vicarius

JULY 2026

Exposed and unfixed: the 2026 state of vulnerability remediation

Table of Contents

Introduction and Key Findings

Introduction & Methodology

For years, cybersecurity teams have invested heavily in visibility. New scanning technologies, cloud security tools, attack surface management platforms, continuous monitoring solutions, and AI-powered security tools have dramatically expanded organizations' ability to identify vulnerabilities across their environments.

Those investments worked. Organizations now know about more vulnerabilities, across more assets, faster than at any point in the industry's history.

The challenge is that the systems used to find vulnerabilities have advanced faster than the processes used to fix them. And now, with AI accelerating both vulnerability discovery and exploit development, teams are accumulating findings at a pace they can't absorb manually.

Most organizations don't have a visibility problem. They have a remediation problem. The more vulnerabilities they find, the more obvious the gap becomes. We built this report to better understand that gap.

We wanted to examine how remediation happens inside organizations. How much of the process is still manual? Who owns remediation work? What happens operationally when a critical vulnerability is discovered? Do security leaders and frontline practitioners share the same view of remediation effectiveness? And why do known vulnerabilities, often sitting in inventories for months or years, continue to appear in breach post-mortems?

To answer these questions, we surveyed security and IT professionals about their day-to-day remediation workflows, team structures, handoffs, tool usage, and reporting practices. The findings provide a benchmark for how organizations approach remediation today, where friction continues to exist, and where opportunities remain to close the gap between finding vulnerabilities and fixing them.

Methodology

To understand how organizations approach vulnerability remediation, patching, and remediation operations, we surveyed 300 IT and cybersecurity leaders across the United States and United Kingdom. Respondents worked in organizations with between 500 and 2,000 employees and represented a range of industries, including financial services, manufacturing, information technology and services, healthcare, automotive, and government.

Participants were drawn from both IT and cybersecurity departments. Respondents from IT teams were screened to ensure responsibility for patching and remediation activities, while cybersecurity respondents were responsible for vulnerability management programs. The sample included an even distribution of managers, directors, and vice presidents, providing perspectives from both strategic decision-makers and those closer to day-to-day operations.

The survey explored remediation workflows, ownership models, team collaboration, handoffs, tooling, reporting practices, and the operational steps that occur after vulnerabilities are identified.

Data collection took place in April 2026 in collaboration with Global Surveyz, an independent survey company.

Key Findings

01 | Remediation is still mostly manual.

Vulnerability remediation remains largely a human process. On average, respondents report that 58% of their remediation activities require direct human intervention, with 74% of organizations reporting that more than half of their remediation workflow is still manual. While many teams have automated discovery, scanning, and reporting, the work of prioritizing, approving, deploying, and verifying fixes continues to rely heavily on people, creating a natural limit on remediation speed and scale.

02 | The team that finds it usually can't fix it.

82% of organizations can't consistently remediate a vulnerability within the team that identified it. Instead, remediation depends on handoffs, shared ownership, or workflows where ownership changes based on the situation. Every handoff is a delay, and every ownership question is another opportunity for remediation to stall. For most organizations, fixing the vulnerability is only part of the challenge. Coordinating who fixes it is the rest.

03 | Finding a vulnerability is the easy part.

When a critical vulnerability is identified, 75% of organizations don't immediately remediate it. They create a ticket, send an alert, or notify an asset owner. The finding moves through a workflow. The exposure stays open. Only 25% deploy an automated remediation action directly from the platform. For everyone else, discovery has become a handoff instead of the beginning of immediate remediation.

04 |

79% of organizations experienced a security incident in the past 12 months involving a vulnerability that was already known and present in their inventory. More than half report that the vulnerability had been identified 30 to 90 days before the incident occurred. This is not primarily a zero-day problem. It's a remediation problem. The vulnerability was found, tracked, and understood, but the process needed to eliminate the risk failed to close the gap before it was exploited.

Survey Report Findings

Human intervention remains the norm in vulnerability remediation

For all the discussion around automation, vulnerability remediation remains heavily dependent on human effort. Only 7% of organizations have achieved fully automated remediation with zero human intervention. For everyone else, humans are still in the loop. On average, 58% of remediation activities require human intervention, with half of all respondents falling in the 50-74% range.

The pattern suggests teams have automated the parts that were always easier to automate: discovery, scanning, and reporting. Remediation is where that progress slows. Deciding what to fix, securing approvals, deploying changes, and verifying outcomes remain human-driven activities in most organizations. The data suggests that remediation maturity still lags well behind detection maturity.

The consistency of the results across company sizes and industries reinforces the broader story. This isn't a challenge confined to a particular industry or organization size. It's an industry-wide reality.

A practical benchmark: Review your remediation activity from the last 30 days. How many steps required a person to initiate, approve, deploy, or verify a fix? The answer may reveal more about your remediation maturity than any dashboard.

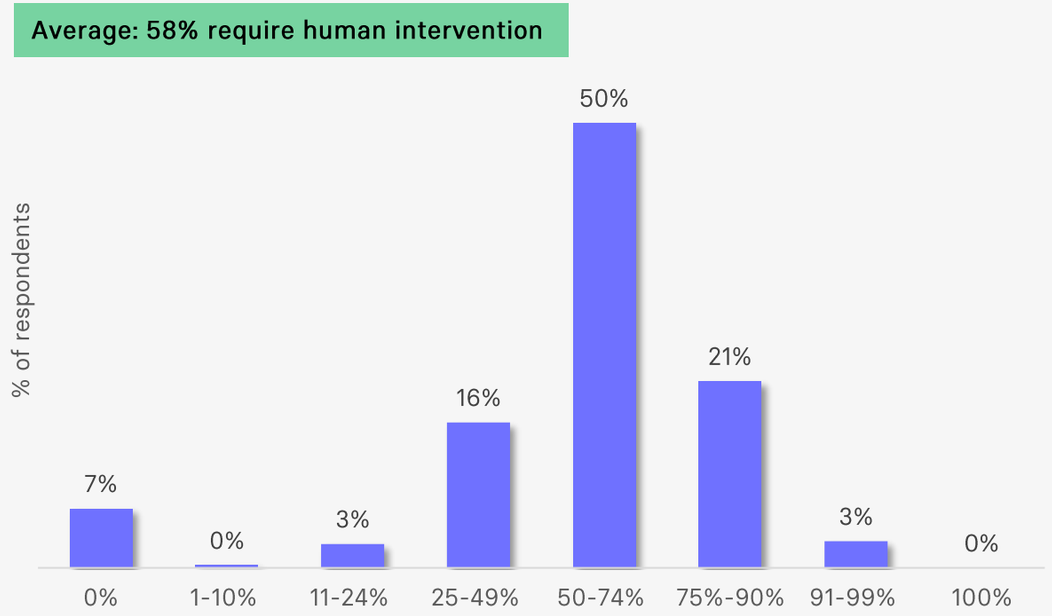

Figure 1: Percentage of manual vulnerability remediation requiring human intervention

