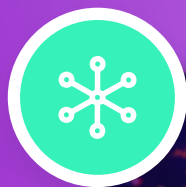


THE 2023 State of Risk Reduction: A Need for Speed

Security Teams Wrestle to Reduce Risks
in Complex Environments With Manual Workflows





Executive Summary

For security teams today, reducing organizational risk often feels like a giant — and hugely dissatisfying — game of Whac-a-Mole. In rapid succession, risks keep popping up from various siloed scanning tools. Remediating these risks requires a tedious and labor-intensive series of steps focused on deduplication, prioritization, and routing of issues to an appropriate “fixer” somewhere in the organization. This burden on already resource-strapped security teams is an efficiency killer.

Lengthy remediation times, friction among business units, endless backlogs of unassigned remediation tasks, and an inability to scale to match today’s ever-increasing pace of risk discovery and remediation requirements are just some of the ill effects of this disjointed approach. Include frustrated and dispirited security workers in the fallout as well.

A new study, commissioned by Seemplicity and conducted by Dark Reading, provides fresh insight into how security pros handle the challenging remediation life cycle from discovery to resolution. The research reveals the obstacles security professionals face when coordinating remediation activities. The data exposes the outcomes — in increased workload and diminished risk posture — that arise from lengthy remediation times, inefficient and uncontrolled manual processes, the lack of managerial visibility and oversight across the risk life cycle.

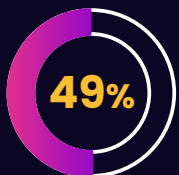
Our findings also spotlight the advantages of automating most or all of the remediation life cycle. Virtually every common barrier to efficient remediation identified in the research can be addressed through available technology that integrates with scanning tools, then automatically aggregates and normalizes findings, identifies remediation owners, tracks remediation progress, and shares the backlog burden among all of the organization’s stakeholders.

TOP FINDINGS



It Takes Nearly 4 Weeks to Remediate Critical Security Risks From Start to Finish

A granular look at the end-to-end risk-reduction process shows remediation life cycles consistently measured in weeks, not days. The research shows that it takes nearly 4 weeks for the average organization to get from risk discovery to verified resolution. For some organizations, the process of performing the actual fix may not be as efficient, which would extend the timeline to be even longer.



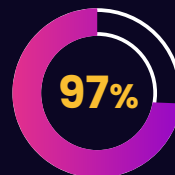
49% of Security Professionals Don't Know Who to Contact to Fix Risks or Verify Fixes

When it comes to fixes, slowdowns start early, particularly when the process remains mostly manual and loosely managed. Locating the correct fixer, getting a response to a remediation request, and verifying successful fixes are top-time consumers for most organizations. Small wonder since half of the security teams (49%) approach these important issues informally or through trial and error.



The Average Organization Manages 3 to 5 Security Tools, Adding Complexity and Slowing Down Remediation

The data clarifies that manual tasks and multiple feeds from disparate scanning tools conspire to drag down speed-to-remediation. The average organization manages 3 to 5 tools that actively identify unexploited security risks. Meanwhile, more than 1 in 3 (36%) has more than 6 siloed risk feeds to manage.



97%* would focus on proactive security tasks if remediation was efficient

Organizations get bogged down on manual, human-centric tasks like prioritization and verification. If there were better and faster ways to remediate risks, respondents said they would spend the time gained from better and faster ways to remediate risks on forward-looking activities, such as additional architecture review (70%), threat modeling (58%), and security awareness training (51%).

*97% of respondents checked at least one of the options provided (Architecture review, Threat Modeling, Security awareness training for the organization, or Planning future initiatives).

INTRODUCTION

Remediation Under Pressure

Flaws in business technology systems are unavoidable. IT systems weaknesses and the heightened risks associated with them are pervasive and constant in modern, decentralized, perimeter-less environments. And the problem is expanding. So far, through the end of November 2022, the **National Institute of Standards and Technology (NIST)** logged a record 23,096 new weaknesses, or nearly 70 per day. That's a 26% jump from the year prior.

