Cyber Threat Readiness

2023 Report

SWIMLANE

Table of Contents

JAMES BREAR
CEO of Swimlane

At the time of writing this, there are more than 660,000 open cybersecurity roles in the U.S. alone. Last year saw 317,050 open roles in Europe, the Middle East and Africa (EMEA) and 2,163,468 open roles in the Asia-Pacific (APAC) region. A prevailing truth looms large: There will never be enough skilled cybersecurity talent to close the widening gap. Organizations in every industry and every corner of the world are struggling to find and retain qualified professionals who can handle the complexity and severity of threats.

With growing challenges, the Biden Administration's National Cybersecurity Strategy and the U.S. Securities and Exchange Commission's incoming cybersecurity regulations are putting a spotlight on the requirement to close the gap in enterprise security. And with the added threat of AI and machine learning in the hands of threat actors, it's only a matter of time before AI-powered attacks outpace defender efforts. This will impact every enterprise, no matter the industry or vertical, calling for organizations to scale their defenses.

Companies must confront these challenges and embark on a proactive problem-solving journey. Organizations need a clear path forward to ease the burden on security teams so they can focus on high-level threats while also demonstrating value in security investments.

At Swimlane, we wanted to play an active role in closing the industry-wide gap in cybersecurity, and to do so, we went directly to the source. We surveyed more than 1,000 cybersecurity professionals across all levels and key industries and from around the world to unpack the true struggles of people, process and technology.

We hope this report shines a light on the fundamental cybersecurity issues organizations face, from the security teams on the ground addressing threats in real-time, to the executives tasked with meeting evolving regulations. May these findings serve as a catalyst for dialogue, igniting discussion that paves the way for a new era of cybersecurity, where an optimal balance between human expertise and technological advancements can be achieved.

Sincerely,

James Brear

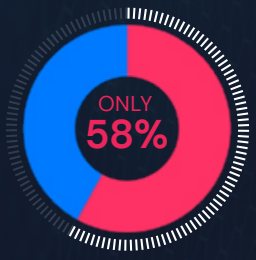
Executive Summary

Amid the growing number of security alerts, emerging threats and complex security processes required to secure organizations today, we sought to learn more about the current state of enterprise security operations (SecOps). Swimlane partnered with Dimensional Research, a leading independent research firm, to conduct ***a global survey of more than 1,000 security professionals and executives across North America, Europe, the Middle East and Africa (EMEA), and the Asia-Pacific (APAC) region.***

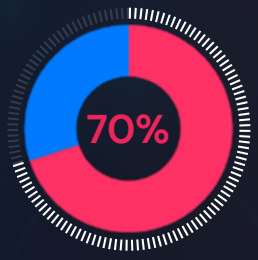
Together we investigated the perceptions of cybersecurity among on-the-ground security professionals and executives, the current trends in hiring and retaining talent, and the effectiveness of tools leveraged to address today's top cybersecurity challenges. In this report, we explore some of the key findings from our survey.

Key Findings

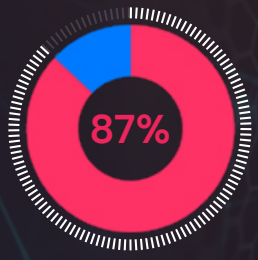
A Top-Down Security Disparity



58% of companies address every security alert.

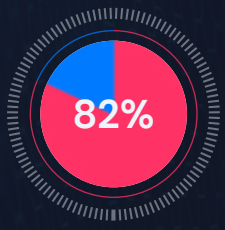


70% of executives think all alerts are being handled, starkly contrasting the front-line roles that address the alerts and reported only 36% are handled.



87% of executives believe that their security team possesses what is required for the successful adoption of heavy scripting security automation tools. Only 52% of front-line roles stated they have enough experience to use heavy scripting security automation tools properly.

Struggle to Hire and Retain Talent Amplifies Risks



82% of companies report it takes three months or longer to fill an open security position, with 34% reporting it takes seven months or more.

One-third of organizations believe they will never have a fully-staffed security team.

More than 9 out of 10 of participants report business issues resulting from security team turnover.

84% of respondents in the **healthcare sector** said security team turnover presents a risk to their organization.

80% of respondents in the **government sector** said security team turnover presents a risk to their organization.

78% of respondents in the **financial services sector** said security team turnover presents a risk to their organization.

