mondoo
Fix Now. Fix Forever.

2025 State of **Vulnerability Remediation**

Uncovering challenges, gaps, and the path forward

Published October 2025

Table of Contents

Abstract: Vulnerability remediation, which is essential for robust cybersecurity, can be a challenging workload. This report, based on a survey of IT operations and security professionals, explores the current state of remediation. It was commissioned by Mondoo, the pioneer in Agentic Vulnerability Management, and conducted by Virtual Intelligence Briefing. The report highlights problems facing remediation teams, such as tool sprawl, low confidence, alert fatigue, recurring vulnerabilities, and lack of visibility and detail, as well as issues like automation.

Foreword

Soo Choi, CEO and Co-Founder at Mondoo

"Bad actors are using AI to launch attacks faster than ever. Many organizations are still hesitant to automate processes for remediating vulnerabilities, but in an AI-driven world, slow defenders get left behind, and, let's face it, breached. At Mondoo, we understand that effective vulnerability remediation is not just about identifying threats, but about successfully eliminating them and preventing their recurrence so attackers can't exploit them. For this reason we commissioned this report to shed light on the current state of vulnerability remediation, uncovering the significant challenges, but also the promising pathways forward. I hope you enjoy reading the report and that it provides useful insights to help you further optimize your vulnerability remediation efforts."

Introduction

Vulnerability remediation is essential for maintaining a strong security posture. If not resolved quickly enough, vulnerabilities create risk exposure, in some cases catastrophic. Getting it right is not easy, however. This report, based on a survey of IT operations (IT ops) and security professionals, reveals that remediation is challenging across multiple dimensions, with organizations experiencing pain due to tool sprawl, alert fatigue, the recurrence of vulnerabilities, and cyber incidents resulting from remediation delays.

While most of the organizations covered by the survey reported relatively rapid remediation, the level of confidence in their remediation capabilities was low. Respondents were aware that they need better coordination and visibility, along with better information—and, perhaps most importantly, workflow automation to reduce the remediation gap.

Respondent demographic summary

This report is based on a survey of 125 IT and security professionals:

Manager level	**62%** work at the manager level and **19%** at the director level.
Medium-Sized	The companies represented are small to medium-sized, with **32%** employing between 501 and 1,000 people and **32%** employing between 251 and 500.
IT Ops and Security	**42%** work primarily in IT operations, **15%** in security, and **42%** work in both IT ops and security.
North America	**96%** are in North America, 2% work in the DACH region of Switzerland, Germany, and Austria, and 2% from Europe.
Range of Industries	Respondents come from a range of industries. The most represented were **manufacturing (42%), technology (26%),** and **finance (16%).**

The full survey demographics are listed in the appendix.

A brief overview of vulnerability remediation

Vulnerability remediation is a process that involves identifying and addressing security problems in software and other IT systems that make them vulnerable to cyber threats. Examples include unpatched operating systems and malicious code inserted into applications through the software supply chain. The vulnerability remediation workload typically spans the IT ops and security teams. Since there are tens of thousands of new vulnerabilities introduced each year, it's simply impossible to fix all of them. For most organizations, the goal is to identify the most serious vulnerabilities and prioritize them for proactive remediation to reduce the risk of breaches and outages.

Key Insights

REMEDIATION WORKFLOWS ARE STILL LARGELY MANUAL: 62% of respondents have manual remediation workflows, and only 2% are fully automated. Manual processes make it extremely hard to keep up with the thousands of vulnerabilities that are constantly being discovered and defend against bad actors using AI to launch attacks at machine speed.

REMEDIATION REPORTING IS AD HOC AND INFREQUENT: 52% of respondents say they report 'quarterly', 'rarely', or 'never' on their remediation efforts. Only 18% run weekly reports. 39% of respondents don't use a vulnerability remediation tracking tool, and have to rely on manual tracking using spreadsheets. Without regular reporting, it's very difficult to track progress, manage risk, and ensure accountability.

TOOL SPRAWL CAUSES LOWER REMEDIATION CONFIDENCE: Respondents that experience tool sprawl reported 51% lower remediation confidence than those that didn't. This is likely because the more tools need to be managed, the more difficult it is to get a unified view into vulnerability remediation across the entire IT infrastructure, leading to lower confidence.

RECURRING VULNERABILITIES ARE A COMMON ISSUE: 40% say more than 5% of vulnerabilities recur, with 44% saying vulnerabilities are reintroduced during redeployment. Not fixing the root cause of issues is likely a driver of vulnerability recurrence, given that vulnerabilities not fixed in IaC or containers are bound to recur.

MOST ORGANIZATIONS DON'T USE REMEDIATION SLAS: 60% of respondents don't have any remediation SLAs, and of those that track SLAs, 65% have to analyze data manually. Tracking remediation SLAs is crucial for reducing security risk because they help ensure vulnerabilities are fixed promptly, so that compliance requirements are met and critical issues are fixed before attackers can exploit them.

MOST ORGANIZATIONS FIX CRITICAL VULNERABILITIES IN UNDER 3 DAYS: 71% of organizations claim they remediate critical vulnerabilities within 24–72 hours. Considering that CISA's requirement is to fix critical vulnerabilities within 15 days, this is a good result. However, when taking into account the low remediation confidence level and lack of SLA tracking, it's possible that the actual time may be somewhat longer.

LACK OF REMEDIATION GUIDANCE IS A MAJOR PAIN POINT: Lack of access to remediation steps and code (42%), as well as details on the asset and precise location of vulnerabilities (37%), slows down remediation and causes friction between IT ops and security teams.

LACK OF CONFIDENCE IN REMEDIATION ABILITIES: Only 9% of respondents are 'very confident' in their remediation capabilities. The reason for this low confidence can be caused by technical, organizational, and procedural issues that overwhelm and hinder security teams. Lack of regular reporting and SLA tracking means that it's difficult to understand remediation progress and risk exposure.

ALERT FATIGUE IS BIGGEST REMEDIATION PAIN POINT: 53% say alert fatigue is a significant remediation pain point, followed by too many tools (40%), and not enough visibility (40%). Alert fatigue happens when teams are overwhelmed by alerts, many of which are irrelevant, duplicate, or false positives, creating a desensitization that makes it difficult to distinguish real dangers from background noise. Alert fatigue can lead to missed critical threats and burnout.

MORE INFORMATIVE TICKETS WILL PROVIDE BIGGEST REMEDIATION IMPROVEMENT: 44% say auto-creating tickets with all relevant information will improve remediation. Including detailed asset information, guided remediation steps, and code snippets in vulnerability remediation tickets means that developers understand the specific context, reason why the vulnerability needs to be remediated, and have all the technical details they need to quickly and effectively fix security issues.

Report findings

The survey reveals that organizations are struggling with vulnerability remediation. They have an excess of siloed tools and manual processes. Responsibility for the workload is typically shared, but the combination of the security and IT ops teams is neither catching all the vulnerabilities nor remediating them.

1 Companies are dealing with tool sprawl

Companies covered by the survey use an abundance of security tools. Almost half use more than five tools. This "tool sprawl" may be due to an accompanying sprawl of applications, clouds, and endpoints that are covered by separate tools. Whatever the cause, though, the need to stay on top of so many tools, each of which may handle vulnerability remediation in its own domain, is stressful and works against efficiency, visibility, and completeness in remediation.