Of the flaws found last year, 10,342 — an average of 28 per day — are classified as “critical” or “high severity” issues, according to the U.S. Cybersecurity and Infrastructure Security Agency (CISA). In lockstep with discovery, average times for fixing published weaknesses are steadily increasing even as the lag time between found flaws and working exploit shrinks from days to sometimes just a few hours.

In the risk pressure cooker, security teams tasked with rooting out and remediating both published and unpublished weaknesses in their own corporate environments are in a race against the clock. It's not unusual for an average-sized security team to amass upwards of 60,000 unaddressed risks every 6 months.

This onslaught of issues can quickly overwhelm risk management programs, particularly when complicated by complex departmental relationships and conflicting priorities among security and development teams. Corraling

problems churned out by siloed security scanning tools and forcing them through manual security prioritization and distribution bottlenecks prevent even the best-intentioned organizational efforts from remediating risks efficiently.

At a high level, the most time-consuming aspects of remediation among security teams we studied remain finding the appropriate party responsible for making the fix, issuing the formal remediation request, getting an acknowledgment that the risk is being addressed, and verifying the fix once it's accomplished (**FIGURE 1**).

This is the reality for the overwhelming majority of security teams today, the research shows. The solution, the data suggests, depends most prominently on relieving vastly outnumbered security team members of manual remediation tasks and automating remediation workflows in order to route issues directly to the developers responsible for fixing the problems. This task-automation exchange remains the most reliable and efficient approach for freeing up security resources and getting risks off the books before they can be exploited.

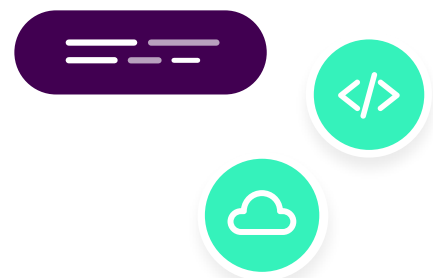
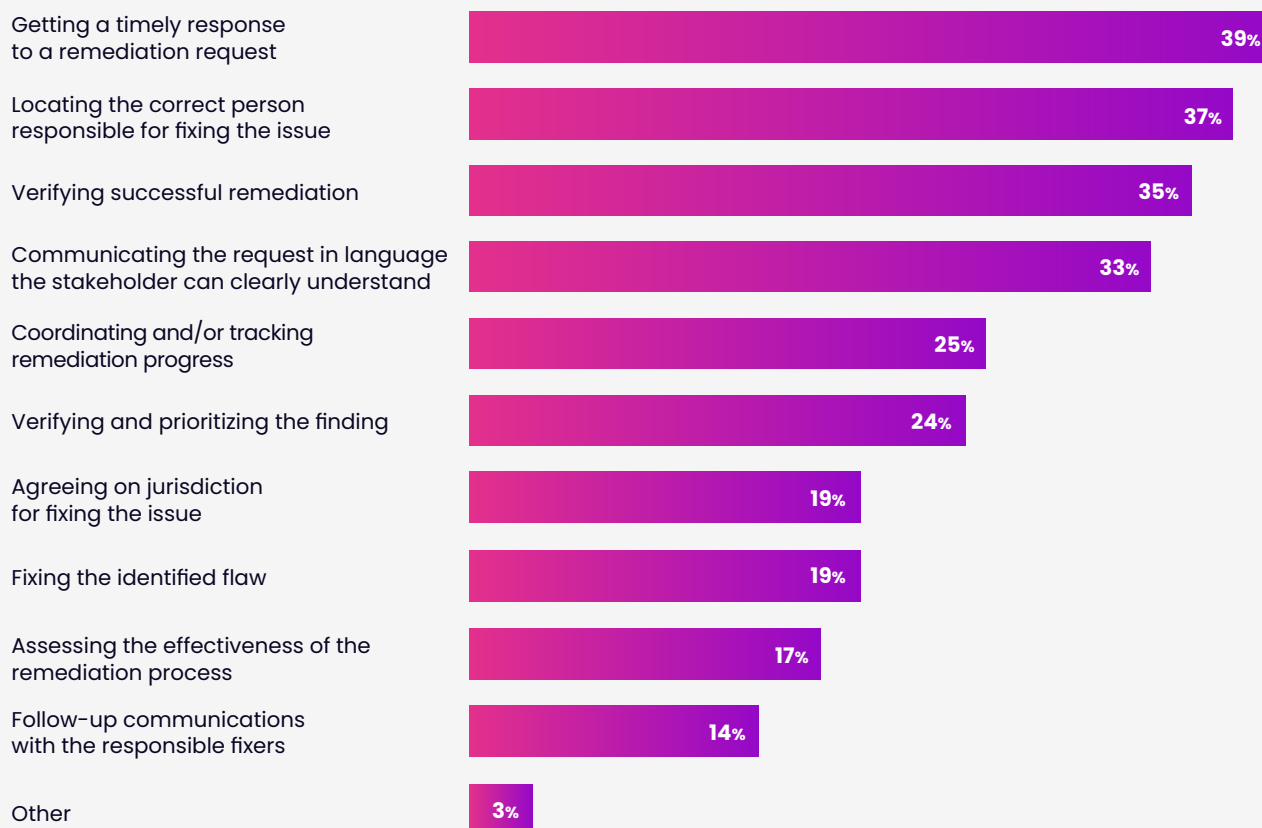