The Implications of Security Automation

78% of organizations that address every alert use a **low-code security automation** solution.

98% of participants cited benefits to automation solutions with a low-code user experience, citing the **ability to scale the solution with the team's experience with less reliance on coding skills**.

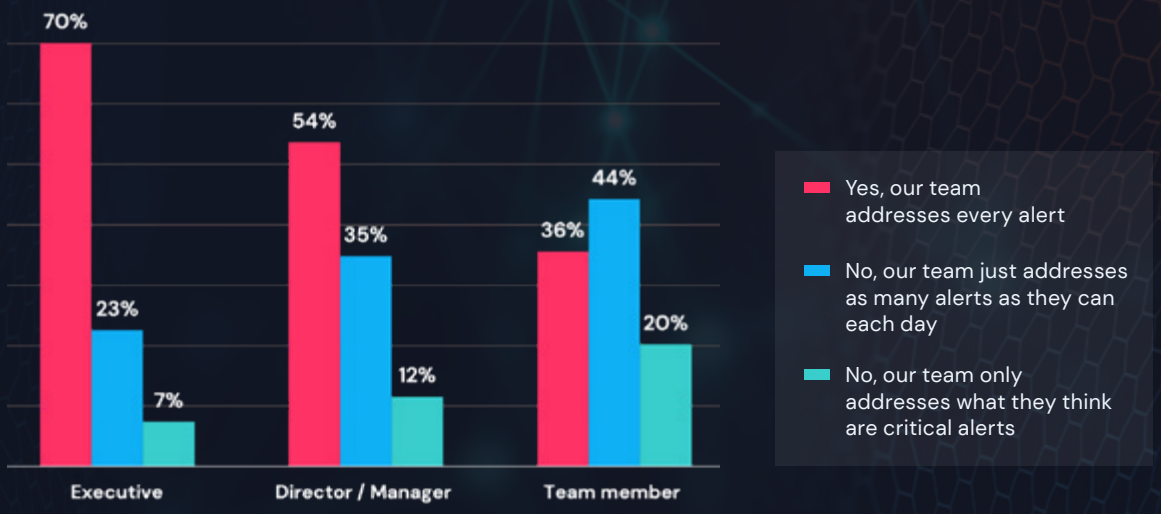
SWIMLANE

A Top-Down Security Disparity

Cybersecurity has undergone a significant shift, transforming from an IT problem to a pervasive business imperative. Executives now understand that it is a matter of when - and not if - they will experience a cyberattack. As a result, cybersecurity now has a seat at the table of executive and boardroom conversations. Proposed regulations from the U.S. Securities and Exchange Commission set to be finalized in the fall of 2023 will further these conversations, as public companies will need to disclose whether their entire board, specific board members or a committee are responsible for cybersecurity within their business. One problem remains: Executives and security analysts are not aligned.

Despite the increased discussions at the C-suite and boardroom level, a glaring disparity has emerged between executives who believe that every security alert is being addressed and the teams on the ground addressing the alerts. 70% of executives across the globe believe all alerts are being handled, starkly contrasting the 36% of front-line roles that address the alerts. The truth is only 58% of organizations are actually addressing every single alert.

At your organization, can the security team address every security alert that comes in?
(by seniority)

