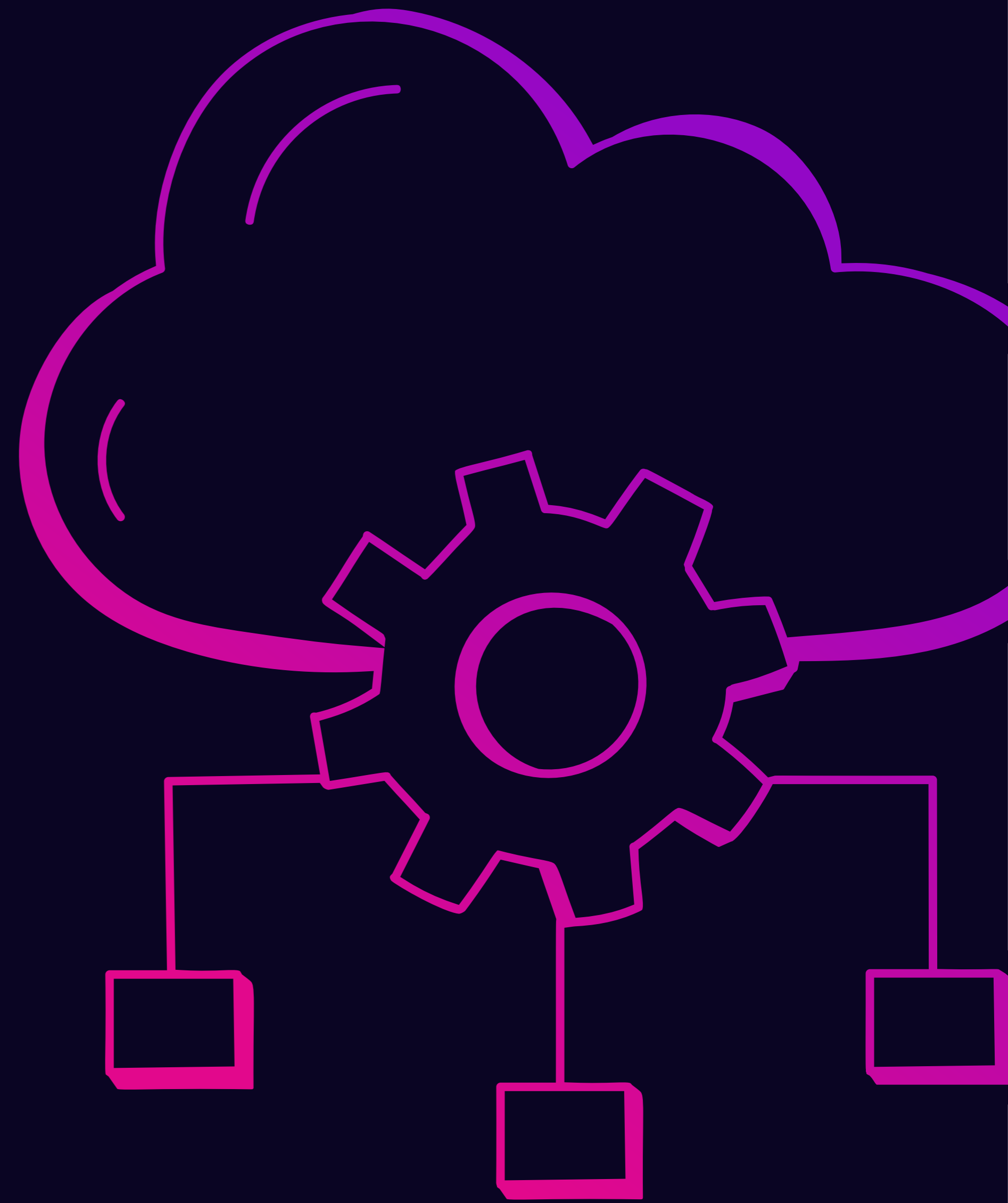


# Streamlining DevSecOps

Remediation Plans  
that Minimize Disruption

EBOOK



This eBook offers practical insights and actionable steps to help senior development executives navigate the complexities of modern DevSecOps and adopt Remediation Operations (RemOps) to ensure smoother workflows and more efficient security practices.