Additionally, respondents with tool sprawl are more likely to report low confidence in remediation: 53% of respondents experiencing tool sprawl reported low confidence in remediation, versus only 35% of respondents not experiencing tool sprawl. That means that tool sprawl reduces the confidence in remediation by 51%.

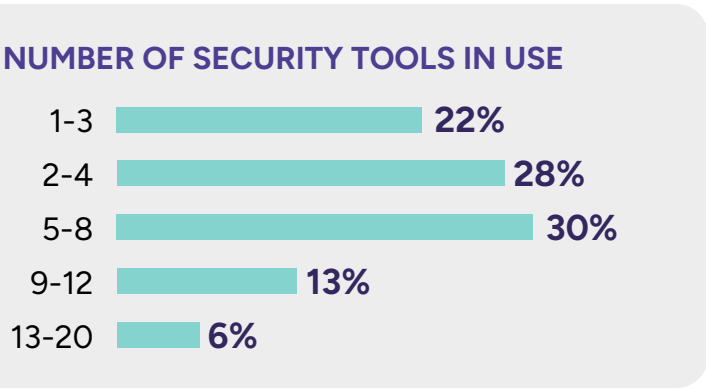
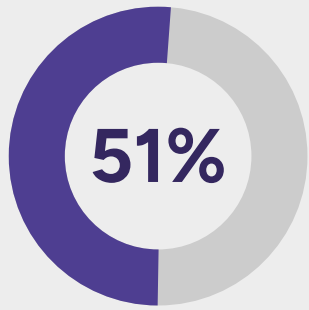


Figure 1 – Responses to the question, "How many security tools are you using across your cloud, on-prem, SaaS, endpoints, and software development life cycle environments?"



lower confidence in remediation when experiencing tool sprawl

2 Many still rely on manual processes for remediation tracking

When it comes to tracking vulnerability remediation, surprisingly, a third of respondents said they used manual processes, such as spreadsheets for this purpose. The next most popular tracking tool was the Atlassian Suite/JIRA (used by 27% of respondents). JIRA has automation capabilities, but other findings in this survey suggested that use of JIRA is largely manual. The same is probably true for Azure DevOps (14%).

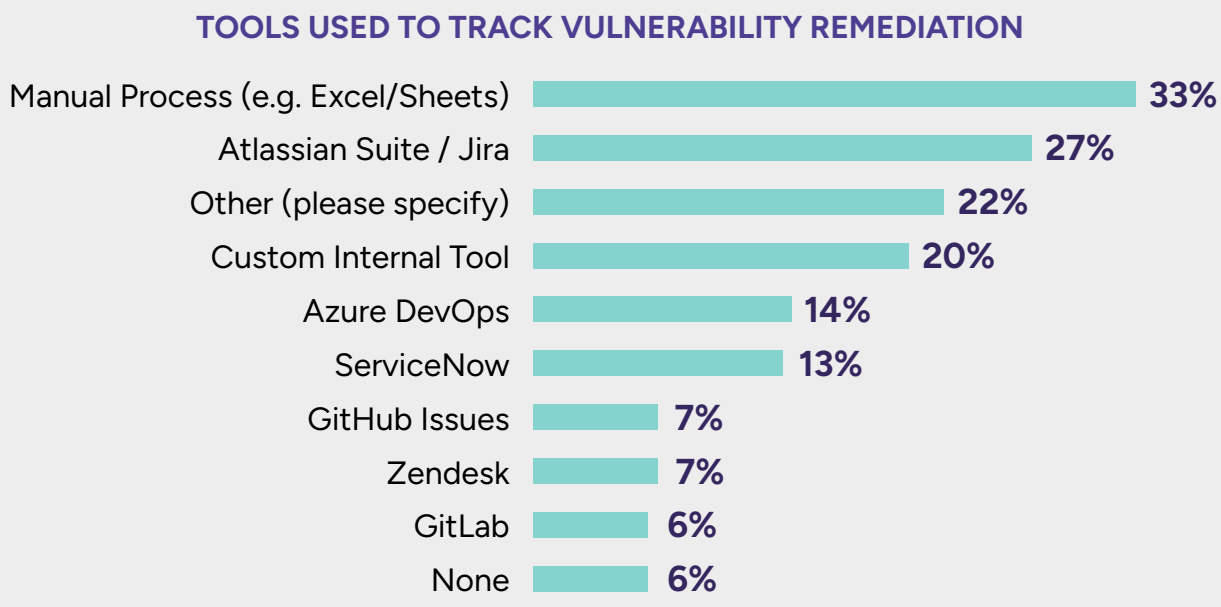
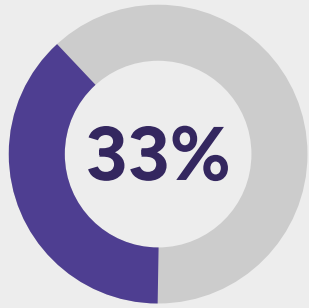
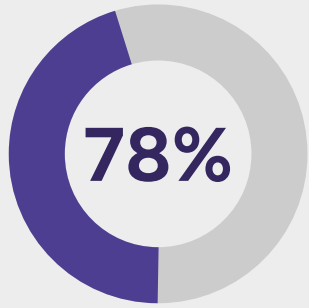


Figure 2 - Responses to the question, "What tools do you use for tracking vulnerability remediation?"

Asked separately to select which tool their organization uses, 57% chose Microsoft Intune. This was the most popular choice by a wide margin. Intune integrates with Microsoft Defender for vulnerability management. Its predominance suggests a focus by IT ops on vulnerability remediation for endpoints.



use manual processes to track vulnerability remediation



estimate < 5 vulnerabilities per machine per month

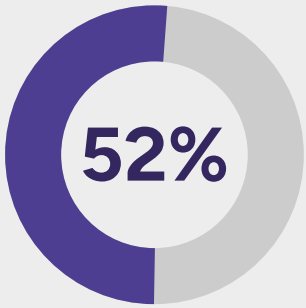
3 Not all vulnerabilities get detected...

Seventy-eight percent said they found fewer than five vulnerabilities per machine per month. Ten percent said 6-10 vulnerabilities, and only 11% said they found more than 10 vulnerabilities per machine, per month. The number of detected vulnerabilities will vary based on a number of factors, including detection ability, vulnerability recurrence, existence of shadow IT, asset type, and more. Based on Mondoo's experience with clients, it is likely that there are significantly more vulnerabilities present, but they're probably not all being detected.

4 Remediation responsibilities are mostly shared by IT and security teams

Who is responsible for vulnerability remediation? At 46% of companies, it's a shared responsibility between security and IT ops teams. This arrangement makes sense, given that security teams often lack the personnel and skills to do the remediation work. IT ops usually "owns" the systems in question, anyway. For 28%, IT ops is primarily responsible for remediating vulnerabilities and misconfigurations reported by security. Just 14% say that security is primarily responsible.

Who is primarily responsible for remediating vulnerabilities and misconfigurations reported by security?



report quarterly, rarely, or never on their remediation efforts

5 Frequency of remediation tracking and reporting is low

The organizations surveyed do not track and report their remediation efforts frequently. Just 18% do it weekly, and 30% are reporting monthly. Over half (52%) are reporting either "quarterly", "rarely," or "never." These results suggest an overall lack of awareness of how well remediation is going and little clarity on the remediation of high-priority vulnerabilities.