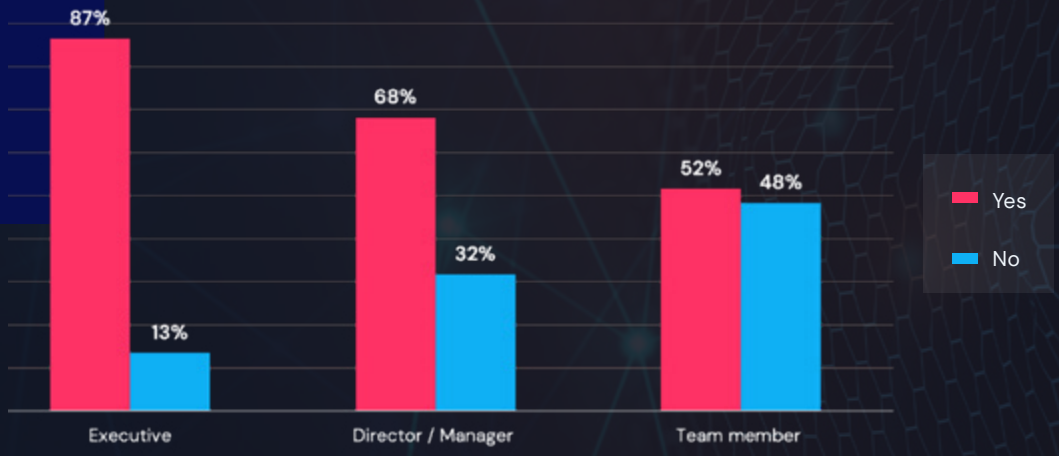


SWIMLANE

When it comes to building a fully-staffed security team, 82% of executives believe they will eventually have a fully-staffed security team, but only 52% of security team members think this will be a reality.

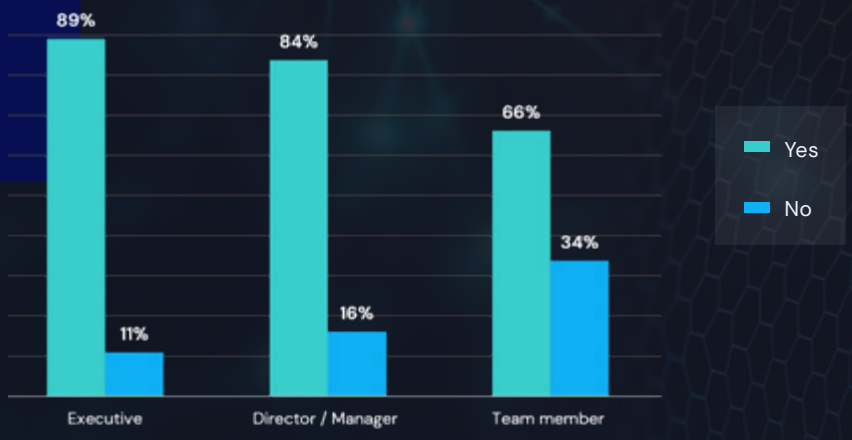
The disparity doesn't stop there, as there is a notable disconnect between the team's skill-set and available resources to adopt heavy scripting automation tools. While 87% of executives believe that their security team possesses what it takes for successful adoption, managers and frontline personnel expressed an opposing viewpoint with only 52% of front-line roles stating they have enough experience to use heavy scripting security automation tools properly.

In your opinion, does your company's security team have enough experience and coding resources to utilize a 'full-code' security automation solution?
(by seniority)



Aside from automation platforms, executives hold the belief that SIEM solutions are yielding tangible benefits. However, a contrasting sentiment emerges from managers and security team analysts who believe it is difficult to verify SIEM operations. 89% of executives are confident their SIEM solution is operating as intended, while only 66% of team members share the same sentiment.

Can your organization verify that your SIEM solution is actually operating as intended?
(by seniority)



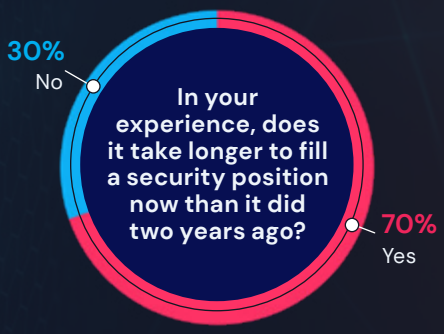
This undeniable top-down disparity shows an evolving disconnect between executive perception and the boots-on-the-ground reality of security teams. The security industry at large lacks technology that provides a system of record. This type of tool is essential in bridging the gap as it gives executives actionable insights to know the efficacy of their systems, the processes in place and their people. Clearly, the solutions in place today are no longer cutting it.

Struggle to Hire and Retain Talent Amplifies Risks

Security analysts are expected to investigate and remediate thousands of alerts daily while keeping up with an ever-evolving threat landscape, new technology and under-staffed security operations centers (SOCs). Adding to this, the current pool of potential workforce is failing to keep up with the demand, primarily due to a lack of interest among young individuals entering the job market. The fast-paced world of cybersecurity creates a challenge for organizations looking to find candidates with the right combination of technical skills, experience and industry-specific knowledge.