Senior engineering managers face the difficult task of embedding security into software development workflows without sacrificing speed or agility. DevSecOps emerged to bridge the gap between traditional development approaches and evolving security requirements, enabling organizations to integrate security within the continuous integration and delivery (CI/CD) cycle. Yet, as security demands increase, development teams are left with the challenge of ensuring that security checks don't bottleneck production. Balancing security needs with the push for rapid releases has become a critical, often overwhelming, responsibility for leaders in development.

A smart, structured approach to vulnerability and exposure RemOps offers an elegant and scalable path forward, allowing development managers to streamline remediation while keeping developers focused on core work.

By recasting vulnerability management as an enabler of agility and security rather than a source of friction, engineering leaders can protect software integrity without slowing progress.



## THE STATE OF DEVSECOPS TODAY

Integrating security into software development is no longer optional. DevSecOps addresses the critical need for embedding security into the CI/CD pipeline, ensuring that security practices align seamlessly with development goals. However, achieving such alignment is met with many challenges.

Development managers face systemic issues such as the overwhelming volume of findings, excessive noise of redundant findings, the manual triaging of vulnerabilities and synchronizing security efforts alongside rapid development cycles. Moreover, development and security teams often work with competing perspectives. This lack of alignment and cohesion can lead to bottlenecks and inefficiencies.

Balancing speed and security has become a persistent challenge for senior development managers. Without a cohesive strategy, organizations risk compromising both innovation and application security.



## VULNERABILITY MANAGEMENT THROUGH A DEVELOPER'S LENS

For development teams, the promise of DevSecOps often feels like a double-edged sword. While integrating security into workflows is essential, it brings unique challenges that disrupt productivity and impede innovation. The day-to-day reality of vulnerability management is marked by never-ending backlogs, endless prioritization tasks, and constant cross-functional coordination - responsibilities that can quickly overwhelm even the most efficient teams.

As DevOps practices push for faster release cycles, vulnerabilities accumulate rapidly, creating an overwhelming backlog that can obstruct productivity and stymie agile development goals. The challenge is compounded by the need to coordinate between teams, each with different perspectives on prioritization and risk. This tension often leads to delays in remediation and duplicated efforts, with vulnerabilities falling into the gaps between departments when ownership is unclear.

Adding to the complexity, many security findings lack actionable insights. Various tools use different scoring scales, and there is often a lack of context, making it difficult for developers to understand what requires immediate attention versus what can wait. This excessive noise means teams waste valuable time manually triaging issues instead of addressing them.

Development managers need a streamlined approach to vulnerability management - one that integrates with existing development processes and empowers teams to address security in stride. By simplifying how vulnerabilities are consolidated, prioritized, and assigned, they can avoid getting mired in the details of every issue, allowing their teams to focus on building and delivering well-built, secure software at speed.



# WHAT IS REMEDIATION OPERATIONS (REMOPS)?

RemOps is a structured approach to vulnerability management that streamlines security processes, automates workflows, and clarifies accountability across development, operations and security teams. At its core, RemOps aims to eliminate the inefficiencies and bottlenecks that plague traditional vulnerability management, enabling organizations to address security threats without disrupting development velocity.

## The Definition of RemOps

RemOps encompasses the orchestration and automation of cybersecurity processes required to identify, prioritize, assign, and resolve vulnerabilities. It acts as a bridge between security and development teams, ensuring that remediation becomes a proactive and integrated part of the software development lifecycle (SDLC) rather than a reactive, ad-hoc effort.

## The Core Principles of RemOps

### CONSOLIDATION OF FINDINGS

RemOps aggregates security findings from multiple tools and domains into a single, unified source of truth. By deduplicating redundant findings, normalizing formats and transforming multiple findings into a single fix, teams gain clarity on the most critical risks and can focus their efforts accordingly.

### AUTOMATION OF WORKFLOWS

With RemOps, manual triaging and task assignments are replaced by automated processes. Vulnerabilities are prioritized based on tailored rules and routed directly to the appropriate teams or individuals within tools like Jira, Azure DevOps or ServiceNow, ensuring seamless integration into existing workflows.