6 Organizations experienced breaches due to delayed remediation

Nearly one in ten respondents said their organizations have experienced a security incident due to a delay in vulnerability remediation. Although 9% represents a significant number, it is likely that the actual number is higher. The 9% finding does not align with industry research that suggests that many breaches occur due to the exploitation of unpatched systems. The cohort surveyed here may be good at remediating the most urgent vulnerabilities, so their risk exposure is lower than the norm.

7 Vulnerability remediation pain points

Vulnerability remediation can be a stressful workload. Challenges range from a lack of information about vulnerabilities to siloed information and "alert fatigue," the most common pain point cited by 54% of respondents. This condition results from people having to respond to an excessive number of security alerts, including for vulnerabilities. Overwhelmed with notifications, people may struggle to prioritize or even get to potential security risks. Other notable pain points include "too many siloed tools" (40%) and "not enough visibility" (40%).

The latter two issues reflect inefficient and inadequate security workflow design. Bigger picture, the survey reveals the lack of a systematic, feedback-based remediation cycle. There's no single source of truth connecting runtime changes, CI/CD pipelines, and incident data.

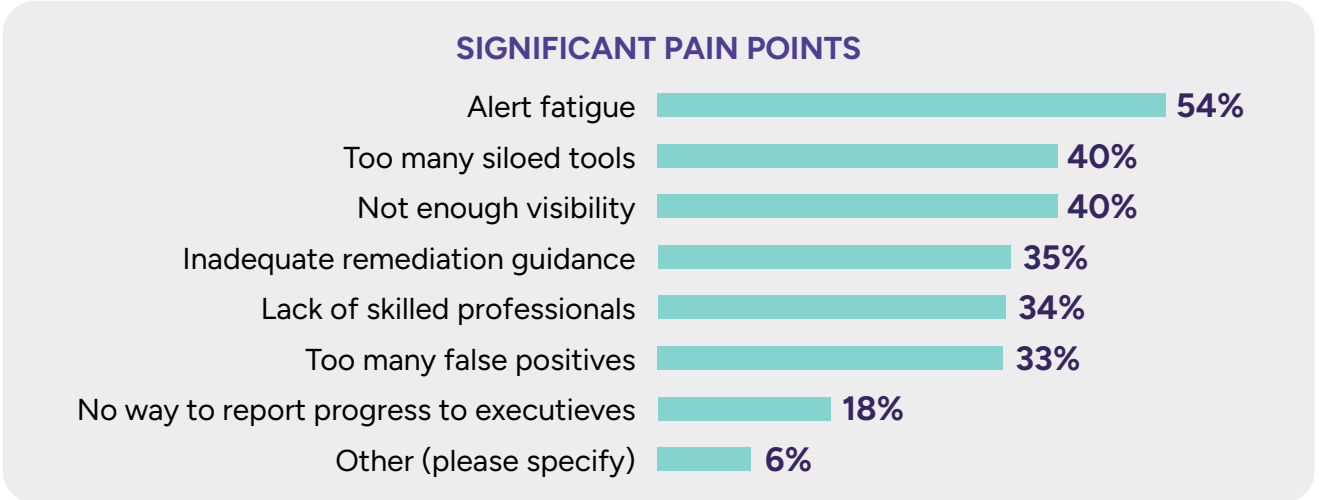


***Figure 3** - Responses to the question, "Which of the following do you consider to be significant pain points?"*

Asked, "What are the biggest pain points for remediating vulnerabilities and misconfigurations reported by security?" 44% said "manual effort needed to find the owner of an artifact and fix it." It is not always clear who owns the system or component that requires remediation, e.g., is it the developer who wrote the code or the admin who controls the runtime environment? Manual efforts to identify artifact owners can lead to delays and wasted cycles.

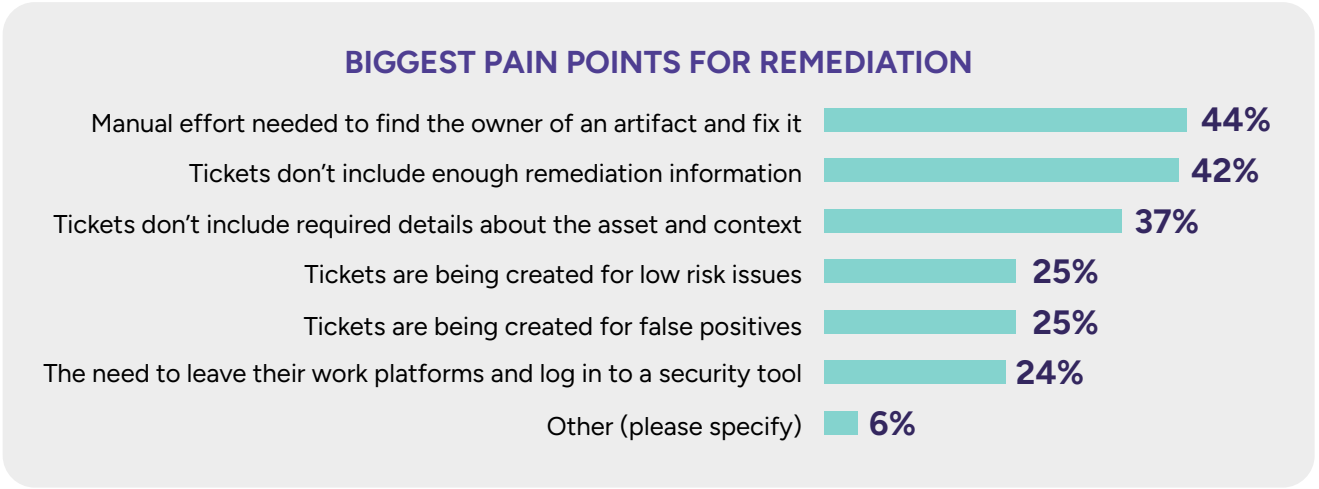
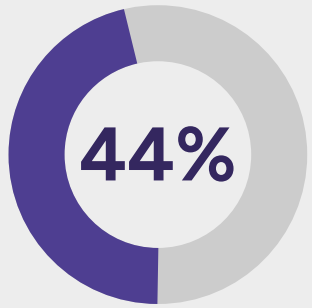


Figure 4 *- Responses to the question, "What are the biggest pain points for remediating vulnerabilities and misconfigurations reported by security?"*

A related problem is when tickets don't include enough remediation information (cited by 42%) or lack details about the asset and context, e.g., this vulnerability has a high priority because it is exposing a business-critical system to risk of breach.

The complaint that tickets are "being created for low-risk issues" or "being created for false positives" (each cited by 25%) underpins the experience of alert fatigue. If people have to spend time processing meaningless alerts, that's a frustrating waste of time - time that could be spent on remediating the actual critical vulnerabilities.