Remediation maturity looks better on paper than in practice

At first glance, the survey results paint a positive picture: 62% of respondents rate their organization's remediation program as somewhat mature or very mature. When asked how they believe frontline IT and security teams would rate the program, 57% gave the same positive assessment.

The challenge is that these perceptions don't fully align with what we saw in Figure 1. If organizations were truly operating highly mature remediation programs, we'd expect to see much lower levels of human intervention. Instead, respondents reported that 58% of remediation activities still require manual involvement.

This suggests a disconnect between how organizations define remediation maturity and what their day-to-day operations actually look like. Many teams may have mature processes for identifying vulnerabilities, tracking remediation efforts, and reporting progress. Yet the underlying work often remains heavily dependent on people.

The seniority breakdown adds another interesting dimension. Directors are the most likely to describe their programs as very mature (29%), while VPs are the least likely (13%). The leaders closest to executive reporting may have a more cautious view of how much remediation work still remains.

A practical benchmark: Ask your most senior remediation engineer the same question you'd answer in a board update: "How mature is our remediation program?" If the answers differ significantly, you may have a visibility problem before you have a process problem.

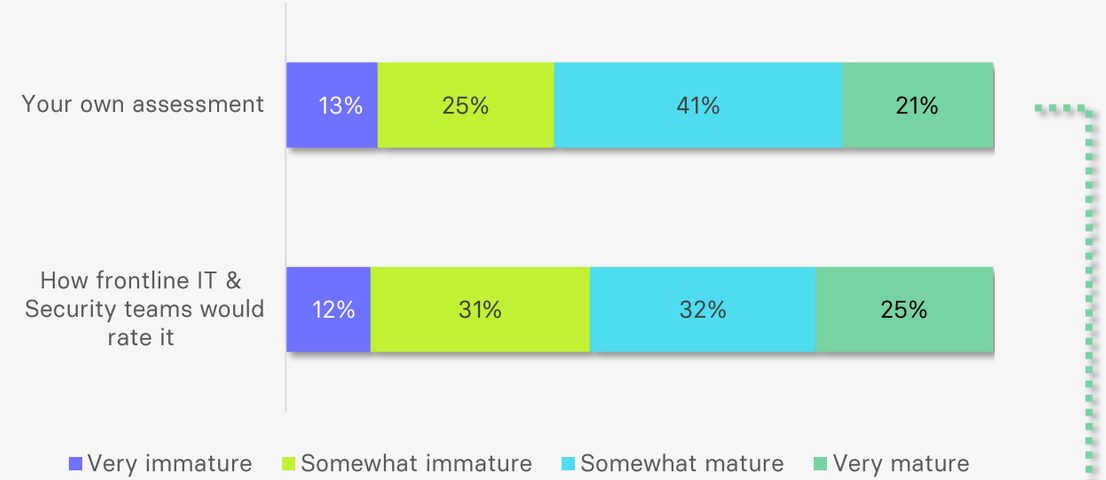

Figure 2: Perception of organizational remediation maturity: leadership vs. frontline teams

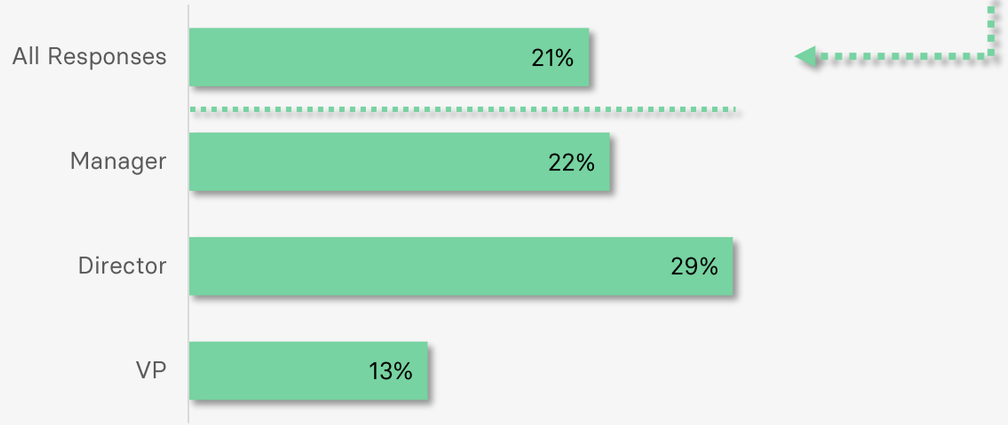

Figure 3: "Very mature" by job seniority

Remediation challenges are organizational, not technical

Only 10% of respondents say they don't face major challenges in vulnerability remediation. The other 90% report some form of friction, suggesting that remediation remains difficult even for organizations with established vulnerability management programs.

The most commonly cited challenge is competing priorities (22%). In many organizations, remediation doesn't have a protected time. Vulnerabilities get addressed when other projects, outages, or business demands allow. When remediation consistently loses priority battles, the issue isn't technical. It's organizational.

Change management and approval processes rank second at 17%, highlighting another common bottleneck. Teams often know what needs to be fixed and how to fix it. The delay comes from approvals, coordination, and deployment processes. Every additional approval step extends the window between identifying a vulnerability and reducing risk.

Taken together, the top challenges point to a common theme: remediation struggles are rarely caused by a lack of visibility. More often, they're caused by competing priorities, organizational processes, and limited authority to act quickly.

The findings help explain why remediation continues to lag behind detection. The barriers are often embedded in workflows and decision-making structures rather than technology itself.

A practical benchmark: Review your last three remediation SLA breaches. Were they caused by technical blockers, or by competing priorities, approval processes, and waiting for sign-off? The solution to the second category won't come from a better scanner.