### CLEAR ACCOUNTABILITY

RemOps establishes clear ownership for remediation tasks by assigning vulnerabilities to the right stakeholders. This eliminates confusion about who is responsible for addressing specific issues and ensures that nothing falls through the cracks. By tracking progress against SLAs, teams are held accountable for timely and effective remediation.

### PROACTIVE, CONTINUOUS EXPOSURE MANAGEMENT

Instead of waiting for vulnerabilities to pile up, RemOps promotes a proactive approach where points of exposure are addressed continuously and in stride with development processes. This minimizes security debt and reduces the risk of critical vulnerabilities being overlooked.



# THE IMPORTANCE OF EFFICIENT REMEDIATION OPERATIONS IN DEVSECOPS

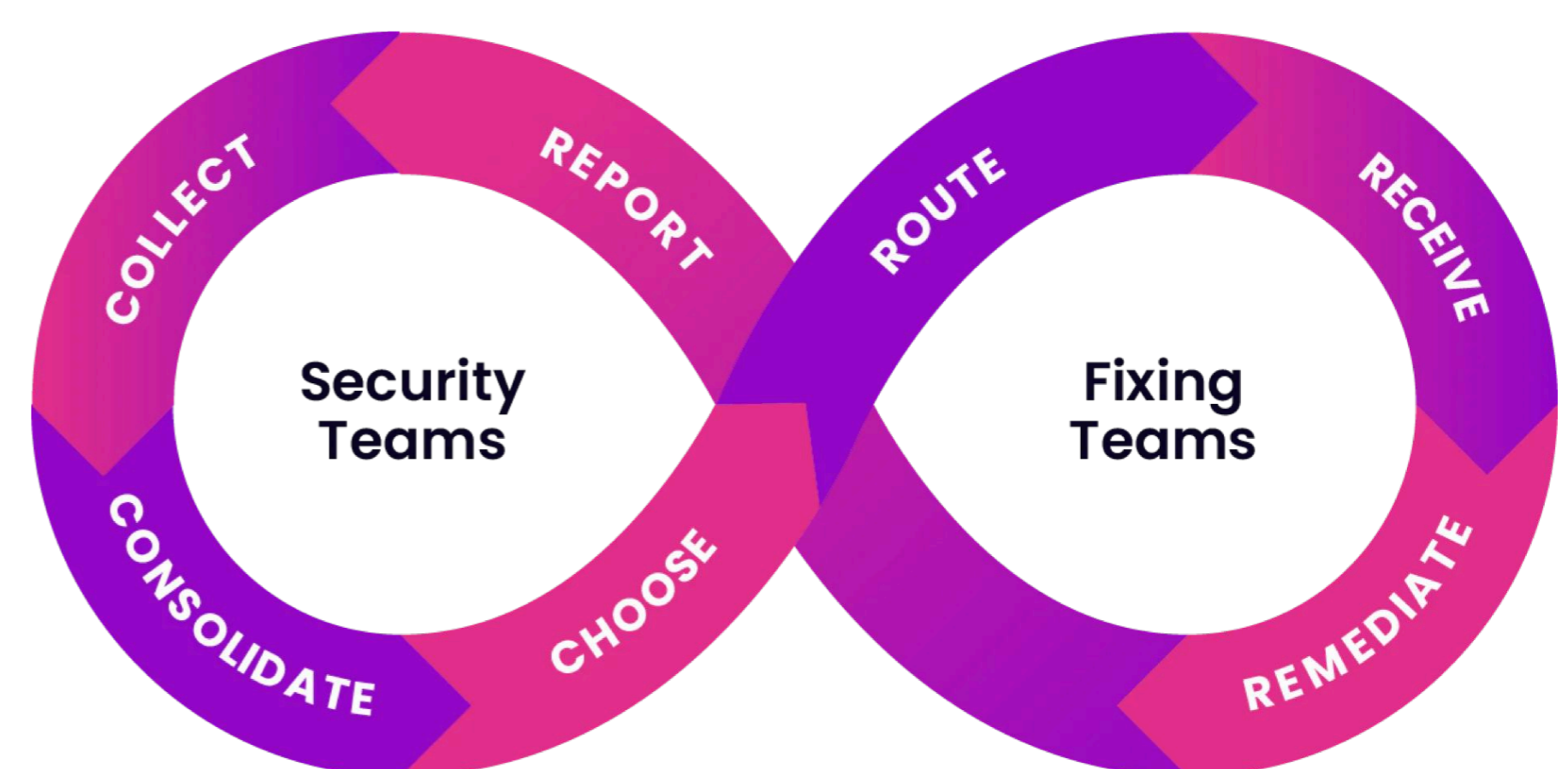
RemOps addresses the challenges of traditional vulnerability management by transforming remediation into a streamlined, automated process, reducing redundant efforts and ensuring security efforts don't disrupt development progress. Rather than treating remediation as a separate, siloed activity, RemOps integrates it as a component of software delivery, shifting to a more proactive approach.

