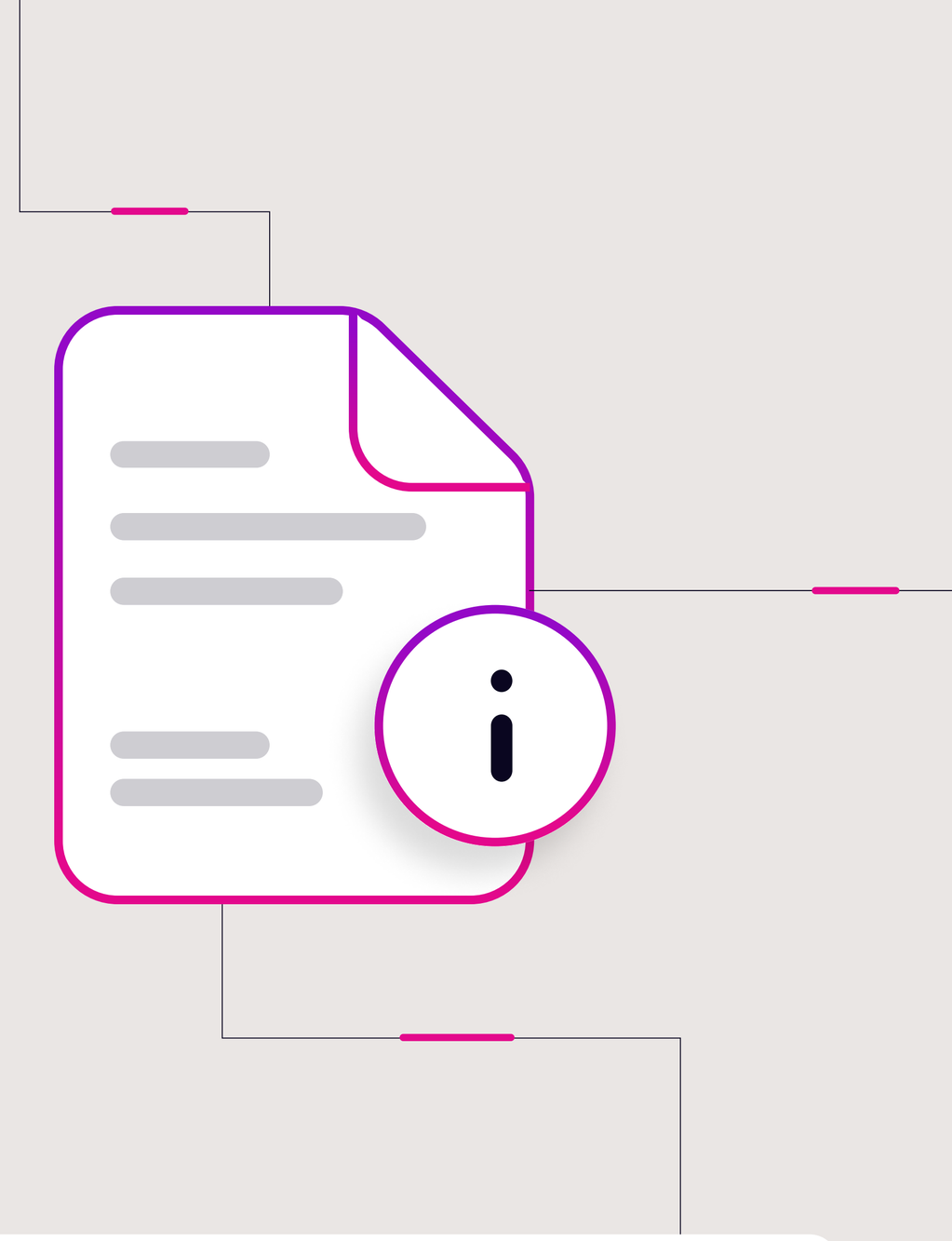
seemplicity

Managing Vulnerability Noise



GUIDE

The Importance of Noise Reduction

Whether your team is trying to establish a scalable exposure management program or is just looking to refine processes in general, managing vulnerability and exposure testing noise is an important step that will maximize efficiency and improve visibility overall. For growing organizations, especially those with extensive SaaS and cloud offerings, and those developing their own software, managing testing noise can be a daunting task. Fortunately, by following established principles outlined in this guide, security teams can set themselves up for success and tackle the masses of data generated by their scanning tools. By addressing specific challenges with repeatable strategies, organizations can overcome noise, streamline workflows, and reduce risk.