FIGURE 1

Time-Consuming Aspects of Vulnerability Remediation

Which of the following are the most time-consuming aspects of coordinating vulnerability remediation with stakeholders outside the security team?



Obstacles and Timelines: A Granular Look at Remediation Processes

The current remediation reality in a typical business environment lacks automation and an unhealthy dose of manual, inefficient activity. With that suboptimal framework as a given, how teams approach remediation can differ from situation to situation and team to team. The variability and unpredictability of remediation turn this process into an expensive one, as organizations have to figure out what needs to be done ad hoc.

For our research, we asked security pros to estimate the time needed in business days to accomplish **6 fundamental remediation tasks in order**:

01 Logging

Adding the risk to the current list of open issues once it is discovered and reported.

02 Verification

Researching to determine that the issue is new, unique, and unresolved through previous remediation.

03 Prioritization and Deduplication

Assessing risk to determine the urgency of the fix and compiling congruent issues into a single remediation ticket.

04 Resource Location

Identifying and locating the responsible stakeholder in the best position to implement remediation.

05 Assignment

Communicating effectively with the remediation owner to notify them of the issue and request a fix.

06 Tracking and Verification

Keeping track of the issue as it moves through the remediation process, then verifying the effectiveness of the solution once the ticket is reports as resolved.

Respondents were asked to include both the actual time frame for each action item as well as any lag time accumulated between the stages. The results offer both a granular task-by-task look at the remediation burden as well as an overall timeline for closing security weaknesses in real-world business environments.

The average organization takes 18.5 business days to go from discovery to verified risk resolution (**FIGURE 2**). Steps that involve codifying, communicating, and verifying remediations dominate the timeline. Note that for some organizations, the processes they have for

actually performing the fixes may extend the timeline even longer.

Within that period, the typical respondent tells us they spend 2 to 3 days each on initial remediation tasks, including logging discovered risks and verifying the need for resolution. From here, the process bogs down noticeably, with the security team increasingly reduced to the role of middleman in the remediation workflow. The average team spends 3 to 4 business days prioritizing findings, then an additional 3 to 4 workdays identifying the correct stakeholder responsible for making the fix, including determining which project management platform they use and how best to assign them the task.

Nested in this part of the process is the prototypical remediation bottleneck. For the majority of security professionals polled, simply locating the correct party to make a fix encapsulates an unholy trifecta of manual labor, inconsistency, and lack of formal process.

FIGURE 2

Average Remediation Time by Company Size

How many days does it take your organization to accomplish each of the following tasks, including any lead time accumulated between steps?

Avg. Remediation Days by Company Size	Overall Days	Up to 1,000 Employees	1,000–9,999 Employees	10,000 + Employees
See finding from the moment it has been discovered	2.31	2.52	2.17	2.5
Confirm finding is new and unresolved	2.8	2.54	2.65	3.23
Prioritize findings	3.5	2.52	3.66	3.92
Identify remediation owner, ticketing system, and board	3.26	2.71	3.56	3.28
Open ticket and notify remediation owner	2.44	2.94	2.6	1.69
Track and verify risk has been resolved	4.16	4.48	4.4	3.53
Total Process Time Average Days	18.48	17.71	19.03	18.15

Data: Dark Reading survey of 108 IT cybersecurity professionals at companies with 100 or more employees.