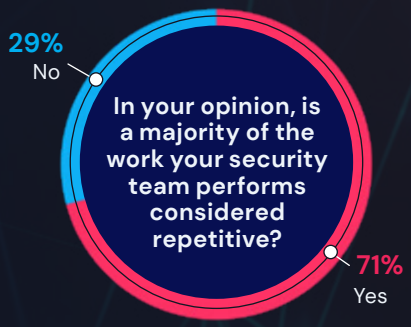
Facing a brutal market, 82% of organizations report it takes three months or longer to fill a cybersecurity role, with 34% reporting it takes seven months or more. 70% of companies also report it takes longer to fill a cybersecurity role now than it did two years ago. The challenge has led one-third (33%) of organizations to believe they will never have a fully-staffed security team with the proper skills. As noted above, this is where the disparity lies between executives and security teams on the reality of building a full team.

At your organization, on average how long does it take to fill a security staff position?

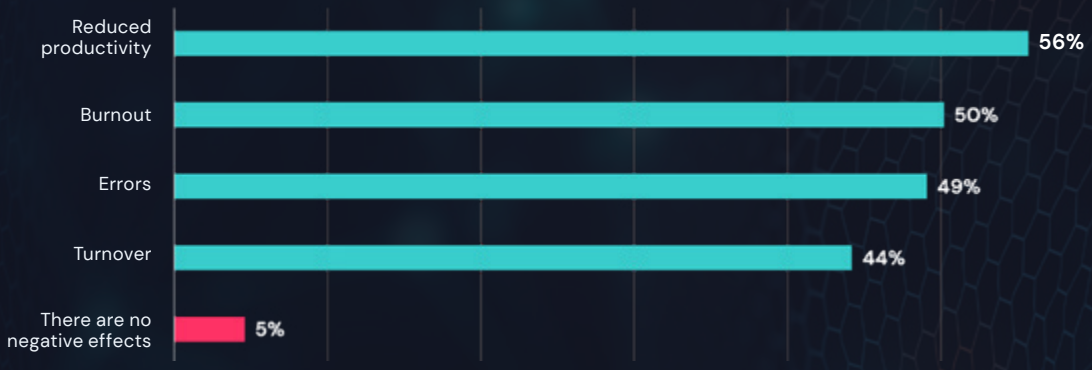


The struggle to hire new cybersecurity talent is not unique to any specific region or country; it's a global issue. 77% of respondents from EMEA, 70% from North America and 60% from APAC said it's taking longer to fill a security position now than it did two years ago.

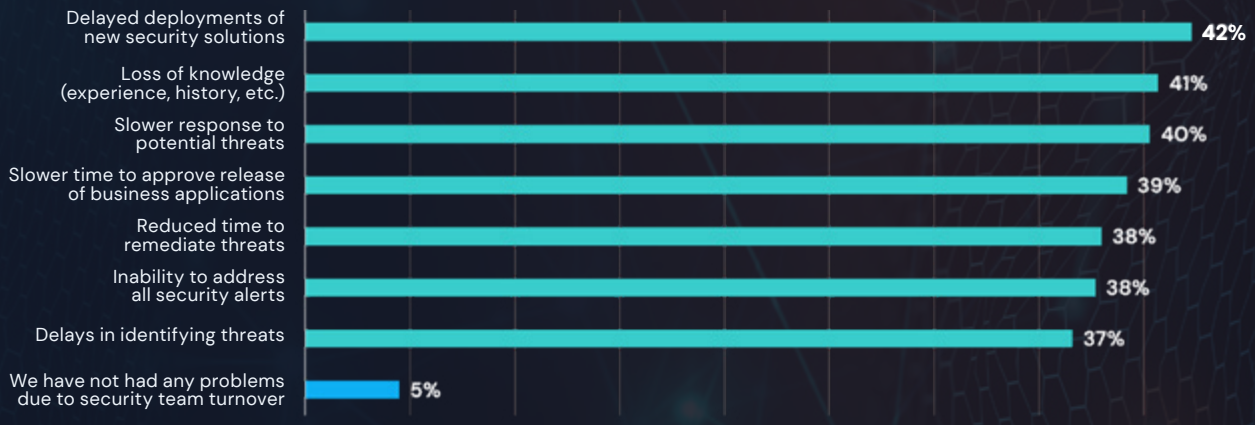
The exhausting and monotonous routine for a majority of analysts has led to alarming levels of employee turnover across the industry, reduced productivity, and burnout. This widespread attrition poses a substantial risk to businesses, jeopardizing their operational stability and resilience. More than nine out of 10 participants report business issues resulting from security team turnover, including slower threat identification, response, remediation, and the inability to address alerts.



