Remediation Operations

A STEP-BY-STEP GUIDE TO VULNERABILITY REMEDIATION

an eBook by seemplicity

Table of Contents

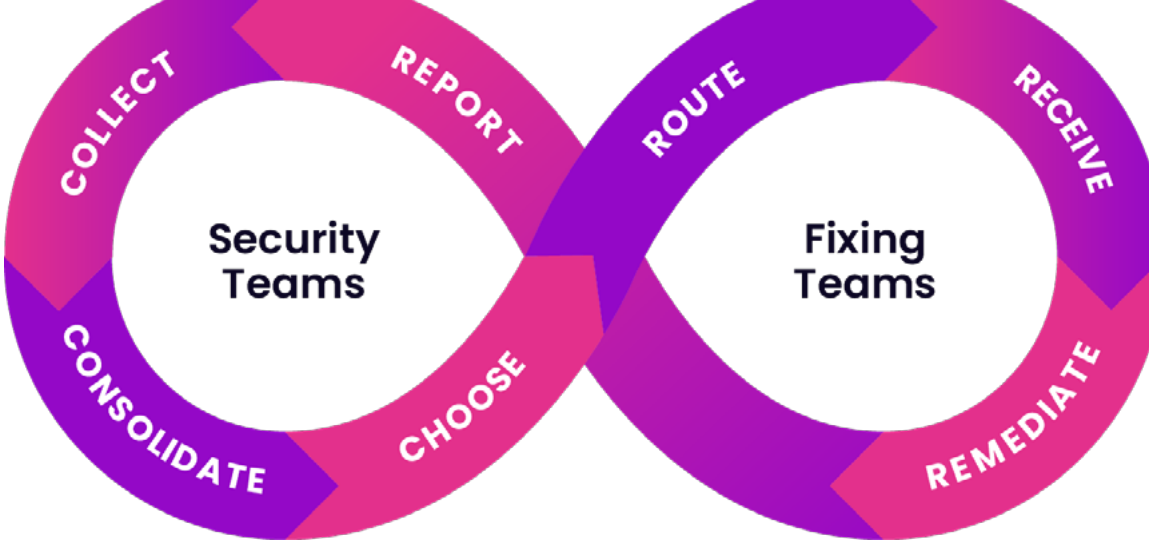
Introduction

In the ongoing battle against cyber incidents, many organizations have resorted to conducting multiple risk reduction programs simultaneously across their attack surface—with each often requiring their own domain-specific teams and tools to scan, discover, identify, and remediate security findings.

With overlapping capabilities, multiple tools inevitably create redundant reports of risks, contributing to the overall noise in the process. Security teams are then tasked with making sense of separate formats, scoring systems, noisy scanners, and complicated remediation workflows before they can accurately assess and remediate risk to the organization.

Thankfully, there are tried-and-trusted methods for remediating vulnerabilities across multiple domains and at scale. While most methods involve significant manual processes, one emerging category seeks to automate as much as possible. Remediation Operations is the collection and automation of cybersecurity business processes that minimize risk by mobilizing the right teams with the data and context they need to eliminate, reduce, or accept risk findings.

This guide will present the basics of Remediation Operations which, when executed well, allows you to accelerate risk reduction, maximize security team productivity, and ensure confidence and compliance. Whether you are an IT professional, a business owner, or a SOC manager, applying the following principles will help your organization streamline the vulnerability management process.



Steps to Remediation

A successful Remediation Operations program incorporates seven essential steps. When carefully applied, they help minimize uncertainty and expedite remediation. This approach provides security teams with a structured, repeatable process that ensures no critical steps are missed and resources are efficiently allocated. It also allows organizations to spot abnormalities, evaluate effectiveness, and make adjustments as needed.

01

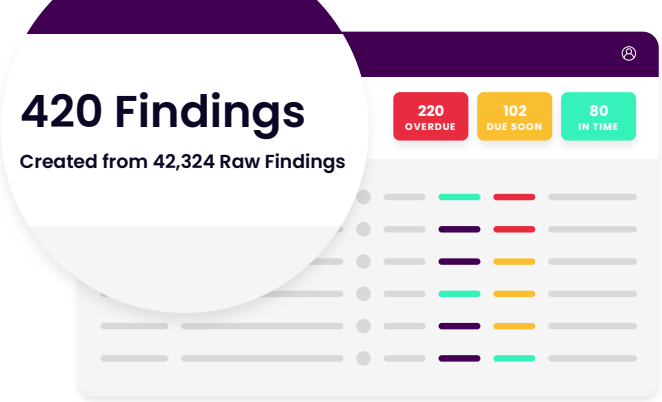
COLLECT

Collect Security Findings

The first step in Remediation Operations is to collect security findings. Systematically gather security risks and vulnerabilities from pen testing, vulnerability scanners, and all your other security testing tools. Make sure you're covering all the domains you operate in, like on-prem, cloud, code, SaaS, etc.