Half of the respondents (49%) depend on informally routing fix requests based on past experience or resorting to trial-and-error use of company directories (**FIGURE 3**). 1 in 8 (12%) have no consistent approach to the required task at all.

Once the fixer identification hurdle is crossed, the typical security team then spends 2 to 3 days opening the ticket and notifying the remediation owner. The final step measured in our research is the longest for the vast majority of security professionals we surveyed. Verifying that the responsible stakeholder has properly resolved a weakness takes 4 to 5 more business days at the end of each remediation cycle, the data shows. While remediation is a time-consuming burden for all organizations, the process doesn't impact all security teams equally.

Security teams at small companies (those with fewer than 1,000 full-time employees) and those at large enterprises (more than 10,000 employees) enjoy total remediation cycles slightly below the overall average of 17.7 and 18.1 workdays, respectively.

Meanwhile, respondents from midsize organizations of 1,000 to 10,000 employees, a plurality of our response pool, reported above-average total remediation times of just over 19 business days. For these SME businesses, discovery and notification steps are on par with both smaller and larger peers. Prioritizing issues, finding a responsible fixer, and verifying

resolution, however, put a collective drag on the process, resulting in longer total remediation time. In fact, prioritization, assignment, and verification steps for midsize respondents are nearly 10% higher than the group average for those tasks and more than 19% higher than the small-business segment. As we'll examine further below, midsize businesses face a confluence of complications. They are large enough to embrace more sophisticated, multifaceted security programs and employ multiple security scanning tools but often lack the team size and manpower heft of their larger enterprise counterparts to help manage the complexity and scale of the risk telemetry such systems tend to create.

It's important to note that these remediation figures represent the average security organization. Individually, a significant number of respondents report far more protracted remediation cycles. Better than 1 in 10 (12%) put the total remediation process at approximately 90 business days or better than 4 calendar months.

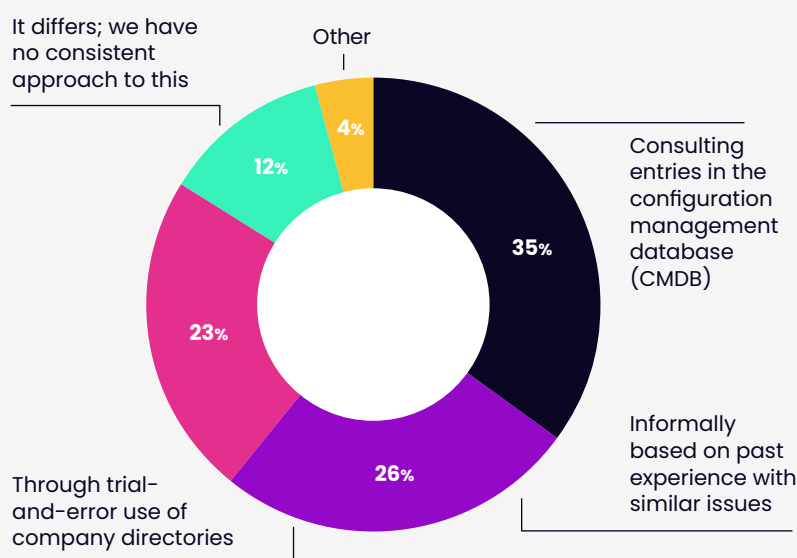
Moreover, all of these figures represent the estimated workload attributed to a single risk. For the typical organization, multiply this burden by 50,000 to 60,000 fixes flowing through the remediation system in any 6-month period, and it quickly becomes clear that the current fragmented and largely manual approach is unscalable and unmanageable.

FIGURE 3

Determining Correct Stakeholder

How do you typically determine the correct internal stakeholder responsible for remediating security weaknesses once they are discovered, assessed, and prioritized by your team?

61% Rely on Informal Knowledge



Data: Dark Reading survey of 108 IT cybersecurity professionals at companies with 100 or more employees.

Real Time-to-Remediate: A Host of Complications

Just what takes security teams so long to process fixes for the risks they find?