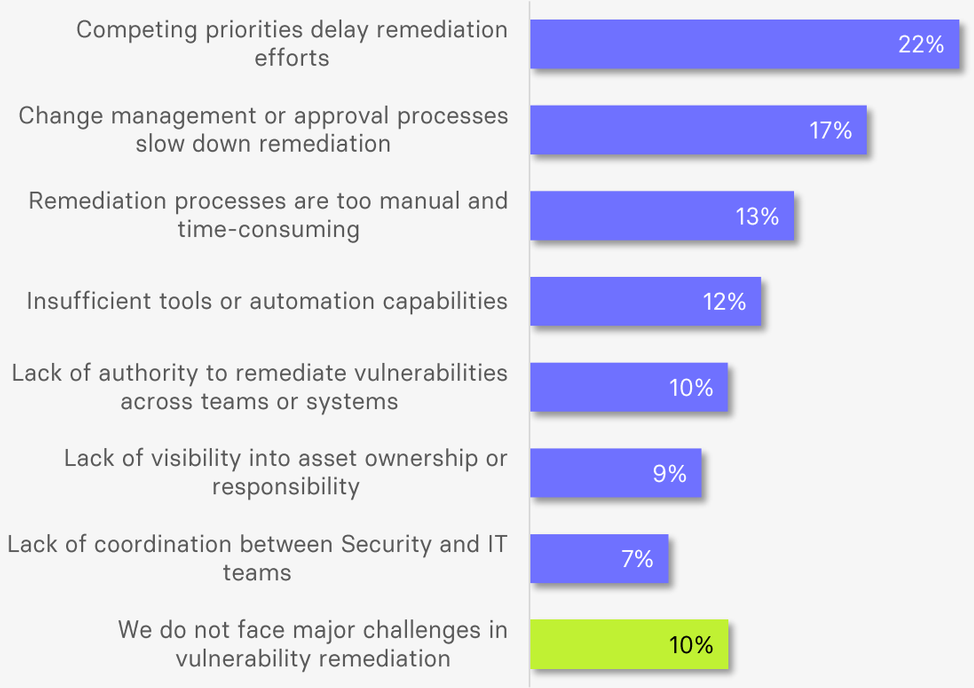

Figure 4: Primary organizational challenge in vulnerability remediation

Critical vulnerabilities are still routed through manual workflows

When a critical vulnerability is identified, the most common response isn't remediation. It's creating a ticket.

42% of respondents say their primary action is creating a task in a system such as Jira or ServiceNow. While tickets help track work, they don't reduce risk on their own. A ticket is a handoff mechanism, not a remediation action. The vulnerability still needs to be prioritized, assigned, approved, fixed, and verified.

Only 25% of organizations report deploying an automated remediation action directly from the platform. That means three out of four organizations still rely on downstream processes and human intervention, even when dealing with critical findings.

The remaining responses largely shift responsibility to people. 18% send alerts to security teams for manual review, while 15% notify asset owners and expect them to take action. This is one of the most fragile response models in the data. Responsibility is handed to someone who may lack the security context, tooling, authority, or urgency needed to remediate the issue quickly.

Many organizations have built effective systems for identifying critical vulnerabilities, but far fewer have built equally effective systems for responding to them.

A practical benchmark: Find the last critical CVE your team identified and trace what happened during the first 24 hours. If the answer is "a ticket was created," ask who had the authority to move it forward without escalation.

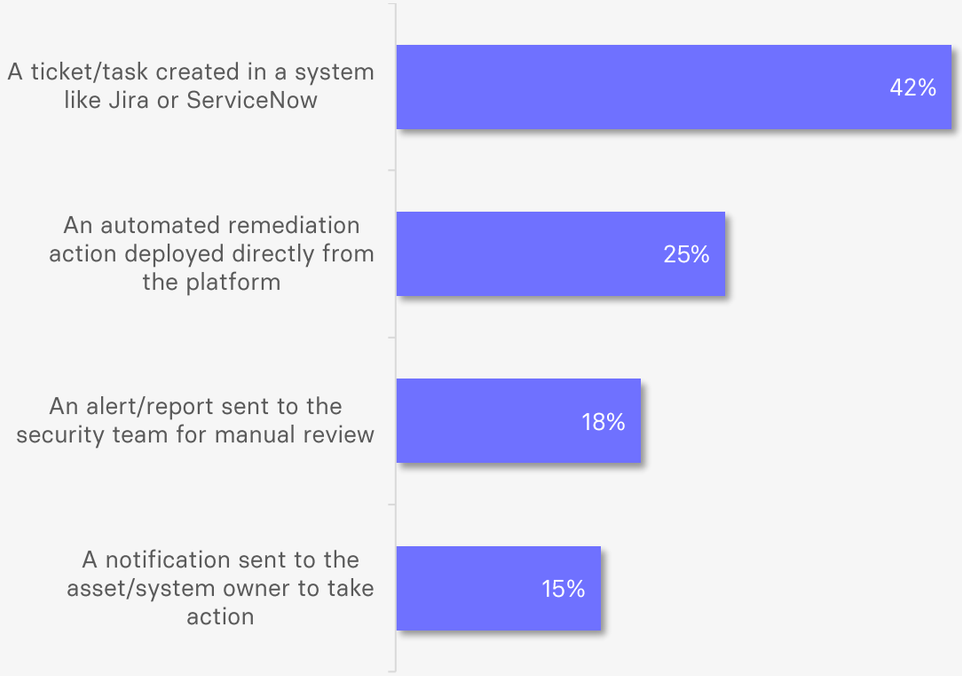

Figure 5: Primary action following critical vulnerability identification

Most vulnerabilities can't be remediated by the team that finds them

Only 18% of organizations report that the team identifying a vulnerability can fully remediate it without involving other teams. For everyone else, remediation depends on handoffs, shared ownership, or additional stakeholders.

This matters because every handoff introduces delay. The moment responsibility moves from one team to another, urgency can fade, priorities can shift, and accountability becomes less clear.

The most concerning finding is that 38% of respondents say remediation ownership depends on the situation or is unclear. In practice, this means more than a third of vulnerabilities don't have a clearly defined path to resolution. When ownership isn't explicit, remediation often slows down while teams determine who is responsible for taking action.