Security Findings Sources

- Application Security
- SaaS Security
- CI / CD Pipeline
- Security Controls Validation
- Cloud Security
- Vulnerability Management
- Pen Testing



02

CONSOLIDATE

Consolidate, Deduplicate & Aggregate Findings

After you've collected findings from your security testing tools, organize them into normalized and actionable backlogs for your fixing teams. Separate security tools (with different risk scoring systems) frequently identify the same vulnerabilities, so you'll need to deduplicate and normalize these on your backlogs. This makes it much easier when you can see the true number of vulnerabilities you're dealing with, and when you can accurately compare them using a unified scoring system.

Intelligent aggregation is an extremely valuable capability in Remediation Operations. Some remediation actions can resolve multiple vulnerabilities (sometimes across multiple resources) at once. Aggregating findings based on remediation can help your organization optimize the remediation process and provide a consolidated view of next steps.

Consolidating, deduplicating, and aggregating security vulnerabilities is crucial for establishing a unified "source of truth." For example, imagine trying to identify whether log4j has resurfaced in your IT ecosystem. If you've done a good job with consolidation, your security teams can locate all instances of log4j vulnerabilities, regardless of whether they were initially discovered by network security scanning, cloud security scanning, or application security scanning tools. This consolidated source of truth makes it possible for you to prioritize remediation efforts effectively, making the most of your available time and resources.

RemOps Tip

Many vulnerabilities have known mitigation measures, and if you can automate your process to pair these fixes to your vulnerabilities, you'll save a good deal of time and effort. Many times, one fix will remediate multiple vulnerabilities. Aggregating findings based on fixes will make even the largest remediation backlogs more manageable.

03

CHOOSE

Choose Remediation Teams & Fix Priority

You need to choose:

- Who will do remediation work
- What needs to be remediated first
- Where remediation will be applied
- How remediation is accomplished

One of the most impactful parts of a good Remediation Operations program is the "choose" step. Each organization will want to automate their remediation process to a different extent, but you will need to choose and clearly outline the rules for how to do it. This will ensure that your remediation efforts align with your organization's goals, security policies, and resource allocation. It also empowers your teams to proceed with confidence in the remediation process, minimizing uncertainty and enhancing productivity.

RemOps Tip

Too often, organizations rely on institutional knowledge to get fixes to the right person or team. While this may work in the short-term, it's not sustainable for large or growing organizations. Document ownership of remediation tasks and put a process in place so everyone knows which requests go to which teams for remediation.

- **Who will do remediation work:**

Choose whether one team, multiple teams, or even a single person will be responsible for handling remediation work. For example, is there a single team responsible for cloud security remediation? What about application security? Once you define each of these remediation teams, you'll be able to send security findings quickly and consistently to the appropriate owners to be fixed. Making these choices in advance will help you streamline remediation across multiple domains in your organization.

- **What needs to be remediated first:**

Many organizations implement fixes based on some measure of the risk mitigated, but sometimes it's not that simple. Different companies have varying security priorities, so you may need to customize how you implement your priority scoring to align with the guidelines of your organization. This customization could even extend to individual remediation teams within your organization as well.

- **Where remediation will be applied:**

You will need to determine which machines or systems in your organization require remediation. Once a vulnerability is identified, it's important to find all the locations that it exists within your organization. This is where aggregation in the previous step comes in handy, as it consolidates information and provides a comprehensive view of the vulnerability's presence throughout the organization. Your remediation teams are then able to decide if they're going to apply the remediation measures across all, some or none of the identified vulnerabilities.

- **How remediation is accomplished:**

Your organization should outline the methods and procedures for remediation. Whether the remediation process involves patching software, reconfiguring systems, or implementing other security measures, it is essential to have a well-documented and structured approach. For example, do manually created exceptions need to be reviewed before they are added to a remediation queue, or are they added automatically? Outlining methods and procedures is essential to ensure that all teams are aligned and understand their roles in the remediation process.

04

ROUTE

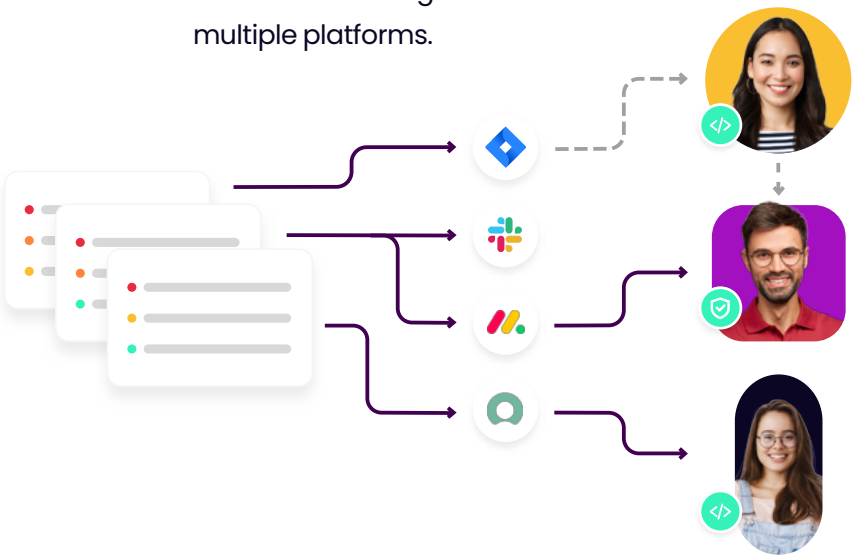
Route to the Fixer in the Appropriate Platform

RemOps Tip

Remediation Operations Platforms keep track of where to route tasks, let you manage overall remediation workflows, and allow you to automatically distribute requests in appropriate platforms like Jira, ServiceNow, etc.