With RemOps, security findings are consolidated and deduplicated from multiple sources, giving teams a clear, unified view of vulnerabilities without the noise of repetitive findings. This proactive system clarifies ownership by assigning tasks directly to designated teams, eliminating confusion and enhancing accountability. Furthermore, automation ensures that remediation tasks flow seamlessly into platforms development and operations teams are already using, keeping security actions aligned with DevOps pipelines. By minimizing manual intervention, RemOps allows development leaders to maintain momentum while managing risk, enabling teams to focus on innovation and delivery with confidence.

In addition to streamlining processes, RemOps fosters better collaboration between development and security teams. Developers are empowered to act on clearly prioritized tasks, while security teams gain confidence that vulnerabilities are being managed systematically. This alignment eliminates friction and ensures that security and development goals work hand in hand to deliver secure software.

## REMOPS IN ACTION

RemOps provides organizations with a clear, repeatable process for integrating security into development workflows. The seven key steps to a successful approach are:



### STEP 1 | Collect Security Findings

The first step in RemOps is systematically gathering vulnerability findings from security testing and scanning tools in CI/CD pipelines and other security sources. This comprehensive approach ensures that all potential risks across on-premises, cloud, and hybrid environments are identified, eliminating blind spots and establishing a strong foundation for further steps.

## **STEP 2 | Consolidate, Deduplicate, and Aggregate Findings**

Once security findings are collected, the next step is to organize and refine them. Consolidating data from multiple tools into a single source of truth simplifies decision-making. Deduplication eliminates redundant alerts, while aggregation organizes vulnerabilities by common fix. This step creates clarity, giving managers a unified, clutter-free view of risks, cutting down on alert fatigue and enabling a clear focus on what truly matters.

## **STEP 3 | Choose - Define Priorities and Ownership**

Effective remediation begins with knowing what to remediate, and who needs to do it. Knowing what to focus on first requires clear prioritization based on risk level, business impact, threat intelligence feeds and other internal and external factors. This prevents teams from wasting time on low-risk issues and aligns remediation efforts with organizational priorities. Equally important is defining ownership for each remediation task, ensuring that every vulnerability is assigned to the appropriate development team or individual. Documenting these decisions reduces confusion and accelerates response times.

## **STEP 4 | Route - Automate Workflows**

Automation is the backbone of an efficient RemOps framework. By automatically routing specific tasks directly to developers' work queues within the tools they already use, like Jira, RemOps eliminates manual back-and-forth, ensuring each vulnerability is assigned without error or delay.

## **STEP 5 | Receive and Accept Responsibility**

Assigned developers must acknowledge and accept responsibility for their remediation tasks, or flag exceptions. This step involves validating the assignment, clarifying details if needed, and ensuring alignment on what needs to be addressed. Clear accountability mechanisms, such as defined service-level agreements (SLA), ensure that all stakeholders remain engaged and proactive.