The answer involves a confluence of factors, starting with the ambitious nature of security programs in today's modern business organizations and complicated by the fractured way many of these programs are developed and managed. Consider how many responsibilities are on a typical security team's plate.

Pen testing, vulnerability management, and application security programs are nearly ubiquitous and feature on the docket for 2/3

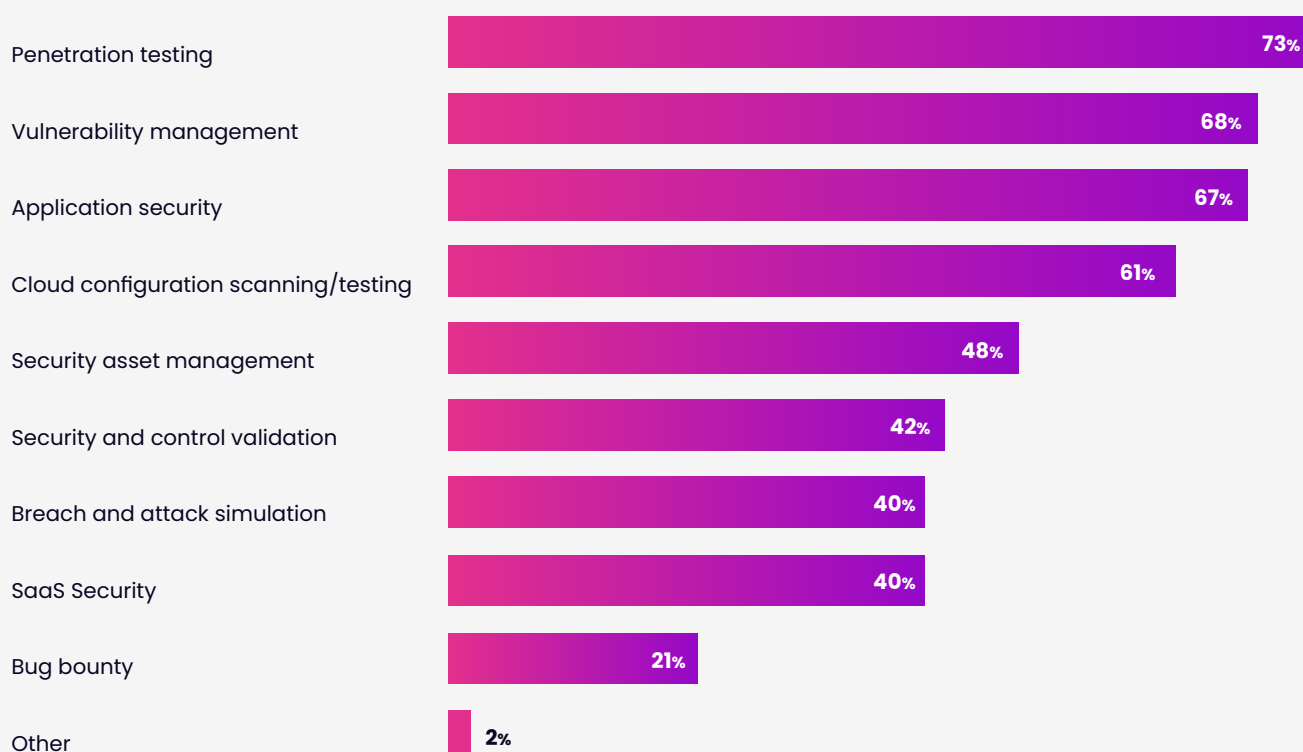
to 3/4 of respondents, regardless of company size (**FIGURE 4**). More than 60% of teams engage in cloud configuration scanning, while roughly 40% to 50% make use of asset management, controls validation attack simulations and software-as-a-service (SaaS) security.

To meet such ambitious security goals, the average organization manages 3 to 5 separate tools dedicated to actively identifying unexploited security weaknesses; more than 1 in 3 (36%) has 6 or more such siloed risk feeds to manage and nearly 1 in 5 (18%) has more than 10 (**FIGURE 5**).

FIGURE 4

Security Programs in Place

Which of the following security programs does your organization currently have in place?