As businesses grow and expand their security program, they often bury themselves with findings from multiple testing tools, each with its own scoring system and limited context. Without a centralized platform to consolidate, deduplicate, and prioritize vulnerabilities and exposures, critical risks are usually overlooked, and communication between teams becomes fragmented. The result is missed service-level agreements (SLAs), reactive fire drills, and a demoralized workforce, all of which throttle an organization's ability to manage its security posture.

Effectively managing vulnerability and exposure testing noise offers extraordinary benefits, especially for growing organizations. By centralizing and prioritizing findings, security teams can allocate resources more effectively, foster better collaboration across teams, and maintain a proactive approach to risk reduction. This helps ensure security efforts are focused on the most critical issues, enhancing both efficiency and confidence. With the right processes and tools in place, companies can move from reactive, fragmented workflows to cohesive, high-impact remediation strategies that strengthen overall security posture.

The Challenges of Vulnerability Testing Noise

To effectively manage vulnerability noise, it's crucial to first understand the challenges you may encounter. Below, we'll explore some common obstacles teams face and then discuss strategies to overcome them.

What is Testing Noise?

Vulnerability and exposure testing noise is non-actionable data generated by security scanning tools, often characterized by duplicate findings, low-priority issues, and findings that lack contextual relevance. Testing noise results when multiple tools, each using different scoring systems and methodologies, generate conflicting results that security teams need to manually sift through to identify meaningful risks. The lack of standardized, consolidated data can obfuscate critical threats, delay remediation efforts, and drain resources. For complex organizations managing SaaS environments, cloud infrastructures, or hybrid networks, testing noise complicates their ability to prioritize and address pressing vulnerabilities and exposures, which increases their risk of exploitation.

Vulnerabilities Without Solutions

Vulnerabilities without known solutions for remediation live in a gray area of testing noise. While they provide important insights into overall security posture, the lack of actionable next-steps can create challenges for security teams. Without a clear path for mitigation, these findings remain unresolved in backlogs, contributing to the overall volume of data and potentially distracting from more critical, fixable issues. Even so, these findings should not be dismissed as noise. Instead, they can influence the strategy for future risk reduction efforts, such as tracking emerging patches, monitoring threat intelligence for exploits, or implementing compensating controls. When managed properly, these findings can complement a broader risk management strategy rather than simply adding to the noise.

Overlapping Findings from Multiple Tools

Growing organizations rely on a number of vulnerability testing tools, such as infrastructure vulnerability scanners, application security scanners, and cloud-specific scanners, to identify vulnerabilities and exposures. While these tools are essential for broad coverage, they often produce overlapping findings that are difficult to consolidate. Each tool has its own format, scoring system, and prioritization method, leaving security teams the challenge of piecing together a coherent picture of their overall risk posture. This results in duplicate findings clogging remediation workflows, making it harder to identify and remediate critical issues. Without a centralized, unified approach to managing these findings, teams waste time navigating unnecessary noise instead of focusing on impactful remediation.

Reliance on Manual Workflows

Unfortunately, many organizations still rely on manual processes, such as editing spreadsheets, to track and report vulnerabilities and exposures. These methods are time-consuming, prone to human error, and usually can’t keep up with the volume of findings generated by modern scanning tools. Security teams could spend hours consolidating data from multiple sources, only to find that the information is outdated by the time it reaches decision-makers. Relying on manual processes delays risk reduction efforts and leaves organizations exposed to threats, increasing the likelihood of exploitation.

Poor Communication Between Teams

Poor communication between security teams, engineering teams, and operations teams is a common challenge enterprises face. Without clear insights, actionable recommendations, and expected SLA timelines, vulnerability findings often get overlooked or ignored. This causes frustration and misalignment between teams. Security teams may accidentally contribute to the issue by presenting findings in disorganized, rigid formats, while engineers might be failing to properly document the reasons for declining or deferring service requests. This miscommunication results in delayed responses, missed remediation opportunities, and strained relationships between teams, ultimately undermining the organization's security posture.