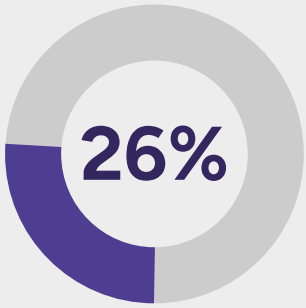
Platform fragmentation is an associated difficulty. This occurs when remediation requires people to leave their work platforms to access security tools, disrupting their regular workflows and diminishing productivity. Switching tasks can even lead to morale problems among developers.



listed "manual effort needed to find the owner of an artifact and fix it" as one of the biggest pain points for remediation

8 Vulnerability recurrence: even a small number is too many

Vulnerabilities have a bad habit of coming back after being remediated. Although at first glance the numbers don't seem that high, with 60% of respondents reporting that fewer than 5% of vulnerabilities and misconfigurations recurred within a month of remediation. Twenty-six percent said the number was between 6% and 10%, and 11% even said between 11% and 30%.



say that between 6% and 10% of vulnerabilities recur

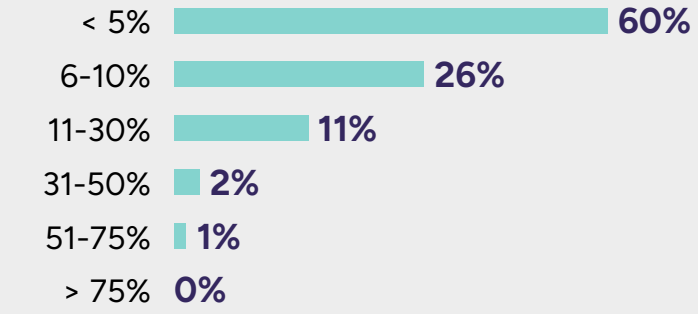
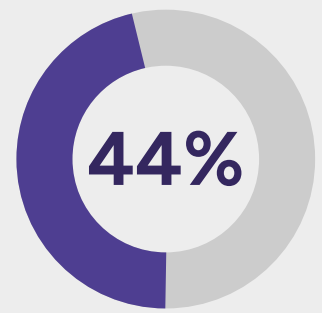


***Figure 5** – Responses to the question, "What percentage of vulnerabilities/ misconfigurations recur within a month of remediation?"*

The reality is that any number of recurrences is too high. Each time a vulnerability fails, it triggers a disruptive workflow that diverts everyone from their current priorities and forces them to spend time on something they hadn't planned on doing, and creates new opportunities for attackers to infiltrate the environment.

Operational factors drive recurrence

The reappearance of a vulnerability can come from a variety of causes. In some cases, the redeployment of software causes the reintroduction of the vulnerability (cited by 44%). This issue is actually a reflection of problems elsewhere in the remediation process, such as vulnerabilities being fixed in runtime, but not in the source code (34%), and a lack of scanning of CI/CD processes affecting source code. A solution may be available for this last issue. An analysis of free text responses finds that teams using GitOps or infrastructure-as-code (IaC) for CI/CD appear better equipped to sustain remediations.



say vulnerabilities are reintroduced during redeployment

Rollbacks of patches, which are sometimes necessary for operational reasons, also cause vulnerability recurrence (cited by 35%). This may occur if IT ops teams need more information on dependencies between software applications and need to undo a patch in order to examine the situation before trying the patch again.

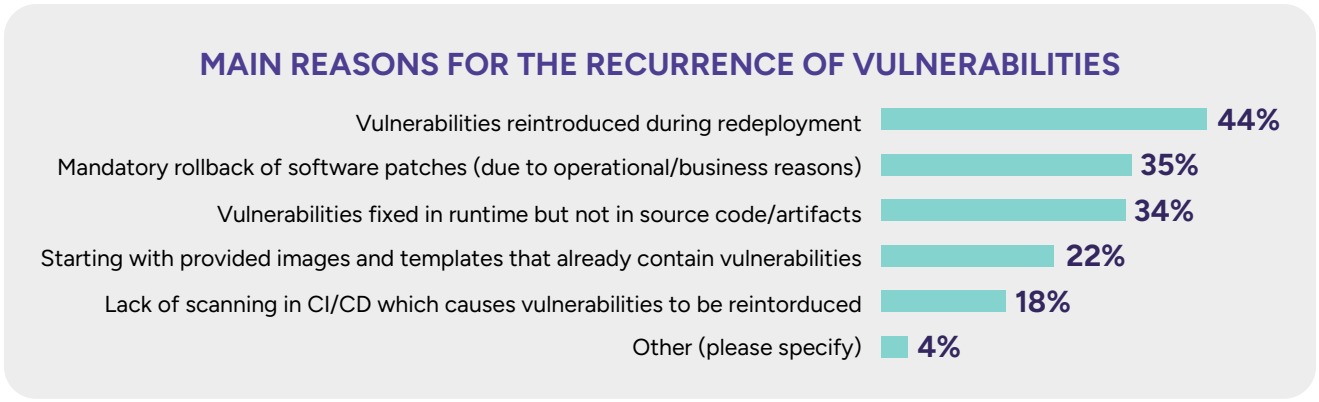


Figure 6 *- Responses to the question, "What, in your opinion, are the main reasons why they recur?"*

9 Confidence in remediation is relatively low

Fewer than one in ten respondents were "very confident" in their ability to remediate known vulnerabilities in a timely manner. Forty-three percent were either "slightly confident" or "not confident at all." These findings should not be surprising. The concerns about tool sprawl, alert fatigue, cumbersome processes, and a lack of visibility align with low confidence.

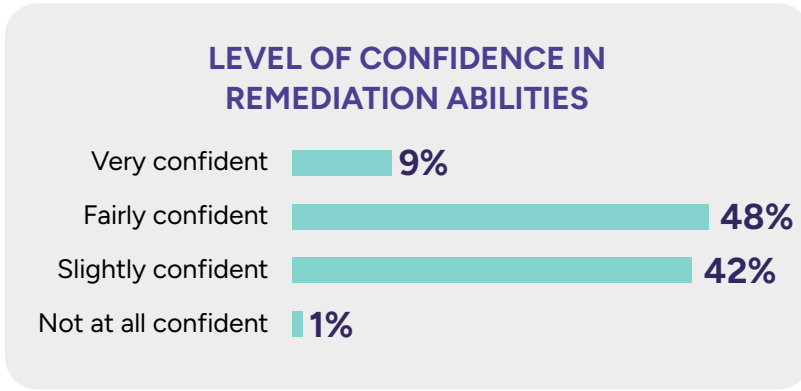
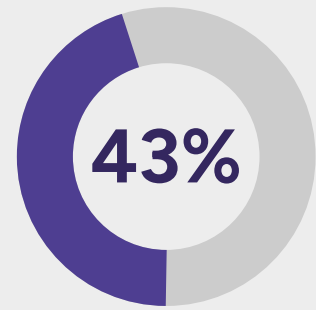


Figure 7 *– Responses to the question, "How confident are you in your organization's ability to remediate known vulnerabilities in a timely manner?"*



are "slightly confident" or "not confident at all" in their remediation abilities

10 The outlook is optimistic

Confidence may be lacking, but the outlook is optimistic. Asked, "Do you believe your organization is improving in its ability to remediate vulnerabilities?" a striking 91% said they either "agreed" or "strongly agreed." What's driving this? Tracking and reporting may be a driver of confidence and a positive view of the future. Teams that report monthly or weekly are twice as likely to report confidence and improvement as others.