Another 43% report that they can sometimes remediate vulnerabilities within the originating team, but not consistently. Together, these findings suggest that remediation workflows remain highly dependent on organizational structure rather than standardized processes.

Larger organizations perform somewhat better, with 23% reporting full remediation capability compared to 13% of smaller organizations. However, the gap is relatively small, suggesting that additional resources help but don't fundamentally solve the underlying challenge.

A practical benchmark: Map a recent vulnerability from identification to verified remediation and count how many teams were involved. For each handoff, ask whether ownership transfer has a defined SLA or relies on informal expectations. The answer may reveal where remediation momentum is being lost.

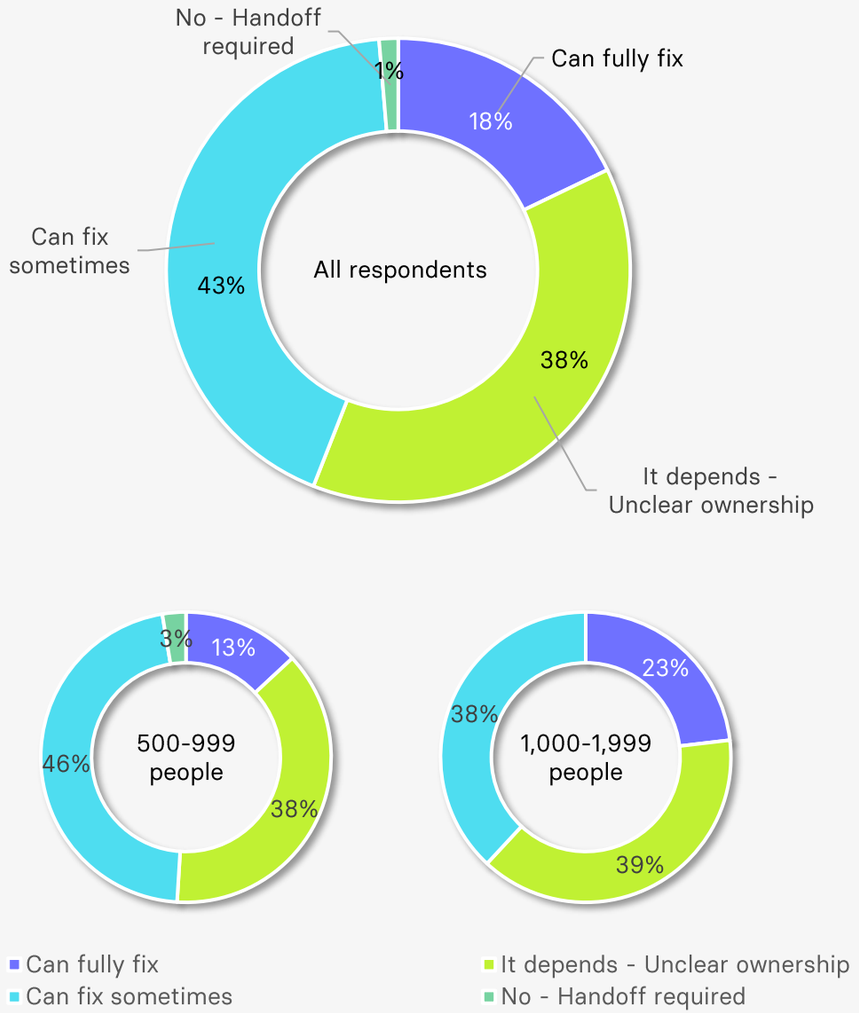

Figure 6: Ability to remediate without external handoff by company size

What does “remediated” actually mean?

One of the most revealing findings in the report isn't about remediation processes or ownership. It's about how organizations define “remediation.”

Only 50% of respondents say a vulnerability is officially marked as remediated after a fix has been deployed and verified through a rescan or automated check. In other words, only half require proof that the vulnerability has been eliminated.

The other half use definitions that focus on activity rather than outcomes. 18% consider remediation complete when a ticket is created and ownership is assigned. Another 13% close remediation once a patch or fix has been deployed, even if there's no verification that it worked.

Perhaps most notably, 18% mark a vulnerability as remediated when leadership formally accepts the risk. While risk acceptance is a legitimate security practice, it isn't remediation. The vulnerability still exists. Treating accepted risk and resolved risk as the same thing can make security posture appear stronger than it actually is.

Organizations aren't always measuring the same thing when they report remediation metrics. As a result, remediation maturity may look very different depending on how "remediated" is defined.

A practical benchmark: Open your tracking system and check what allows a vulnerability to be marked as remediated. If closure can occur before verification, you're measuring activity rather than outcomes, and your risk posture may look better on paper than it does in reality.

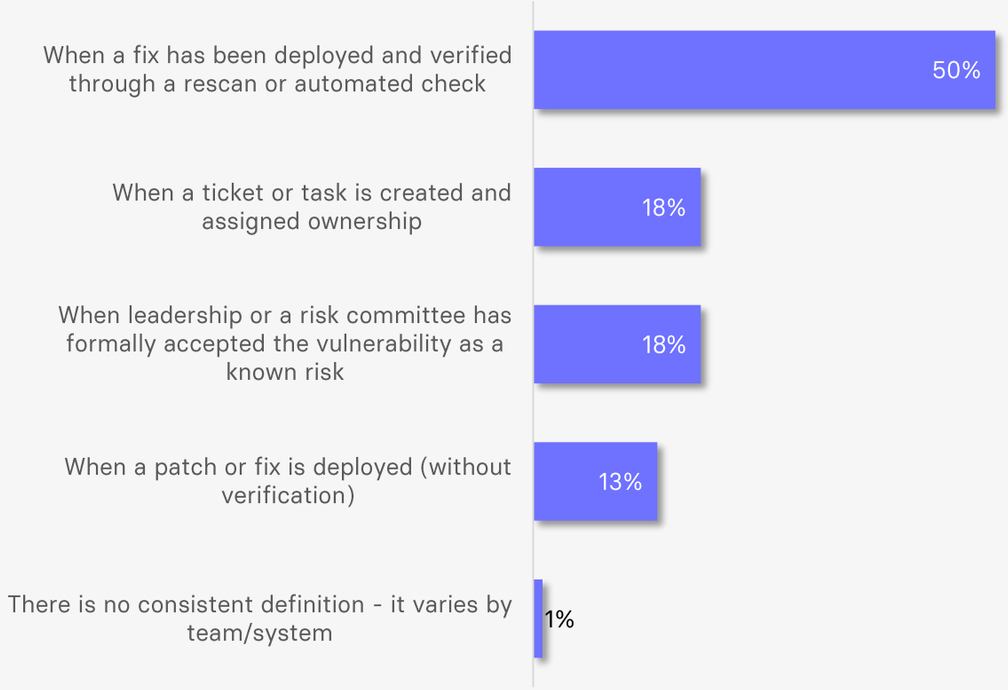

Figure 7: Criteria for official remediation status in tracking systems

Most security incidents stem from vulnerabilities that were already known

Perhaps the most concerning finding in the report is that 79% of organizations experienced a security incident involving a vulnerability that was already known and tracked before the incident occurred.