Routing remediation requests is often done via emails and spreadsheets, which gets disorganized, wastes time, and results in remediation tasks falling through the cracks. Fortunately, it's common for IT Ops, DevOps, and other remediation teams to use sophisticated work management platforms for managing requests within their domains. As those teams have turned to work management platforms to structure their work, you should as well.

For many large organizations, routing requests means submitting tickets on platforms like Jira, ServiceNow, Asana, Slack, and Monday.com. The security team needs to route the remediation request to the appropriate team in the work management platform they use, providing clear instructions and relevant context for the task. Using native work management tools for remediation routing may sound simple, but it can become complex when coordinating across multiple platforms.



05

RECEIVE

Receive and Accept Responsibility

The fixing party receives the request (in their preferred platform), and then accepts responsibility for remediation. Unique cases may need a different team to take action, or the request might need to be denied outright. As part of your remediation process, outline how the fixing team can accept, clarify, reassign, or reject requests if necessary, and track the status

- **Accept:** Owner accepts responsibility for remediation action
- **Delay:** Request needs to be delayed and re-evaluated at a future time
- **Reassign:** The task needs to be performed by a different individual or team
- **Reject:** The request will not be fulfilled
- **Clarify:** The request is unclear, or needs additional context

06

REMEDIATE

Remediate the Vulnerability

Everything up until this point is meant to prepare for, expedite and facilitate remediation. The actual remediation process and time varies depending on the task, but remediation teams should seek to perform this with minimal disruption to regular business operations. Structuring and automating the preceding tasks to remove friction and uncertainty will go a long way toward helping remediation teams focus on their remediation work.

Validation plays a critical role in confirming that the vulnerability has been successfully eliminated and that the previously at-risk system now operates securely. It typically involves retesting and verification to ensure that the vulnerability no longer exists, and that the remediation has not introduced new issues.

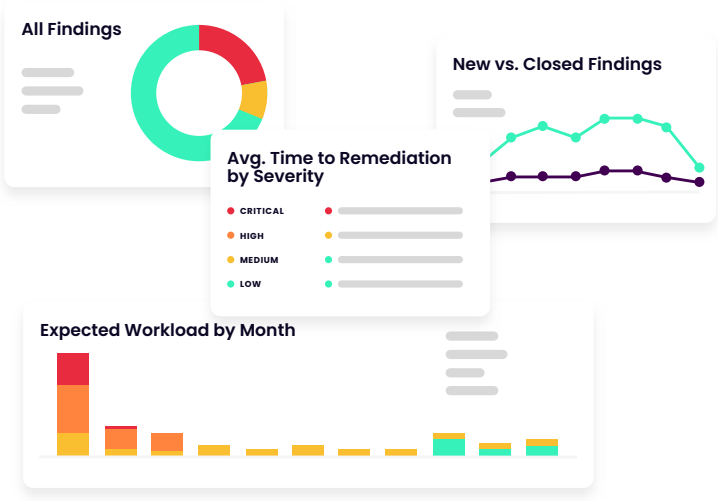
The fixing party receives the request (in their preferred platform), and then accepts responsibility for remediation items such as:

- Patch Management
- Configuration Hardening
- Access Control and Permissions
- Network Segmentation
- Incident Response
- Code Refactoring
- Risk Acceptance
- Workarounds
- Web Application Firewall Rules
- Data Encryption

07

REPORT

Report the Remediation Status



With a structured and automated Remediation Operations process in place, reporting on remediation progress, process compliance and whether service level agreements are being met is straightforward. This includes reporting completed remediation requests on applicable platforms, and documenting the steps taken during remediation. Careful and organized documentation helps with compliance, future audits, and tracking associated changes to code, software, and systems.

Conclusion

Effective Remediation Operations provide a structured, repeatable set of processes that deliver a clear roadmap for reducing risk and addressing risk consistently and comprehensively. It ensures that no critical steps are overlooked and allows for the efficient allocation of resources. Additionally, by carefully monitoring progress throughout the remediation process, organizations can swiftly identify deviations, track effectiveness, and make informed adjustments as necessary. This proactive approach enhances the speed and accuracy of remediation efforts and enables organizations to maintain an adaptable security posture.

If your organization keeps getting stuck in remediation quicksand, we invite you to learn how our advanced Remediation Operations Platform can seamlessly consolidate, automate, coordinate and report on your remediation efforts.

Visit us at seemplicity.io to learn how we help businesses:

01 Accelerate cross-domain risk reduction

02 Enhance visibility

03 Increase accountability

04 Streamline remediation processes