11 How high-confidence teams act

Teams that expressed a high level of confidence in their remediation did the following:

- **Tracked remediation coverage regularly, e.g., weekly or monthly**
- **Reported fewer rollback events**
- **Emphasized coordination between Dev, Sec, and Ops**

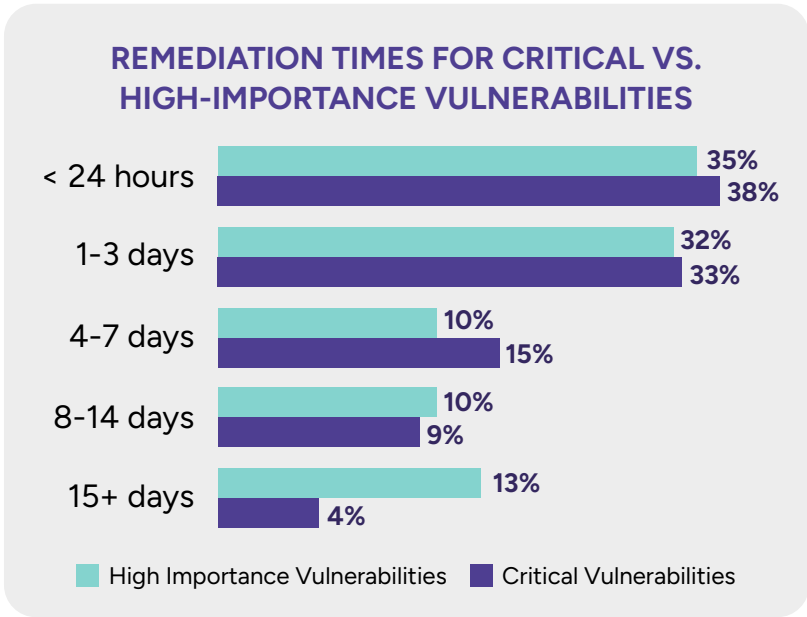
Confidence appears to stem from consistency, not just speed of remediation. Even teams reporting "<24 hours" remediation time still lacked confidence. Remediation success is not about closing tickets, but rather about preventing recurrence.

12 Remediation speeds are generally fast

Assessing the speed of remediation depends on one's criteria for success. Is three days too long to wait to remediate a critical vulnerability? For some organizations, that is unacceptable. For others, it might represent success. The findings suggest that organizations are generally fast to remediate serious vulnerabilities.

Critical vulnerabilities vs. high importance vulnerabilities

Respondents were asked how quickly they remediated critical vulnerabilities versus "high-importance" vulnerabilities. Results for remediation within 24 hours were similar, with 38% remediating critical vulnerabilities in that timeframe, and 35% for high-importance vulnerabilities. The same went for remediation, which took between one and three days, with 33% for critical and 32% for high-importance vulnerabilities. Differences appeared in the longer remediation times. While 4% remediated critical vulnerabilities in 15+ days, 13% took this long to remediate high-importance vulnerabilities.



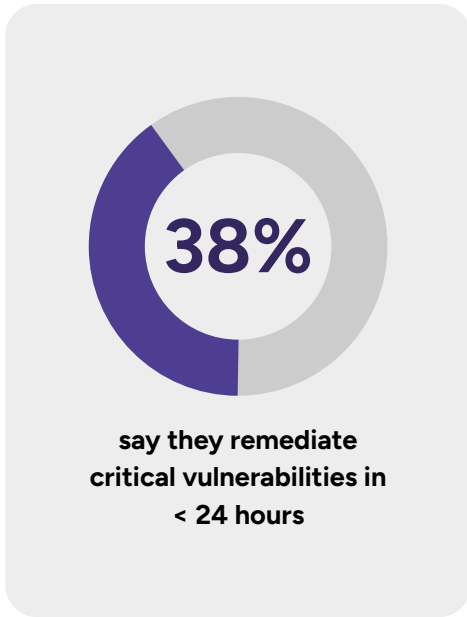


Figure 8 – Comparison of average remediation times for critical vulnerabilities vs. "high importance" vulnerabilities.

13 SLAs: not common, and not commonly met

Respondent organizations do not commonly use Mean Time to Remediation (MTTR) SLAs. Just 40% have set SLAs, and only half of those consistently meet it. Nearly a quarter don't have an SLA and don't plan on creating one. This situation may be due to the difficulty in measuring MTTR across multiple tools and areas of responsibility. The problem is that without an MTTR SLA, it's impossible to establish the performance of the remediation workload, contributing to low confidence and a sense of frustration among team members.

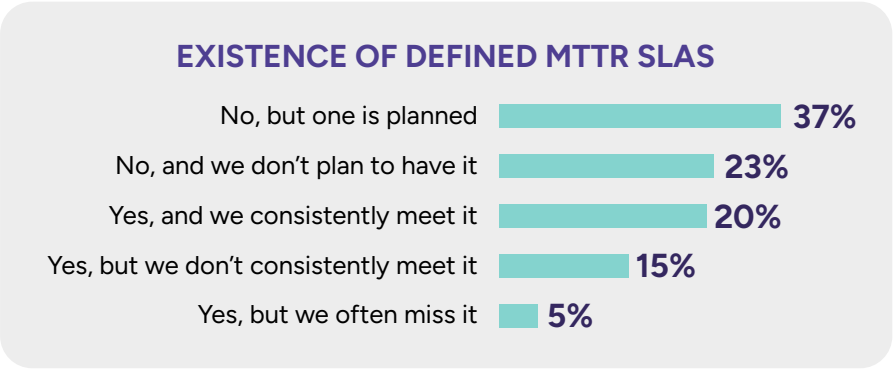
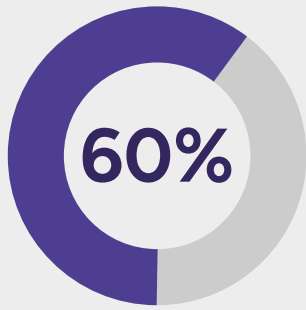


Figure 9 – Responses to the question, "Do you have a defined MTTR SLA for vulnerability remediation?"



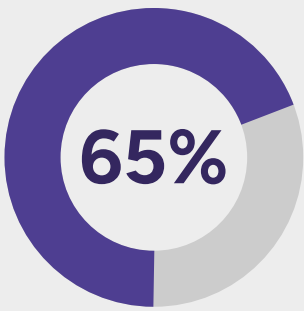
do not have any remediation SLAs

MTTR SLA definitions

Over half (54%) of organizations with SLAs define their target MTTR as less than 24 hours. Based on the MTTR results shared in Figure 8, this suggests that many companies are missing the <24-hour SLA. Twenty-six percent of organizations have a one-to-three day SLA. This seems to be a more achievable SLA, based on Figure 8, where 32-33% reported remediating vulnerabilities in that timeframe.

SLAs and regulatory requirements

The answers to the question, "Do you need to meet any regulatory requirements that require SLAs?" suggest a lack of awareness of compliance frameworks that require tracking and meeting SLAs. Just 22% said "yes." In actuality, many common compliance frameworks mandate remediation tracking. For example, the payment card PCI DSS standard requires organizations to track SLAs and remediate critical vulnerabilities within 30 days. HIPAA, NIST SP 800-53, and ISO 27001 do not specifically require SLAs, but they all mandate that vulnerabilities be remediated in a timely manner. Organizations that need to be compliant must track remediation SLAs in order to meet requirements.