Missed SLAs and Inefficiencies

When testing noise isn’t managed properly, one of the worst consequences is missing SLA timelines for addressing critical exposures. A lack of prioritization criteria or even general guidance for remediation teams results in security teams initiating more fire drills, disrupting planned work and stretching resources thin. This reactive approach not only increases stress across teams but also introduces operational inefficiencies, as findings may need to be revisited multiple times due to a lack of proper coordination. Over time, this chaotic cycle erodes team morale and creates tension between team members.

Real World Challenge

A security team lead at a growing SaaS company spent countless hours each week sifting through findings from multiple tools—cloud security, SaaS-specific scanners, and other infrastructure assessment tools. Each one produced its own reports, scoring systems, and formats, leaving the team with a mountain of data but no clear direction on next-steps. Manually consolidating findings into a single spreadsheet took hours. After the spreadsheets were handed off to engineering teams, managers were unclear on which findings should be prioritized, and they ended up missing SLAs, which increased tension between teams.

On the engineering side, teams struggled to deal with the crushing volume of findings they received. Without proper context or clear priorities, every additional request felt like a fire drill, pushing planned work aside and creating unnecessary chaos. The constant back-and-forth strained communication between security and engineering, leaving both teams frustrated and uncertain about where to focus their efforts. Even though significant time and effort was spent trying to address these issues, the organization still lacked a clear picture of its most critical risks, PCI audits were extremely stressful, and no one felt confident about the path forward.

BUILDING A NOISE

Resilient Vulnerability and Exposure Management Program

STEP 1 Centralize Vulnerability & Exposure Data

STEP 2 Streamline Communication Channels

STEP 3 Prioritize Findings

STEP 4 Align Remediation Efforts

STEP 1 | Centralize Vulnerability and Exposure Data

The first step in building a noise-resilient program is to normalize and centralize findings into a unified backlog. Growing organizations often rely on multiple tools, and while these tools are essential for broad visibility, they also produce siloed reports with overlapping or conflicting findings. By leveraging a unified remediation operations (RemOps) approach, organizations can consolidate findings with conflicting risk scores into a single source of truth.

Centralizing data not only saves time but also allows security teams to focus on remediation strategies instead of wasting effort navigating fragmented tools. Superior RemOps systems also aggregate findings after normalizing and deduplicating findings, which reduces noise and ensures teams are not distracted by duplicate or low-priority issues. With a unified repository of vulnerabilities and exposures, security leaders can make better decisions about where to allocate resources, enabling faster and more effective remediation.

STEP 2 | Streamline Communication Channels

Once findings have been normalized and centralized, the next step is improving communication between stakeholders. Disjointed communication leads to delays and confusion, with engineering teams unsure of which issues to prioritize or why they matter. By leveraging automation to deliver clear status and deliverable metrics, organizations can ensure that relevant stakeholders receive timely, accurate, and actionable information.

Creating detailed dashboards that provide a high-level view of the organization's risk posture while still allowing teams to drill down into specific issues when necessary further streamlines communications. Configuring these according to each organization's needs provides dynamic reporting options that allow stakeholders to track remediation progress, identify outstanding tasks, and monitor trends over time without sifting through spreadsheets or email threads. Depending on each organization's circumstances, teams and individuals may require greater or more limited role-based access to vulnerability and remediation information throughout the organization, which is something that a well constructed dashboard can provide. When everyone has the information required for their remediation roles, it eliminates ambiguity, ensures alignment across teams, and gives leaders confidence that critical issues are being seen and addressed.

STEP 3 | Prioritize Findings

Managing noise requires the ability to differentiate between high-risk and low risk issues. Without proper prioritization, teams spend time on findings that pose minimal threat while missing critical exposures. Industry-standard frameworks like the Common Vulnerability Scoring System (CVSS) can help with prioritization, and they provide a strong baseline for understanding severity, but effective prioritization goes beyond scoring alone. Contextual risk assessments—where organizations evaluate asset criticality, exploitability, and business impact—help teams focus on what truly matters.