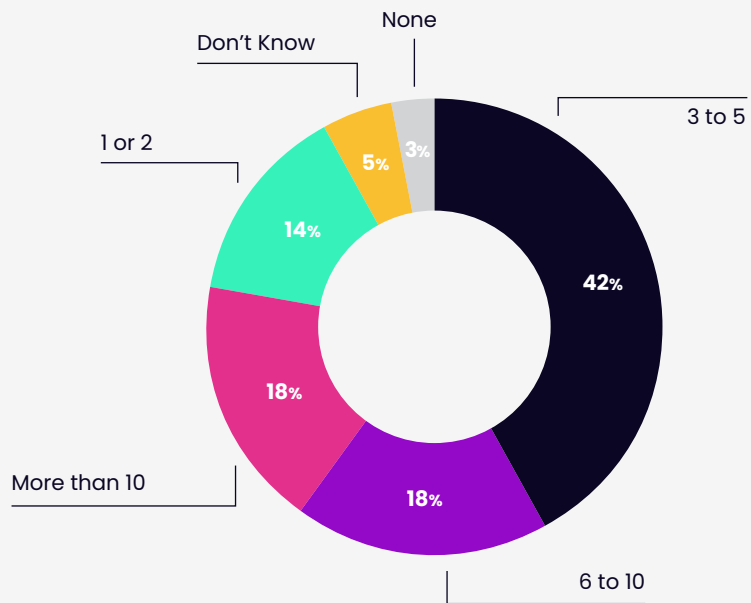
Note: Multiple responses allowed. **Data:** Dark Reading survey of 108 IT cybersecurity professionals at companies with 100 or more employees.

Data: Dark Reading survey of 108 IT cybersecurity professionals at companies with 100 or more employees.

FIGURE 5

Number of Cybersecurity Tools

How many separate cybersecurity scanners/tools that identify security weaknesses (that have yet to be exploited) does your organization have deployed currently?



The robust roster of responsibilities, each with its own siloed management tools and alerting systems, generate a constant flood of results and risk action items. For teams unable to systematically normalize, consolidate and automate their fragmented risk management efforts, all of this disparate telemetry conspires to down speed-to-remediation, the research shows.

Lacking a technical solution to corral and automate their processes, one-way security organizations attempt to get a handle on the risk remediation burden is by adding more team members to the mix.

While the average security workforce we measured supports 11 to 15 full-time members, about half

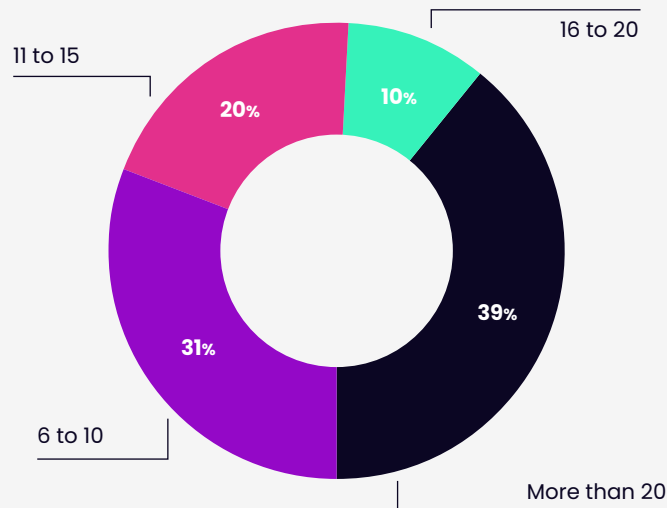
of respondents (49%) say they employ more than 16 security professionals; of that, 39%, a plurality in our dataset, have more than 20 full-time security workers on staff (**FIGURE 6**).

Adding to the security workforce might temporarily relieve the pressure in a system hamstrung by manual tasks and procedural bottlenecks. However, skilled security staff is increasingly harder to find and retain. Last year, (ISC)2 reported an additional 2.72 million workers are needed to staff unfilled positions requiring cybersecurity skills. Clearly, the shortsighted strategy of putting more boots on the ground pales in comparison to the deployment of technologies designed to reduce manual tasks and human intervention in the remediation life cycle.

FIGURE 6

Full-Time Security Team Members

How many full-time workers does your security team employ?