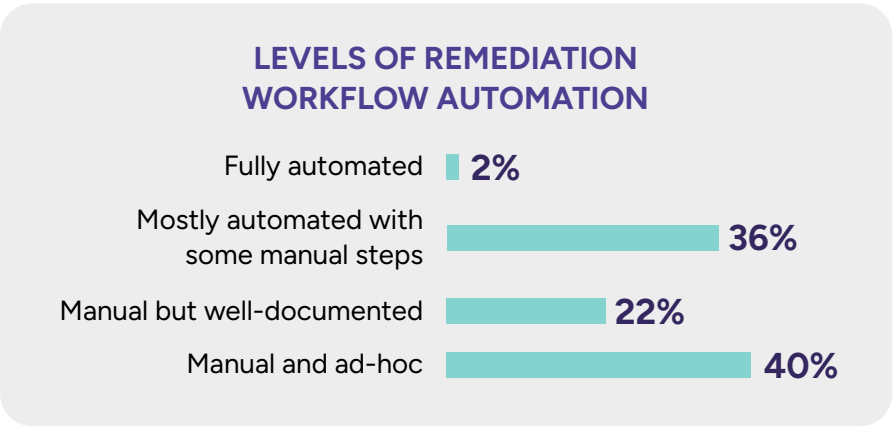
have to analyze data manually to track and report on SLAs

Automated SLA reporting

Two-thirds of respondent organizations lack an automated method for reporting on SLAs. They rely on manual methods for SLA reporting. A third can see current remediation statuses and generate reports. This finding aligns with concerns about a lack of visibility, shared in Figure 3.

14 Rates of workflow automation are low

The vast majority of remediation processes are manual. Just 2% are fully automated. Thirty-six percent are "mostly automated with some manual steps," while 40% "manual and ad-hoc." The frequency of manual or partially manual processes may be due to an excess of tools, which makes automation difficult. Also, full automation requires specialized solutions, which respondent organizations may not have invested in to date.



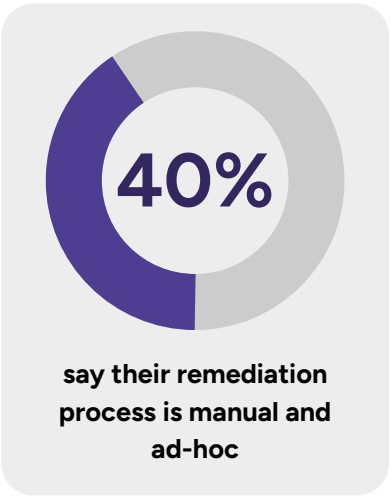


Figure 10 *– Responses to the question, "How automated is your workflow?"*

Automation is also a source of concern due to potential problems it can cause if not properly implemented. Half of the respondents said the risk of "breaking applications or dependencies" was a pain point for automation. Lack of visibility was another issue, with 44% saying it was "hard to know what was remediated, when, and why," and 37% worried about "lack of traceability or rollback options." False positives and low-risk vulnerabilities also make an appearance here, with 38% finding a source of pain associated with automation. Lack of integration between automation systems and CI/CD and IT service management (ITSM) tools was a concern for 29%, while basic organizational resistance was cited by 22%.

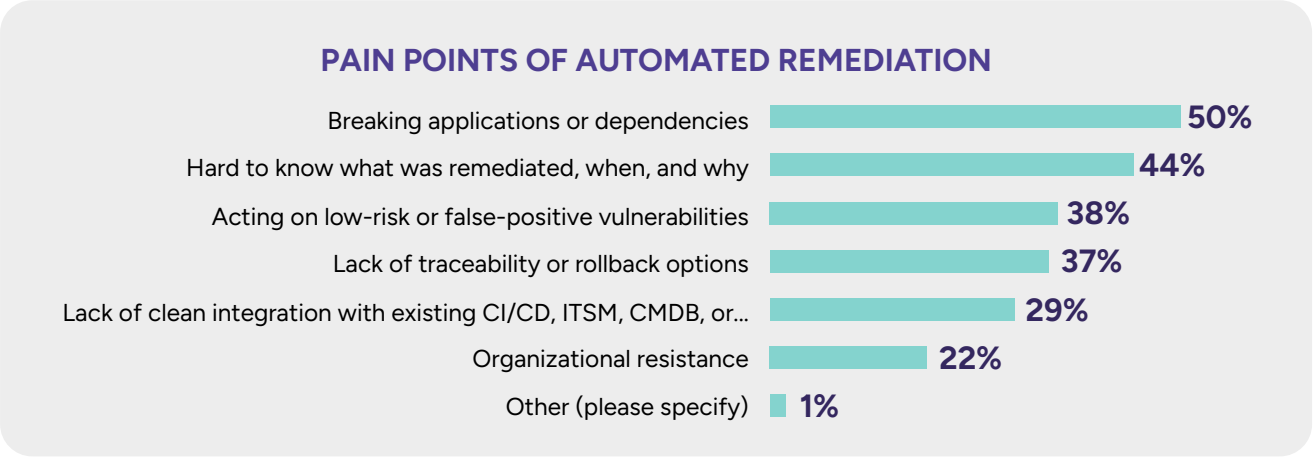


Figure 11 *- Responses to the question, "In your opinion, what are the biggest pain points of automated remediation?"*

Use of CI/CD pipelines for remediation is low

Just 22% of respondent organizations are using their CI/CD pipelines to deliver fixes and remediations. Another 35% are not currently doing this, but want to. This low level of CI/CD use is understandable, given difficulties in integrating remediation systems with DevOps tools. (See Figure 10). Nor do developers relish the work of remediation. However, having four out of five organizations not using CI/CD for remediation is a problematic proposition.

Indeed, this is where several of the core findings of this survey manifest themselves, including:

- **Recurrence of vulnerabilities:** These events stem partly from vulnerabilities remaining in source code and getting reintroduced into production. If the fix occurred at the CI/CD stage, this problem would mostly go away.
- **Low levels of automation:** More manual work means it takes longer to remediate vulnerabilities.
- **Lack of transparency:** If CI/CD pipelines are not used for remediation, DevOps may lack confidence in automated patching because they can't see what is happening by examining code before it is deployed.
- **Confusion over who owns artifacts:** Development teams may lack clarity on which developer should be responsible for a remediation in the code.

The absence of CI/CD appears in answer to a question about the steps necessary to improve MTTR. Thirty-four percent of respondents said that "automated remediation integrated into a CI pipeline" would speed up remediations. (See Figure 12) The idea of "more ownership from DevOps/platform engineers" was cited by 24%.

15 What it will take to improve remediation

Respondents have many ideas for improving remediation, at least as far as speed is concerned. Asked, "Which factors would help you to remediate significantly faster?" 44% said "auto-creating tickets with all relevant info included." (Related ideas included "more remediation guidance and code snippets" (33%), "instantly see owner of artifact" (31%), and "automated ticket tracking instead of just 'fire and forget'" (28%). Taking these steps would do much to address the problems of a lack of information and context. Forty percent said "better prioritization," which is an answer for the issues of alert fatigue and the need to process low-risk vulnerabilities and false positives.