In your experience, what are the negative effects of continuous repetitive tasks?

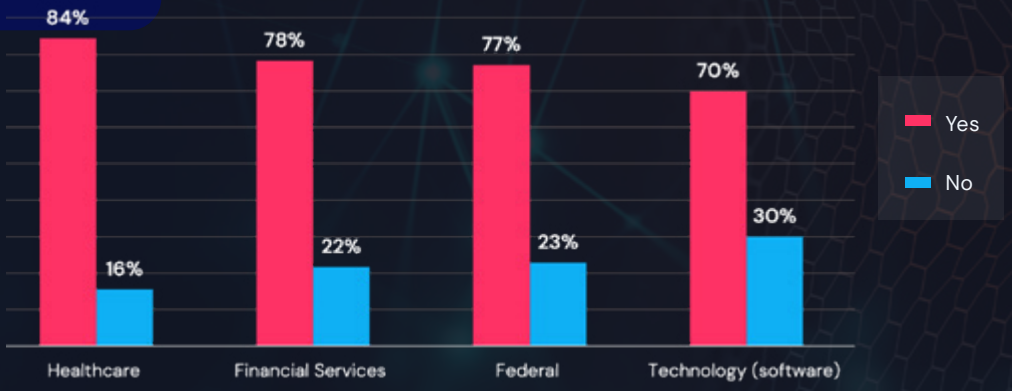


What problems has your organization experienced due to security team turnover?



Healthcare, government and financial services participants stated they face increased risk to their organizations due to security team turnover. This comes as no surprise as these sectors remain key targets for threat actors, all while facing industry-specific regulations. This alarming reality underscores these industries' ongoing struggle with how to contend with malicious actors while operating with leaner teams and constrained resources.

Does security team turnover present a risk to your organization?



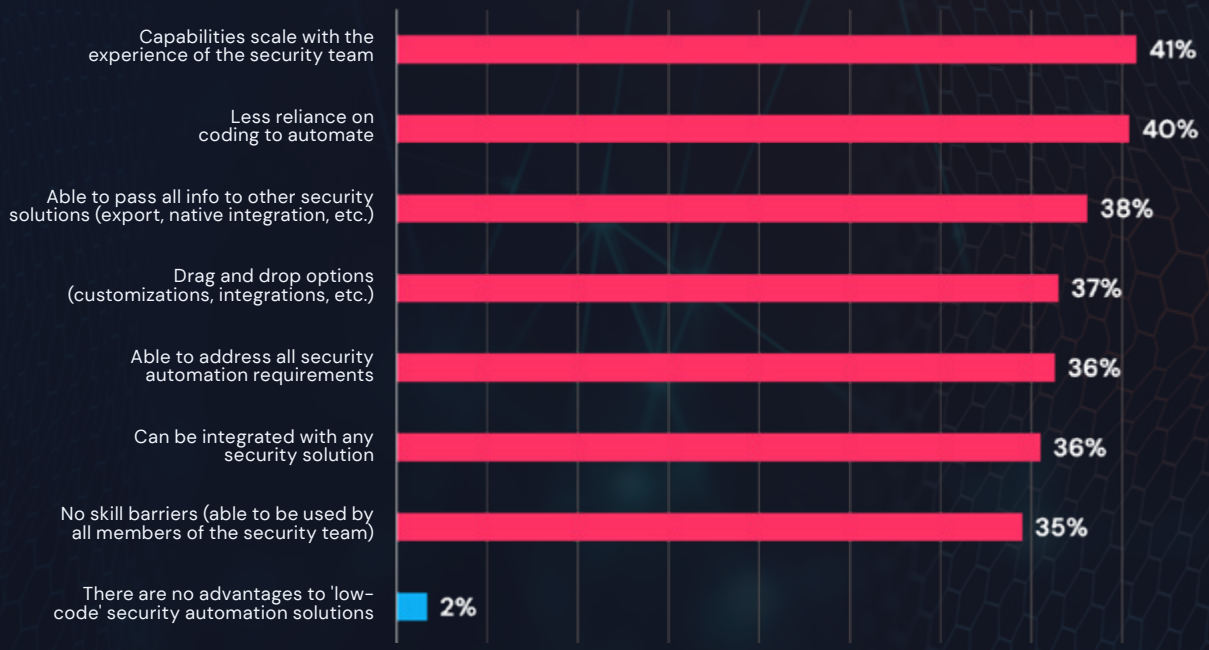
Amidst the persistent turnover and perpetual challenge of finding suitable replacements, preserving institutional knowledge remains an ongoing struggle for security teams. The reality is that in order to retain and attract the talent today's enterprises require, organizations must empower their security teams with the right technology that can keep up with the pace of threats. The modern threat actor will leverage any means necessary to take down a business, which is only amplified by the rise of tools that aid in automating attacks. To combat aggressive and sophisticated threats, security teams must fight fire with fire.