This wasn't a detection failure. The vulnerability had already been identified. The issue was what happened next.

More than half of respondents (51%) report that the vulnerability was known for 30 to 90 days before the incident. Organizations had weeks, and in some cases months, to address the issue but were unable to close the gap before it was exploited.

This reinforces a theme that appears throughout this report: most organizations aren't struggling to find vulnerabilities. They're struggling to act on them quickly enough.

As attackers increasingly use automation and AI to identify and exploit weaknesses faster, remediation timelines measured in months are becoming increasingly difficult to defend. A backlog that once seemed manageable can quickly become an active source of risk.

Ultimately, this data suggests that visibility alone isn't enough. Knowing about a vulnerability only creates value if organizations can consistently translate that knowledge into action.

A practical benchmark: Review your most recent security incident and determine whether the exploited vulnerability was already in your inventory. If it was, identify when it was first discovered and why it remained open. That timeline is your remediation gap made visible.

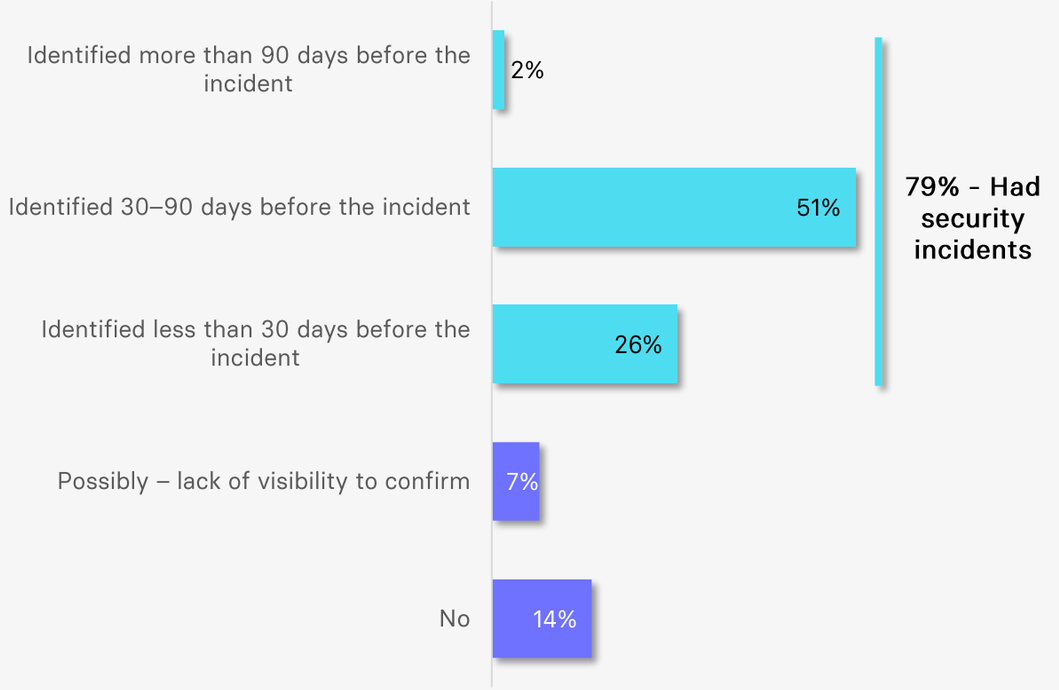

Figure 8: Security incidents involving known vulnerabilities within the past 12 months

Are organizations measuring activity or risk?

When it comes to reporting remediation performance to senior leadership, the most common metric is Mean Time to Remediate (MTTR), cited by 49% of respondents. This suggests that many organizations are focused on measuring speed and operational efficiency.

The challenge is that speed alone doesn't necessarily reflect risk reduction. Figure 9 showed that 79% of organizations experienced a security incident involving a vulnerability that was already known. If vulnerabilities are still being exploited after they've been identified, remediation velocity may not be telling the whole story.

By contrast, only 24% of respondents rank risk reduction among their top reported metrics. While many organizations may still track it, the data suggests that leadership discussions are more likely to focus on how much work is being completed than on whether exposure is decreasing.

This distinction matters. Metrics such as MTTR, open vulnerabilities, and SLA compliance are useful operational indicators, but they primarily measure activity. Risk reduction measures outcomes. One tells you how efficiently the process is moving. The other tells you whether the organization is becoming safer.

The good news is that only 1% report having no formal metrics at all. Organizations are measuring remediation. The bigger question is whether they're measuring what matters most.

A practical benchmark: Review the metrics presented to leadership last quarter. If they focus exclusively on speed, volume, or closure rates, ask whether any of them demonstrate that your attack surface actually shrank. MTTR tells you how fast you're moving, not whether you're moving in the right direction.