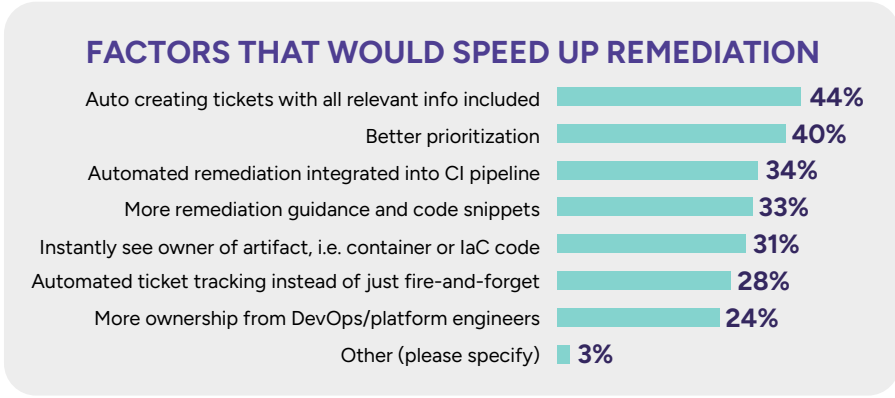
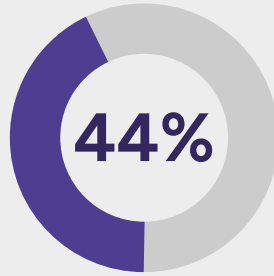


Figure 12 - Responses to the question, "Which factors would help you to remediate significantly faster?"



said "auto-creating tickets with all relevant info included" would speed up remediation

Recommendations

What can we learn from these findings? In short, defenders need to automate more processes to have a chance at being faster than attackers. This can seem like a daunting task, but by implementing automation gradually, setting appropriate guardrails, and integrating into existing workflows, you can build trust and confidence. The most important thing is to start now.

Below we list some practical steps that you can take to start moving in the right direction:

SET SLAS AND AUTOMATE TRACKING

Defining the goals for your vulnerability management program is a crucial first step. Establish achievable Service Level Agreements (SLAs) that can be adjusted as automation increases. It's also vital to automate the tracking of these SLAs to measure performance and avoid adding extra manual work for security and IT teams.

AUTOMATE PRIORITIZATION

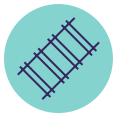
Unsurprisingly, alert fatigue was named as the biggest remediation pain point. It's extremely important to eliminate false positives and low-priority alerts, and focus only on the important issues. Unified vulnerability management solutions with comprehensive contextual insights tend to be more effective at prioritizing than siloed tools. In addition, solutions must collect detailed data on the infrastructure, rather than just superficial information, because this significantly improves prioritization.

AUTOMATE TICKETING

Fully automating ticketing creation with all the necessary remediation steps, code snippets, and asset details so platform engineers can efficiently resolve the reported issue, not only saves manual work and speeds up remediation, but also reduces team friction and frustration. Real ticketing automation doesn't stop at just creating tickets, it should also track progress, verify resolution, close, and automatically reopen tickets when drift occurs.

AUTOMATE PATCHING

Implementing automated patching is probably the most daunting task, but will also bring the greatest benefits. There may be understandable fear of breaking systems and losing control. However it's important to understand that automated patching is really no longer a 'nice to have'. With appropriate human control, versioning, and roll back options, confidence can quickly be built up. Begin with systems of lower priority, then progress to highly specific applications under human supervision. If everything is working well, gradually broaden the scope.



DEFINE GUARDRAILS EARLY

Decide which actions can be automated without approval and which should require human sign-off. At first, you'll probably want to require human approval for every action.

AUTOMATE REPORTING

Ensure that remediation reports can be generated automatically, and set a regular report schedule, preferably weekly. This is important to demonstrate compliance, validate security efforts, improve risk management, and enable informed decision-making.

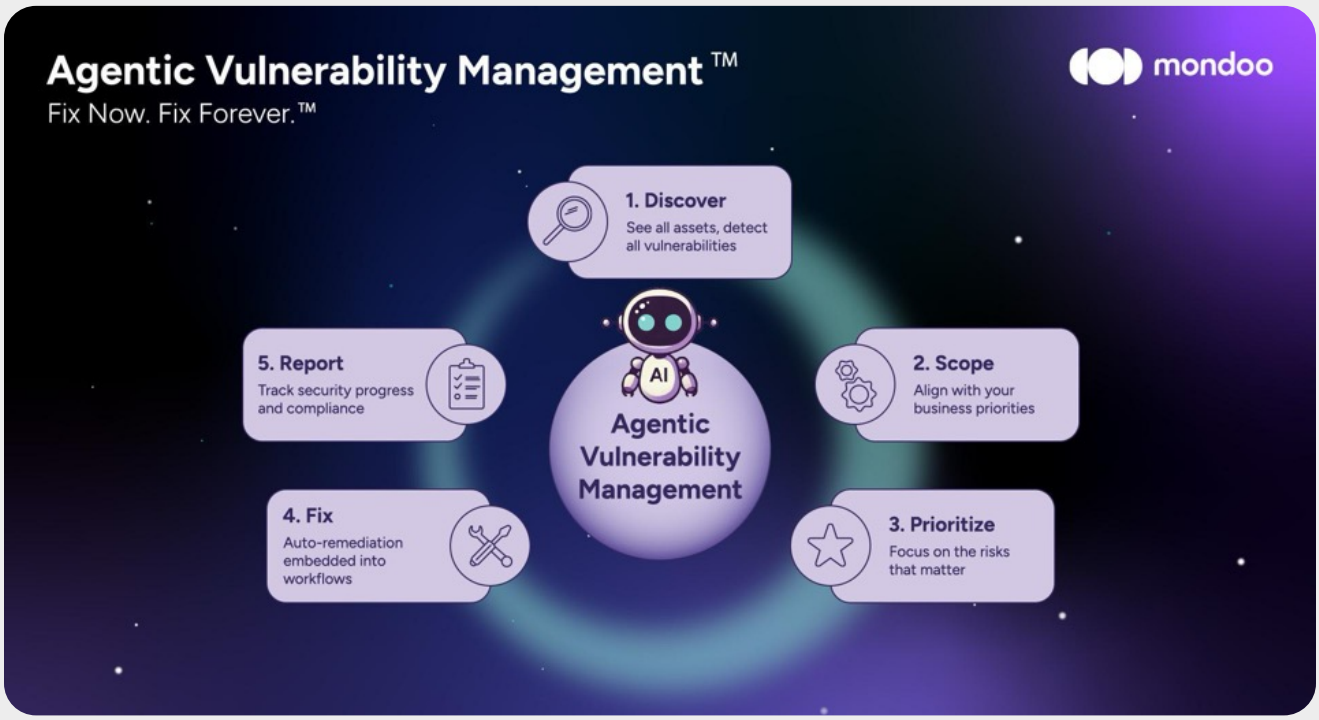
Conclusion

Companies must quickly remediate serious vulnerabilities or face significant risk exposure. This is not always a simple prospect. Problems range from tool sprawl to alert fatigue, a lack of visibility and detail, and little clarity on lines of responsibility. Vulnerabilities can recur after remediation, leading to frustrating do-overs. Survey respondents reported low levels of confidence in their remediation capabilities, despite being relatively fast on MTTR. Organizations lack a single source of truth.

This is not an unsolvable challenge, however. With automation, such as for ticketing and enriching remediation assignments with instructions and contextual data, and reducing manual work with CI/CD integration and automated SLA tracking and reporting, it is possible to make remediation more rapid and efficient. There is a path to better remediation outcomes. Solutions can bridge today's critical gaps through automation with built-in human review and versioning, improved visibility, higher coverage, and actionable remediation guidance.