The Implications of Security Automation

The previous sections of this report have made it abundantly clear that security teams bear an overwhelming burden to prevent business-ending threats. They face thousands of alerts daily that must be addressed, with each alert requiring a handful of manual tasks that must be performed before incident response even begins. SecOps teams are tasked with maintaining compliance in a constantly evolving regulatory landscape. Compounded with a lack of executive understanding and ongoing talent shortages, it's clear that today's cybersecurity professionals desperately need solutions that will empower their teams no matter their size or resources available.

Organizations are leveraging low-code security automation to automate away tedious tasks so that they can address every alert effectively and efficiently. Over three-quarters (78%) of organizations that handle every alert use low-code security automation in their security stack. But the benefits don't stop there. An astonishing 98% of participants cited advantages of low code security automation solutions, such as the ability to scale the implementation based on the team's existing experience and with less reliance on coding skills. When examining the specific geographies of North America, EMEA and APAC, the percentage of participants who observed the advantages of low-code security automation stayed the same across all three regions.

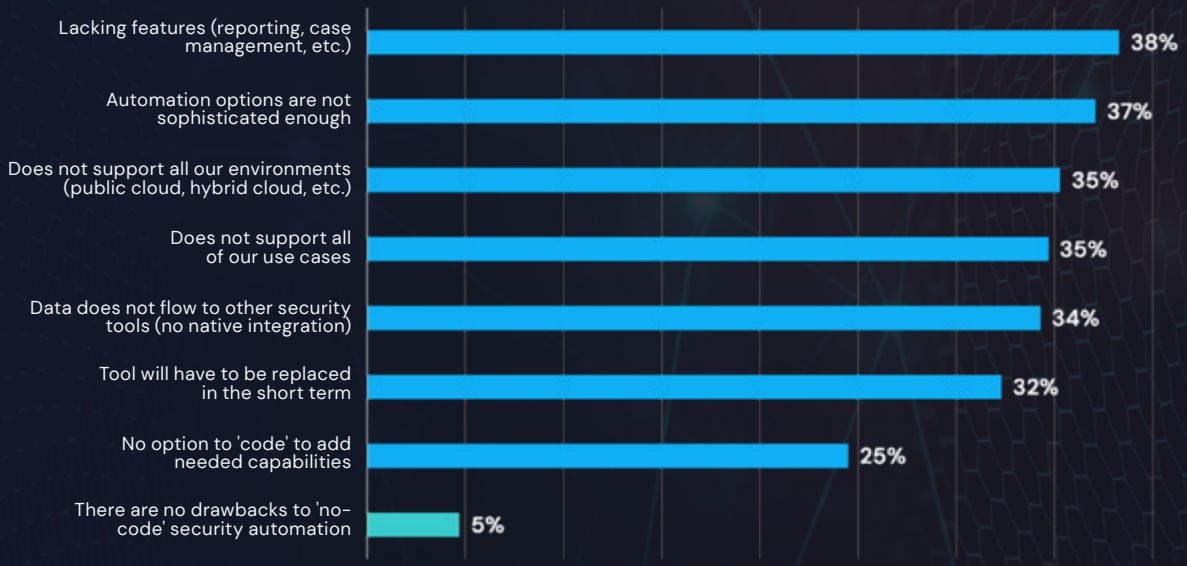
In your experience, what are the advantages of a 'low-code' security automation solution?



SWIMLANE

While no-code tools appeal to organizations with limited resources and smaller security teams that may not have the required scripting skills that full-code automation platforms require, companies are finding that these tools lack customization and sophisticated features that could benefit the team's ability to scale with the business and team as it grows. This makes no-code tools a short-term solution for organizations looking to make simple automated tasks accessible.

