasks rather than manual data management.

For instance, when a vulnerability is detected, an automated workflow can immediately open a remediation ticket in the appropriate system and assign it to the correct team. Additionally, bi-directional workflows can ensure that when a ticket is closed, the results are verified against the next testing scan, with any discrepancies automatically flagged for further investigation.

Automation not only streamlines the remediation process but also ensures that security data is available to the right teams at the right time, enabling more efficient and effective risk reduction.

STEP 6 | Remediate – Where the Hard Work Gets Done

This step is where the actual remediation takes place - whether that involves applying a fix, mitigating a vulnerability, or accepting a certain level of risk. Although this phase is critical, it is often out of the direct control of the security team. The role of the security team in this step is to ensure that the remediation process is well-supported, with clear, actionable tasks and the necessary resources allocated to the remediation teams.

STEP 7 | Report – Measuring Performance and Efficiency

The final step in the transition from data collection to risk reduction is to implement robust reporting mechanisms that track and measure the effectiveness of the remediation process. With an automated routing process in place, organizations can gain real-time visibility into the status of the entire backlog, including metrics such as the number of new findings, the ratio of resolved to unresolved findings, and the average time taken for remediation.

These metrics not only help in assessing the performance of individual remediation teams but also provide valuable insights for continuous process improvement. By comparing performance across different teams or departments, organizations can identify areas of strength and weakness, allowing them to optimize their remediation strategies further.

Moreover, these reports can be used to communicate the effectiveness of the remediation program to stakeholders, demonstrating progress in reducing risk and enhancing the organization's overall security posture.

05

SECURING THE FUTURE

The journey through risk remediation, from the initial challenge of findings overload, to the implementation of a proactive risk reduction strategy, to the final step of reporting, highlights the complexities and necessities of modern cybersecurity management. As we've explored, effective remediation is not just about identifying vulnerabilities; it's about taking decisive, strategic actions that reduce risk and strengthen the overall security posture of an organization.

The remediation lifecycle is a dynamic process requiring constant attention, adaptation, and improvement. The shift from output to outcome is a fundamental transformation in how security is managed and perceived within the organization. By embracing this approach, security teams can move from being seen as a bottleneck to being recognized as enablers of business resilience and success.

The future of vulnerability management lies in proactive, outcome-focused strategies that prioritize risk reduction at every stage. By adopting the practices outlined in this eBook, organizations can build a more resilient security posture, better protect their assets, and confidently navigate the ever-evolving threat landscape. The goal is clear: not just to manage risks, but to actively reduce them, ensuring a safer, more secure enterprise.