About Mondoo

Mondoo is the world's first agentic vulnerability management platform that eliminates - not just categorizes - vulnerabilities. Global enterprises trust Mondoo to prioritize risks by business impact and exploitability through its patented AI-native security model that collects structured, context-aware data from the entire IT infrastructure. Mondoo's customers have reduced vulnerabilities and policy violations by 50% and significantly reduced MTTR. With seamless ITSM integrations and transparent security pipelines, Mondoo enables autonomous remediation and continuous compliance. Mondoo bridges the gap between security and engineering - delivering intelligent recommendations and actionable insights to fix vulnerabilities that matter most to the business.



Mondoo's agentic vulnerability management capabilities include:

PRIORITIZATION

Mondoo agents continuously detect vulnerabilities and misconfigurations in the environment, and leverage deep and wide insights to prioritize issues based on contextual risk factors, business impact, threat intelligence, and exploitability. This ensures that only truly critical issues are sent to IT Ops, reducing alert fatigue and possible friction between security and IT.

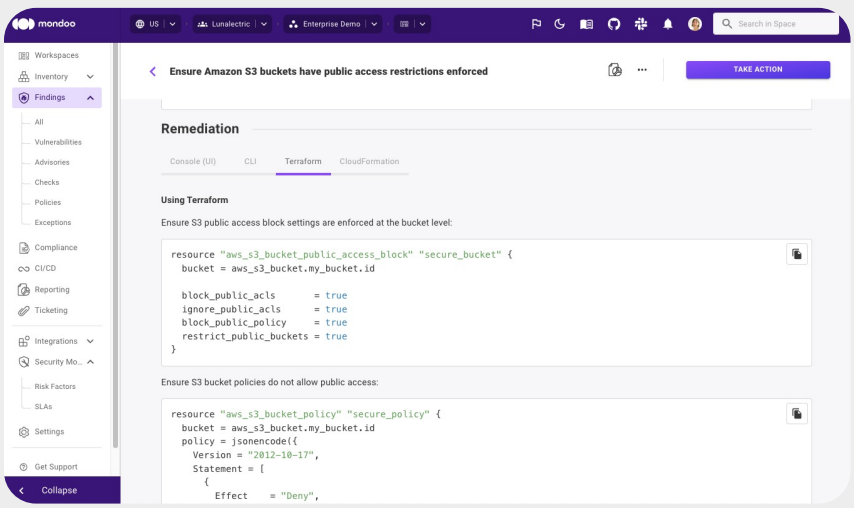
ORCHESTRATION

Mondoo agents orchestrate the entire vulnerability workflow from detection to resolution (we call this the Mondoo Flow), and automatically create tickets in ITSM systems. Agents track tickets to completion, auto-close upon verification, and reopen if drift occurs. Security and platform engineering teams can use their LLM to ask Mondoo questions to speed up tasks and reduce back and forth between teams. This reduces manual work, accelerates MTTR, and simplifies reporting and compliance.

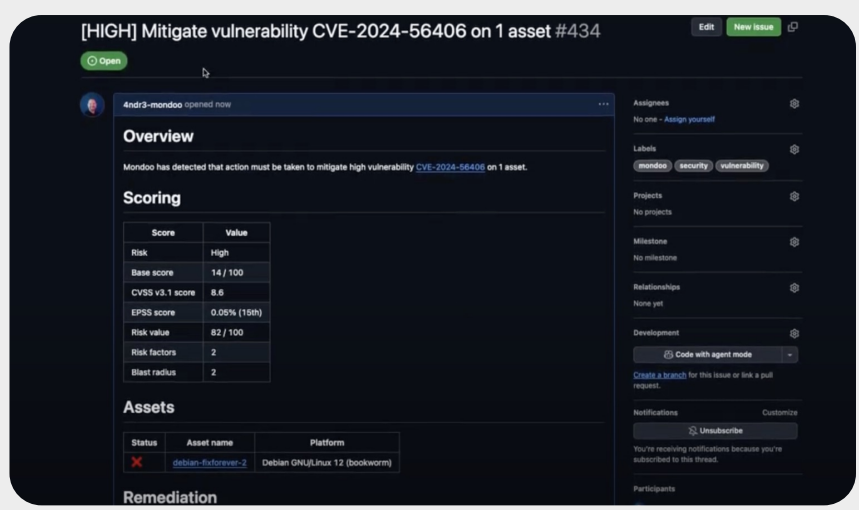
REMEDIATION

Mondoo agents create tickets with detailed information on the affected asset(s), as well as remediation steps and pre-tested code snippets that can instantly be applied by platform engineers. Mondoo also performs autonomous patching using the Mondoo security pipeline and pre-tested Ansible, Terraform, and InTune remediation code, with versioning and rollback. By reducing manual work and integrating into DevOps workflows, Mondoo bridges the gap between security and engineering teams delivering security without sacrificing development speed.

To learn more about Mondoo, visit mondoo.com.



Mondoo provides guided remediation steps and code snippets for detected issues



Agentic vulnerability patching using the Mondoo security pipeline

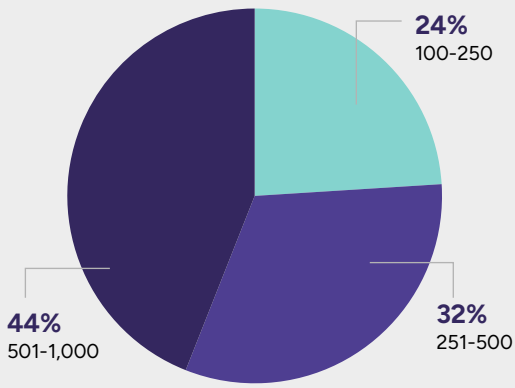
Trusted by companies around the globe:

Calligo · SIS · FVB Frankfurter Volksbank Rhein/Main · T · emnify · FORTUNE 50 Tech Company · FORTUNE 50 Manufacturing Co. · IGZ THE SAP ENGINEERS · Universal Investment · Colosseum Dental

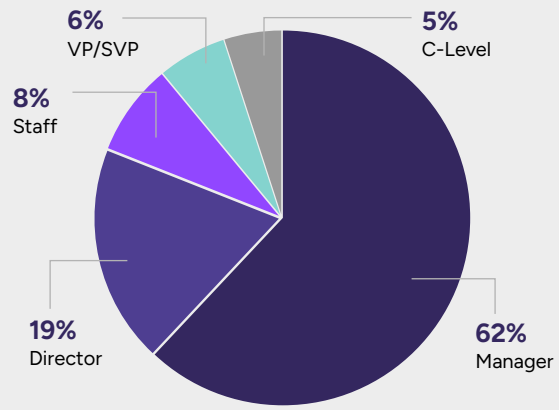
Appendix

Respondent Demographic Details

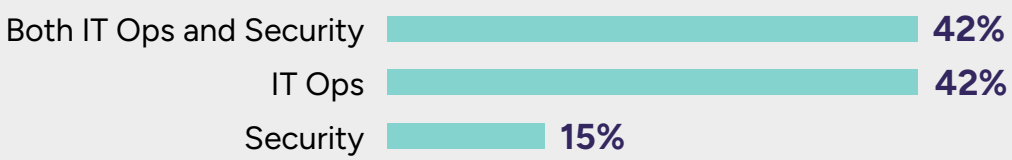
COMPANY SIZE



ORGANIZATIONAL LEVEL



ROLE



INDUSTRY