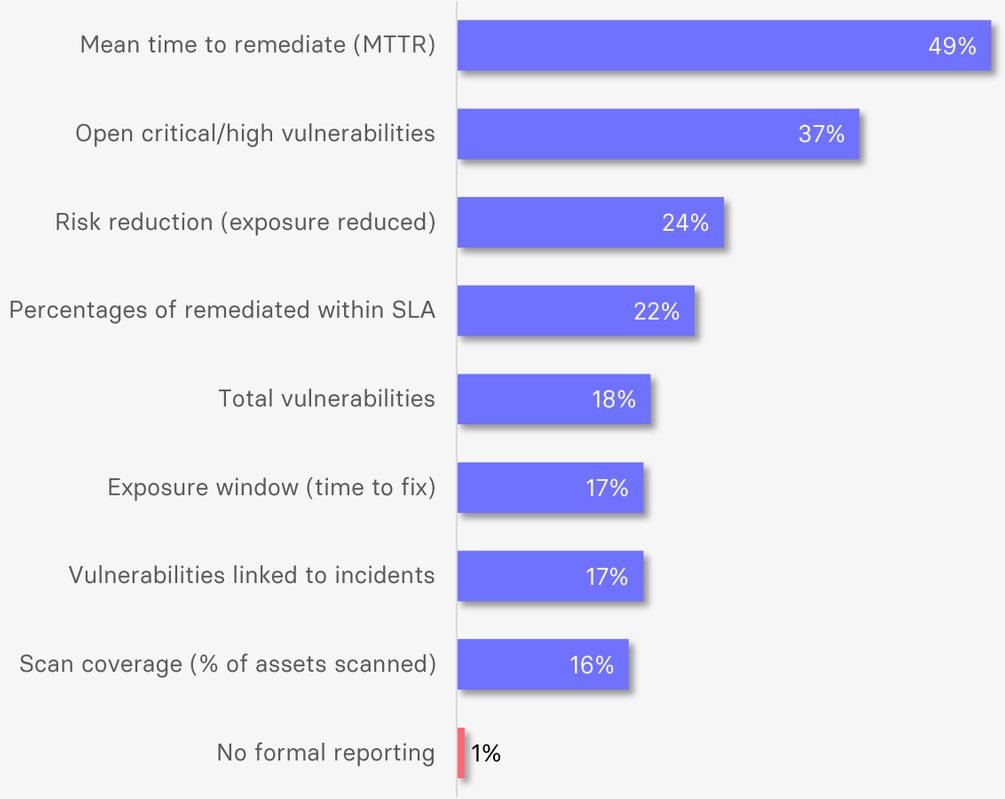

Figure 9: Key performance metrics reported to senior leadership for vulnerability management

*Question allowed more than one answer and as a result, percentages add up to more than 100%

Third-party vulnerabilities remain heavily dependent on manual processes

Third-party applications are often the source of some of the industry's most significant security events. Yet the data suggests that remediation processes for these vulnerabilities remain far from mature.

The most common approach, cited by 35% of respondents, relies on limited automation combined with substantial manual effort. Another 19% depend on direct intervention from IT or security teams. Only 21% report having a standardized, fully automated process for handling third-party application vulnerabilities.

Taken together, this means that nearly 80% of organizations manage third-party vulnerabilities through a combination of manual work, inconsistent processes, delayed responses, or no structured process at all. In an environment where vendor advisories can appear at any time and vulnerabilities can quickly become active threats, inconsistency creates risk.

Perhaps most concerning, 12% of respondents report having no remediation process for third-party vulnerabilities. The vulnerability may be identified, but there is no defined workflow for determining ownership, evaluating risk, or driving remediation.

This reinforces a broader theme throughout this report: identifying vulnerabilities is no longer the primary challenge. Building repeatable, scalable processes to respond to them is.

A practical benchmark: Review your three most critical third-party applications. Do you have a documented remediation process for each one? Not a general patch policy, but a process that addresses vendor timelines, compensating controls, ownership, and what happens when a patch isn't immediately available.

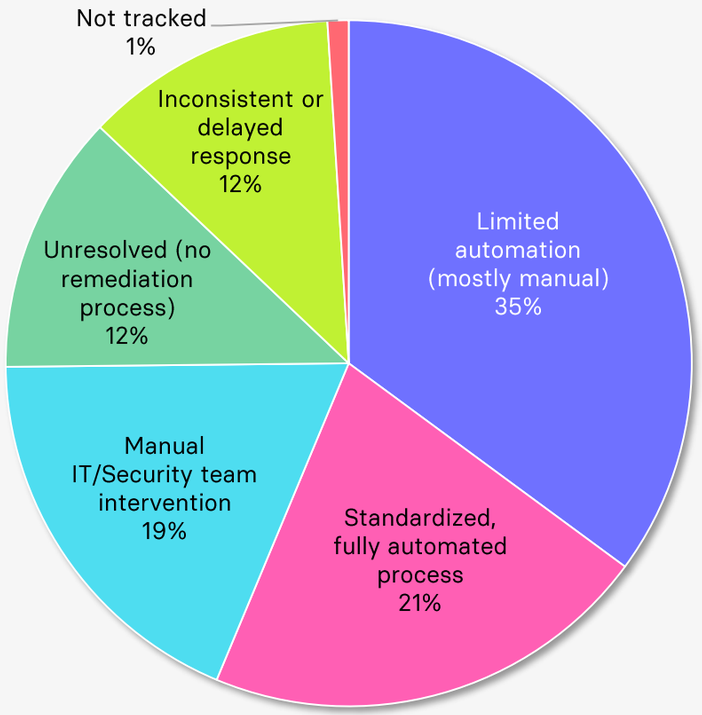

Figure 10: Standard operating procedures for third-party application vulnerability identification

Organizations have options when patches aren't available

One of the more encouraging findings in the report is that organizations aren't relying on a single strategy when a vulnerability lacks an official patch. Network segmentation (55%), virtual patching (54%), and configuration hardening (53%) are all widely used, suggesting that most teams have multiple ways to reduce risk while waiting for a vendor fix.

At the same time, the near-identical adoption of these approaches raises an interesting question. Are organizations following a defined response playbook, or are they choosing whichever option seems most appropriate in the moment? The data shows that teams have tools available, but it doesn't necessarily show that they're applying them consistently.

Custom remediation scripts add another layer to the picture. 35% of respondents deploy scripts to neutralize exposure when patches aren't available. This can be a powerful capability, but it also introduces risk. Scripts created or deployed under pressure can create operational issues if they aren't properly tested, reviewed, and tracked.

Notably, only 1% of respondents report having no interim remediation capability at all. The challenge, then, isn't whether organizations have options. It's whether they can execute those options consistently when a critical vulnerability appears.

A practical benchmark: The next time a critical vulnerability is disclosed without a patch, ask whether your team follows a documented response playbook or relies on individual judgment. If the answer depends on who's on call that day, the process may be less mature than it appears.