Note: Respondents with fewer than 6 full-time security team members were not included in the data set. **Data:** Dark Reading survey of 108 IT cybersecurity professionals at companies with 100 or more employees.

CONCLUSION

The Truth and Consequences of Sluggish Remediation

Saddling overburdened security teams with multiple-point solutions and onerous manual process makes their risk remediation efforts inefficient and unproductive. That's the clear takeaway from the State of Risk Remediation research data.

The less obvious — but no-less impactful — outcome of the report is the growing list of lost security opportunities. Organizations are squandering chances to improve the maturity of their corporate defenses, in large part due to the strain on capacity and capabilities resulting from lengthy, disorganized remediation workflows.

Asked how they would expand security initiatives if better, faster remediation could give them additional time, 70% of respondents said they would engage in additional architecture review, a critical, forward-looking task in the development and maintenance of secure, resilient IT systems (**FIGURE 7**).

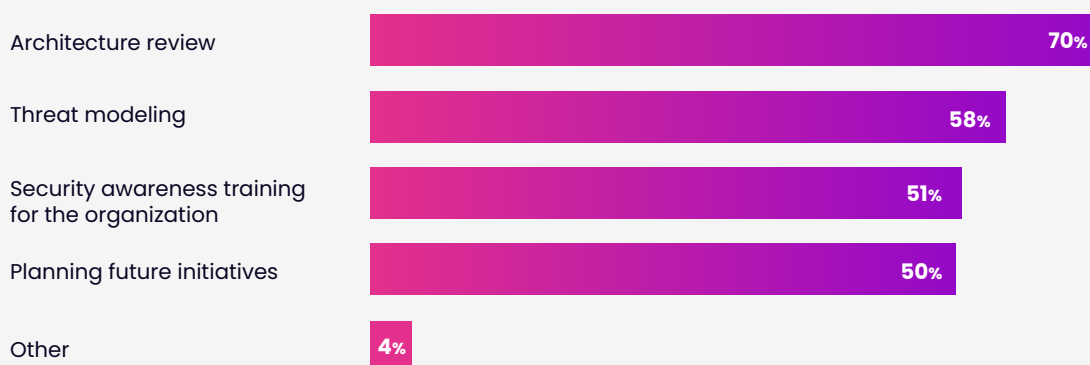
A majority of the security decision-makers we surveyed (58%) said they'd also expand threat modeling exercises, while 51% looked to bolster security awareness training within their organization. Both the development of threat registers and the training of end users are proven methods for improving defenses and reducing risk in corporate environments. Both are also well-known casualties, the first kinds of programs to get cut when the daily grind of risk management consumes available security team bandwidth.

Security professionals clearly want to improve their organization's security maturity and posture through advanced methodologies and robust controls. Those intentions remain largely unrealized, however. The burden of manual risk remediation is a tax that stifles security innovation for the vast majority of teams, our research reveals.

FIGURE 7

Security Focus if Given More Time

Which of the following security-related initiatives would your organization focus on if vulnerability remediation could be made faster and more efficient, thus giving your security team more available time?



*97% of respondents checked at least one of the options provided (Architecture review, Threat Modeling, Security awareness training for the organization, or Planning future initiatives).

Note: Multiple responses allowed. **Data:** Dark Reading survey of 108 IT cybersecurity professionals at companies with 100 or more employees.

KEY TAKEAWAYS



If there's one recurring theme in the research, it's that the combination of too many security tools and too much manual work being conducted across different teams blocks efforts to keep pace with today's risk reduction and remediation workloads for the majority of organizations. The State of Risk Remediation research provides a roadmap for improving efficiency and performance, bolstering organizational defense, and reducing risk — and security team's sanity. Key steps to improving risk reduction include:

Automating Risk Reduction Workflows Will Allow Security Teams to Focus on Strategic Security Initiatives

All of the steps noted by the survey respondents — steps such as locating the correct person responsible for fixing the issue, verifying successful remediation, communicating the request in language the stakeholder can clearly understand, coordinating and tracking the remediation progress — can all be automated with a purpose-built risk reduction platform. Employing judicious automation technology at every point in the process and across disparate scanning and management platforms frees teams to focus on more strategic security initiatives while also improving remediation efficiency and performance.