## **STEP 6 | Remediate**

While a RemOps platform doesn't directly perform the remediation, it provides development teams with everything they need to act swiftly. By delivering timely, actionable information - such as detailed vulnerability data and relevant context - RemOps enables teams to execute fixes and note exceptions with minimal disruption to their workflows. For instance, when facing a high-profile vulnerability like Log4j, a manager can rely on their RemOps tooling to streamline the response efforts, from initial alert to final remediation, keeping development on track and secure without sacrificing speed.

## **STEP 7 | Report and Track Progress**

Continuous tracking and real-time reporting provides a transparent view of remediation progress, process efficiency and SLA compliance. This allows managers to evaluate their remediation processes, identify areas for improvement and ensure that vulnerabilities are being addressed effectively.

When applied cohesively, these seven steps transform remediation operations into a streamlined, proactive process that aligns security with development goals.



## REALIZING THE BENEFITS OF STREAMLINED VULNERABILITY MANAGEMENT

A RemOps platform provides a strategic advantage for development leaders, streamlining the vulnerability management process so teams can maintain focus on high-quality, rapid delivery without being bogged down by security roadblocks. The tangible benefits of streamlined vulnerability management, empowered by RemOps, include:

### ✓ ENHANCED PRODUCTIVITY ACROSS TEAMS

Traditional vulnerability management often pulls developers away from their core work, reducing overall productivity. A streamlined approach eliminates redundant tasks, minimizes manual intervention, and ensures that teams spend their time addressing the most critical issues. With automated workflows and clear prioritization, developers can focus on delivering reliable software without the burden of noise and inefficiencies. This approach transforms vulnerability management from a reactive, fragmented effort into a proactive, integrated process that aligns seamlessly with existing DevSecOps workflows, reducing friction across the board.

### ✓ FASTER TIME-TO-REMIEDIATION

Time is of the essence when it comes to addressing vulnerabilities. Delays not only increase security risks but also create additional pressure on development teams. RemOps accelerates the remediation process by eliminating much of the manual overhead that slows development progress. This significantly reduces the time it takes to identify, prioritize, and resolve vulnerabilities, helping developers stay ahead of risks.

### ✓ IMPROVED COLLABORATION BETWEEN TEAMS

Cross-functional communication capabilities and a single system of record foster better collaboration between security and development, bridging cross-team gaps and clarifying accountability. Development teams are empowered to act on clearly defined tasks, while security teams gain confidence that vulnerabilities are being addressed systematically. This alignment reduces friction and builds trust between teams, ensuring that security objectives support, rather than hinder, development goals.

## ✓ REDUCED RISK AND ENHANCED SECURITY POSTURE

Streamlined processes enable developers to address vulnerabilities proactively, preventing them from escalating into larger issues. By eliminating manual errors, reducing security debt, and ensuring continuous tracking of remediation efforts, organizations can maintain a stronger security posture.

## ✓ LONG-TERM EFFICIENCY AND SCALABILITY

As organizations grow and their security needs evolve, RemOps scales with them. Automated workflows, centralized data, and clear processes ensure that vulnerability management remains efficient even as the volume and complexity of security findings increase. This long-term efficiency enables engineering managers to handle future challenges without overburdening their teams.

## Conclusion

For development managers and executives looking to enhance team productivity and reduce disruptions from security issues, exploring a RemOps platform and its fit within their DevSecOps practice is a critical step forward. By implementing streamlined vulnerability management practices, managers not only improve their security posture but also enable a smoother, more agile development environment that's resilient to the challenges of modern security demands.

RemOps fits seamlessly in DevSecOps environments. It consolidates and prioritizes security findings, automates workflows, and establishes clear ownership, enabling development teams to tackle vulnerabilities efficiently. This proactive, integrated approach reduces risk, enhances productivity, and allows organizations to maintain the speed and agility required in today's fast-paced development environments.

Seemplicity's RemOps platform is designed to support software development's unique needs and goals. Through AI-powered tailored remediation plans, Seemplicity's RemOps platform accelerates risk reduction, empowering development teams to focus on delivering innovation securely and at speed.



To learn more about how **Seemplicity can transform your vulnerability and exposure management process**, read our solution brief and take the first step towards streamlined DevSecOps.

GET SOLUTION BRIEF 