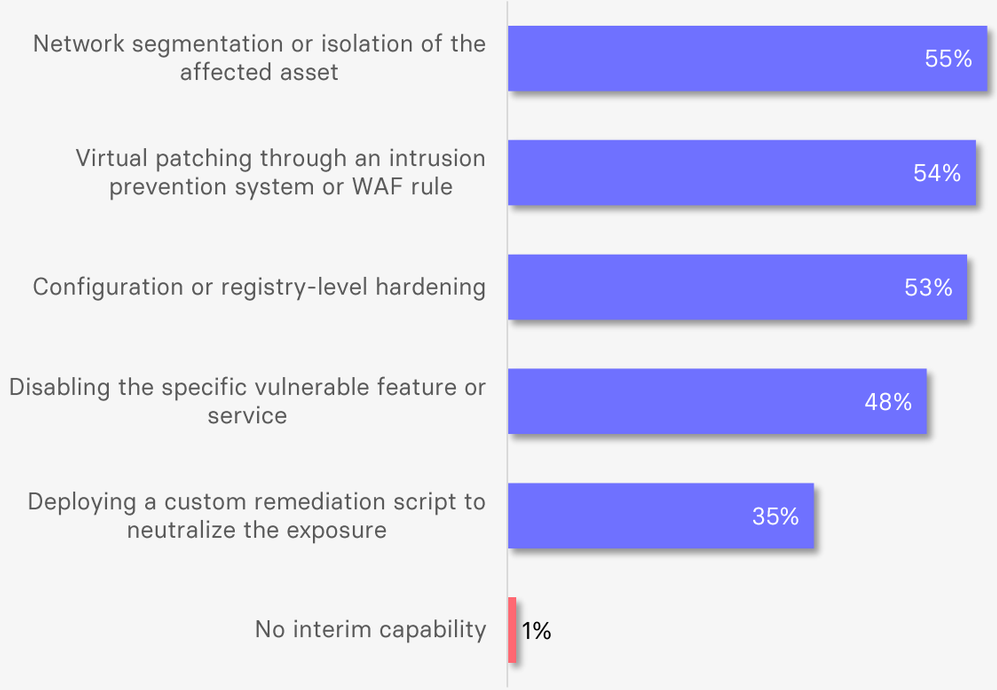

Figure 11: Available interim remediation methods for vulnerabilities lacking official patches

*Question allowed more than one answer and as a result, percentages add up to more than 100%

Remediation is spread across multiple systems

The average organization uses three different tools or systems across the remediation lifecycle. On the surface, that may not sound excessive. But it means vulnerabilities often move through multiple platforms, teams, and workflows before they're resolved.

Each additional tool introduces another handoff point. Information must be transferred, ownership reassigned, and status updated. As the number of systems grows, so does the risk of delays, miscommunication, and lost context.

The challenge becomes even clearer when looking at the upper end of the distribution. 39% of respondents use four or more tools throughout the remediation process. For these organizations, remediation is no longer just a security workflow. It's a coordination challenge involving multiple systems, stakeholders, and timelines.

Interestingly, 14% report using only a single tool. While some organizations may have successfully consolidated their workflows, others may simply be overlooking systems that have become part of the process over time. Ticketing platforms, spreadsheets, email approvals, and manual verification steps all contribute to remediation, whether they're officially counted or not.

Remediation isn't slowed down only by vulnerabilities. It's also slowed down by the complexity of the processes and systems surrounding them.

A practical benchmark: Count every system touched between identifying a vulnerability and verifying it's fixed, including ticketing tools, spreadsheets, and manual tracking steps. If the number is higher than expected, your remediation process may be more fragmented than it appears.

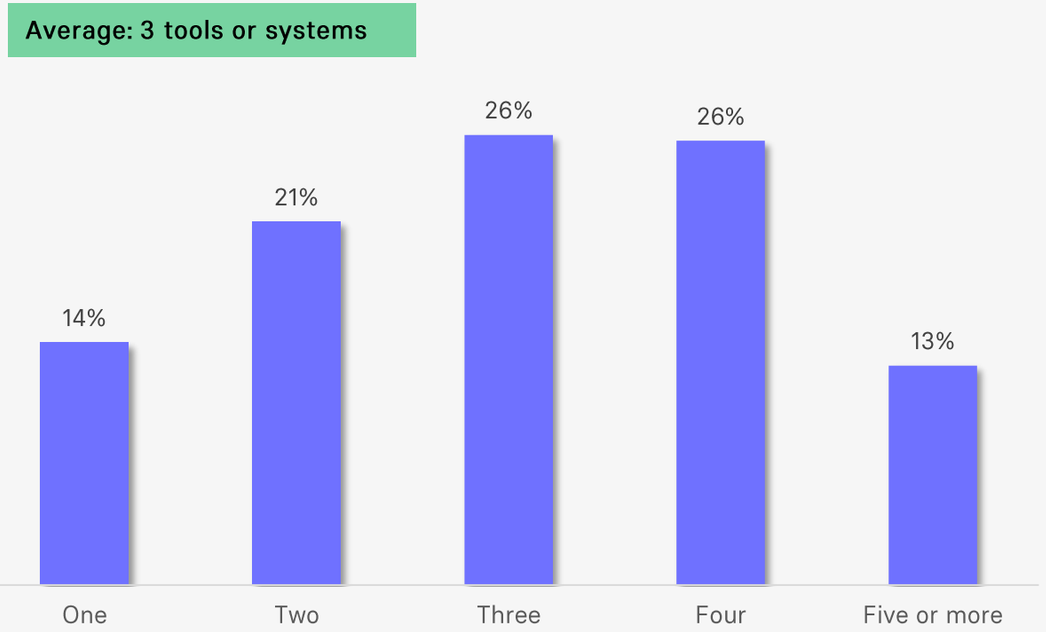

Figure 12: Number of distinct tools utilized throughout the end-to-end remediation lifecycle