Acknowledging Remediation Has Many Moving Parts Will Contribute to More Effective Remediation

Not all risks are created equal, but many teams still treat remediation as a largely binary issue. Risks are either fixed, or they are not. Effective prioritization, along with the ability to aggregate congruent issues in a single remediation ticket, are key steps in making risk remediation manageable. This effort depends on an accurate assessment of risk. Every subsequent part of the remediation process depends on this understanding of organizational risk tolerance and the assignment of remediation priorities based on that risk. Combining threat intelligence, historical attack activity, and internal asset classification helps teams develop a better view of what's really at stake.

Risk Reduction Workflows Require Specific Security Knowledge

Off-the-shelf workflows like those built into many general-purpose business process automation platforms may be fine for streamlining generic areas of the business, but risk remediation is a different breed of challenge. In this critical domain, workflows need to be infused with specialized security knowledge. From data normalization to rules and policy enforcement, an automated remediation workflow tasked with organizational risk reduction is only as good as the security expertise it's built on.

Methodology

Seemplicity commissioned Dark Reading to research timelines, approaches, processes, and perceptions related to the remediation of cybersecurity risks across the organization.

The survey queried 108 IT and cybersecurity managers and executives from midsize and large enterprises on perceptions, strategies, capabilities, capacity, and tactics related to risk management at scale. Issues covered include discovery, prioritization, interdepartmental communication, resolution, and closure of security risks affecting the organization. Respondents' company sizes ranged from a minimum of 100 employees to more than 10,000. In addition to having 100 or more employees, respondents were also screened to ensure that they work at companies with at least 6 full-time security team members.

The survey was conducted online in October 2022. Respondents were recruited via emailed invitations containing a link to the survey. The emails were sent to a select group of Informa Tech's qualified database. Informa is the parent company of Dark Reading. Informa Tech was responsible for all survey administration, data

collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing U.S. privacy laws.

9% of the respondents are from organizations with between 100 and 499 employees, 14% work at organizations that employ between 500 and 999 workers, 37% represent firms with between 1,000 and 4,999 employees. 12% represent businesses with between 5,000 and 9,999 employees, and 28% come from organizations with 10,000 or more workers.

The survey queried respondents with job titles that include chief information officer (CIO), chief information security officer (CISO), chief technology officer (CTO), other security executive (CSO, VP/SVP Security), head of information security or cyber security, head of risk management, IT management and staff, and security architect.

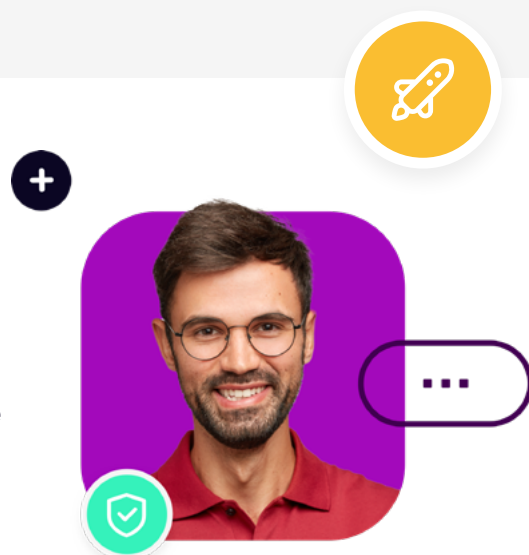
Respondents' organizations represent more than 20 vertical industries, including communications, banking and financial services, technology, manufacturing, healthcare, aerospace, education, and government.

About seemplicity

Seemplicity's mission is to bring every aspect of the risk reduction workflow into one automated platform and enable security teams to oversee the entire remediation process.

Security teams can finally cut noise and manual work and see remediation through. Smart aggregation rules, automated visual workflows, and smart find-the-fixer algorithms ensure every security issue is handled from discovery to resolution.

Seemplicity was founded by cybersecurity veterans Yoran Sirkis, Ravid Circus, and Rotem Cohen Gadol, and its customers include Fortune 500 and publicly traded companies.





The Risk Reduction Platform for Security Teams

SEEMPLICITY.IO