An effective prioritization strategy blends external threat intelligence with internal organizational context. Tools that incorporate real-time exploitability data like the Exploit Prediction Scoring System (EPSS) or the Cybersecurity and Infrastructure Security Agency Known Exploited Vulnerabilities (CISA KEV) lists help teams identify which vulnerabilities are actively being exploited. By layering this data with specific business context, security teams ensure their remediation efforts are aligned with real-world risks. The result is a streamlined process that reduces noise, accelerates remediation, and minimizes exposure to critical threats.

STEP 4 | Align Remediation Efforts

The final step in building a noise-resilient program is to align remediation efforts between security, development, and operations workflows. One of the biggest challenges organizations face is making sure that actionable insights reach the right teams with minimal friction. Security teams spend countless hours consolidating and delivering vulnerability and exposure data to development and operations teams, only to face delays caused by unclear priorities or inadequate context. By providing clear, prioritized insights, security teams can empower development and operations teams to take action quickly and confidently.

Reducing manual effort is key to scaling remediation operations that align with existing development and operations workflows. A noise-resilient approach can leverage knowledge about the organization's priorities, remediation process participants and existing work platforms to automatically route prioritized tasks to the appropriate teams, integrating with ticketing tools like Jira or ServiceNow. This ensures teams receive requests in platforms they're already used to, complete with all the context needed to address issues effectively. It also encourages greater visibility and accountability between teams, as each team receives updates and requests in the platforms of their choice.

Tools and Strategies for Noise Reduction

Organizations need a combination of tools and strategies to effectively manage vulnerability and exposure testing noise. A RemOps platform is one of the most impactful tools a business can use to manage testing noise now, and as they further scale and mature their security program. Top RemOps platforms come with standard features like customizable dashboards, role-based access, and advanced ticketing capabilities. They provide clear visibility into your risk landscape, and help teams prioritize and act on findings without having to switch between multiple tool readouts.

Automation also plays a critical role in reducing noise and increasing efficiency. By minimizing manual data collection and leveraging AI insights, organizations can save countless hours and eliminate human error. Consolidation across scanning tools allows teams to see and respond to emerging risks, ensuring critical exposures aren't lost in the noise so they can be addressed in a timely manner. With the appropriate amount of automation, security teams can focus their efforts on high-priority issues instead of being bogged down by administrative tasks.

Tracking Vulnerabilities Without Known Solutions

When dealing with vulnerabilities without known solutions for remediation, capable RemOps platforms let users temporarily mark a vulnerability as an exception, allowing users to set an exception expiration date, automatically triggering re-evaluation when it expires. Some organizations require a manager's approval for exceptions, and the platform facilitates exception approval workflows to ensure process compliance. When designating vulnerabilities as exceptions, it's essential to document reasoning, approvals, and reminders for re-evaluation.

Measuring Success

Measuring the effectiveness of your noise reduction efforts is essential for long-term success. Start by defining key metrics that align with your goals. These might include reductions in time spent on manual tasks, improvements in SLA compliance rates, and decreases in open vulnerabilities and exposures. Tracking these metrics allows organizations to assess the tangible benefits of their noise management strategies and identify areas for further optimization.

Continuous improvement is necessary for maintaining an effective noise management program. Regularly review your processes and tools to ensure they remain aligned with evolving business needs and threat landscapes. Gathering feedback from development, operations and security teams is equally important. Their insights can help uncover bottlenecks, streamline workflows, and ensure all stakeholders are aligned in their efforts to manage risk effectively. By fostering a culture of continuous improvement, organizations can refine their strategies to stay ahead of emerging challenges.

The Path Forward

Managing vulnerability and exposure testing noise is a difficult security challenge, especially for rapidly growing organizations, but with the right tools and strategies, it can be effectively managed. Centralizing findings, streamlining communication, prioritizing findings, and aligning teams are all critical steps toward reducing noise and improving efficiency.

As a next step, evaluate your current tools and processes to identify gaps and inefficiencies. Consider adopting a RemOps platform to consolidate data, streamline communication, and prioritize vulnerabilities in a way that scales with your organization. By taking proactive measures, your organization can reduce testing noise, enhance team collaboration, and achieve risk reduction outcomes.