Demographics

Country, Industry, Company Size, Department and Job Seniority

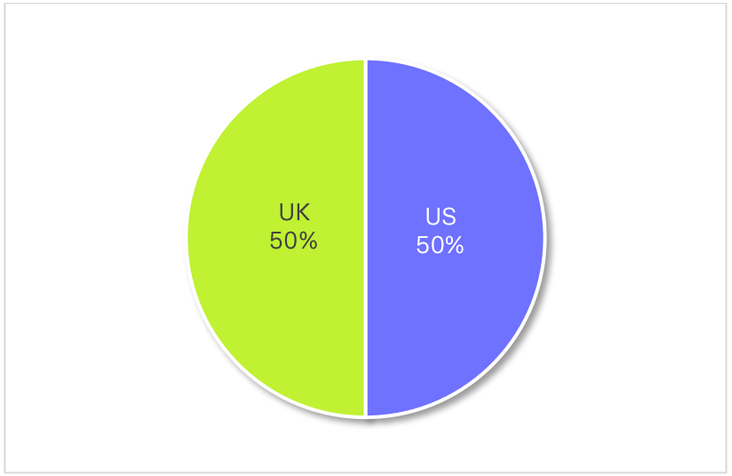

Figure 13: Country

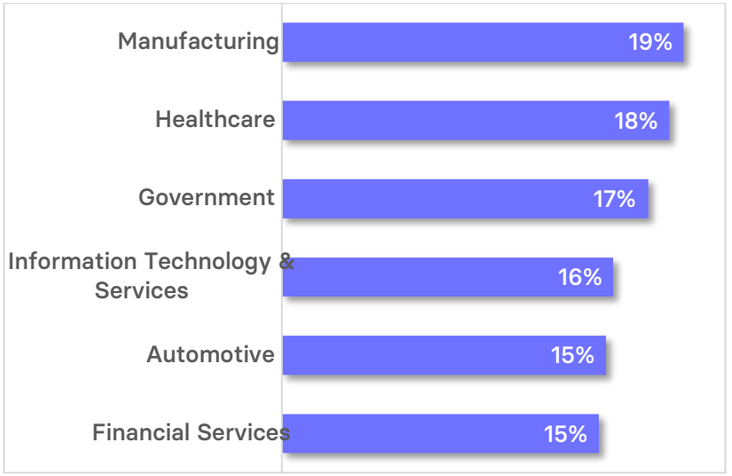

Figure 14: Industry

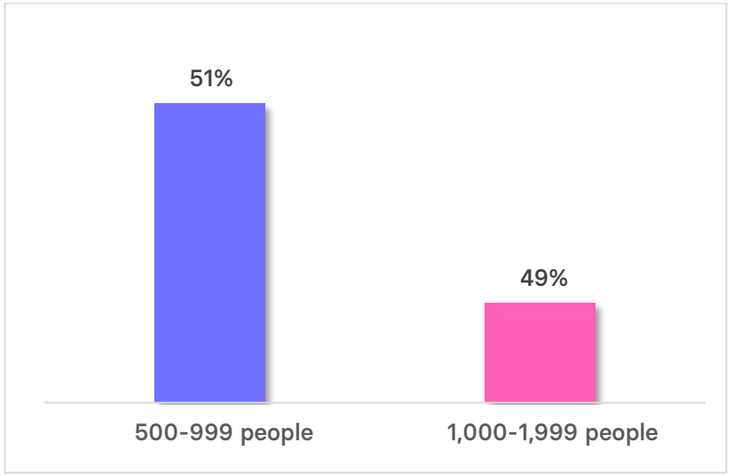

Figure 15: Company Size

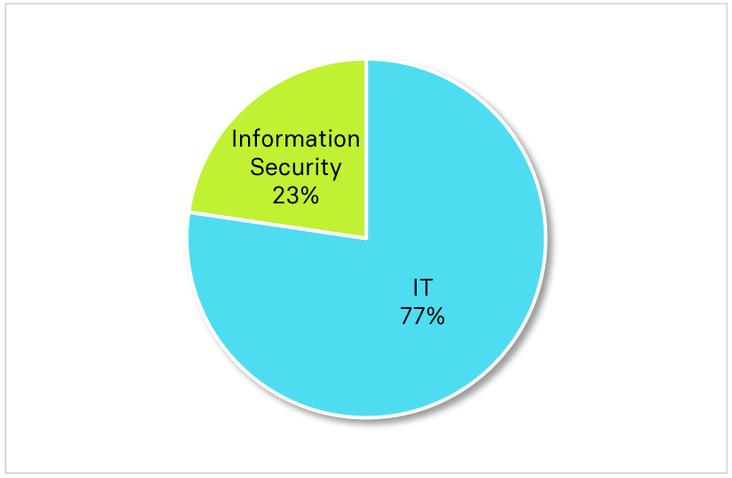

Figure 16: Department

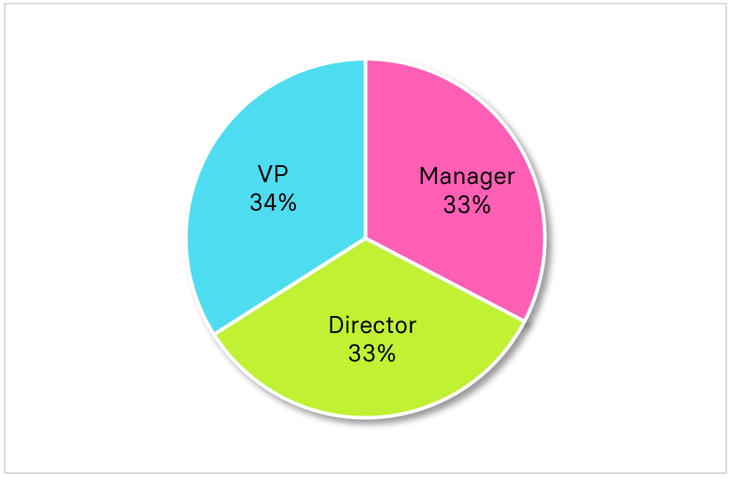

Figure 17: Job Seniority

About Vicarius

Vicarius revolutionizes vulnerability management by closing the loop between problem detection and proactive resolution. The company's portfolio is built on two flagship pillars: vRx for advanced, native remediation at scale, and vIntelligence, an agentic validation engine that delivers continuous AI-driven security insight and orchestration.

Now with vRx and vIntelligence, Vicarius offers a full remediation cycle. With 1000+ customers in 60 countries, vRx by Vicarius streamlines and automates risk mitigation for security teams, SMBs, and enterprises.

Schedule a call with Vicarius

Visit us at:

www.vicarius.io

Email: info@vicarius.io