In your experience, what are the drawbacks of 'no-code' security automation?



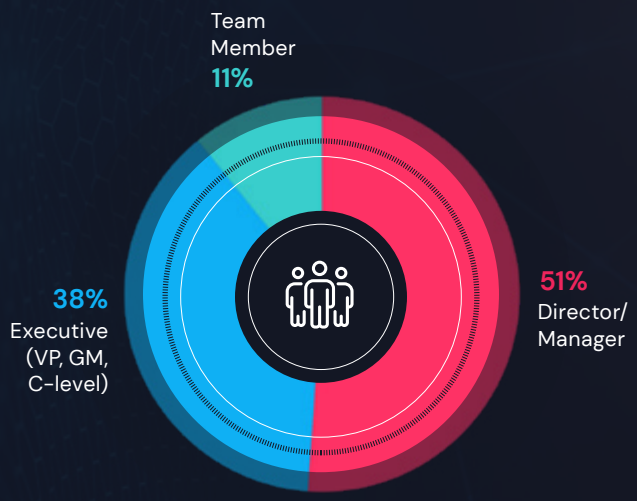
Today's enterprise security teams are in need of solutions that arm and empower security teams to address and overcome pervasive security challenges. Traditional Security Orchestration, Automation and Response (SOAR) solutions can be burdensome due to their required extensive scripting. On the other hand, no-code security automation is simplistic and often lacks necessary case management and reporting capabilities. Low-code security automation offers a solution that is both approachable enough for those with no coding experience and sophisticated enough to satisfy the most demanding security operations. These low-code solutions help address alerts faster to help overcome process fatigue and talent shortages, while also helping organizations quantify the business value of the solution in a UX-friendly, visual way that is easy to communicate to executives and the board of directors.

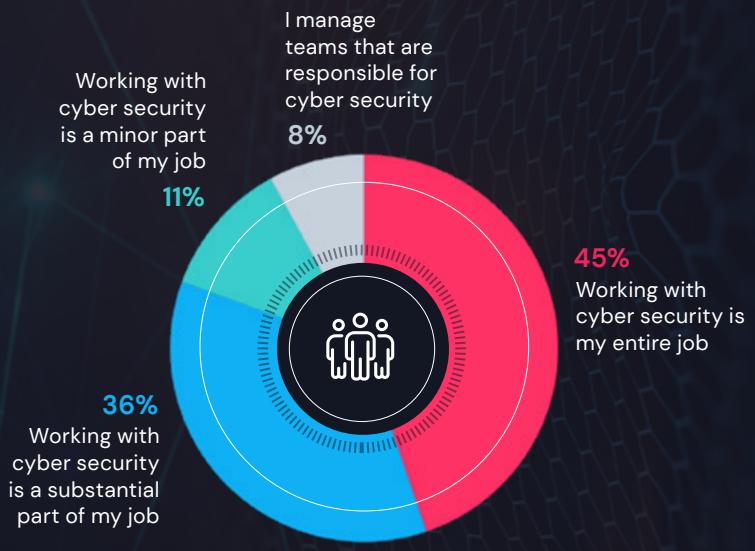
Methodology

Security professionals and executives at enterprise companies with at least 5,000 employees and $600M in revenue were invited to participate in a survey on their company's security practices. The survey was administered electronically, and participants were offered a token compensation for their participation.

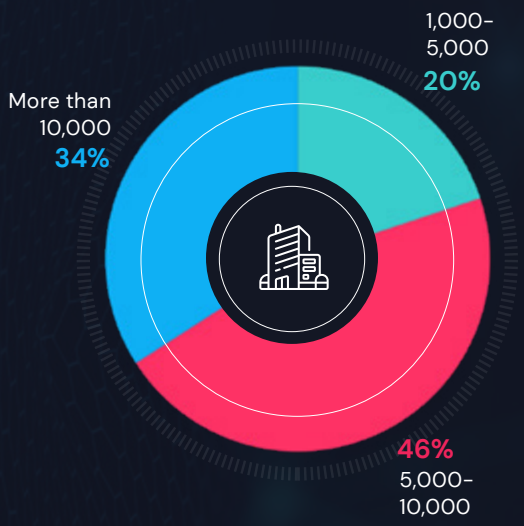
A total of 1,005 qualified participants completed the survey. All participants had enterprise security responsibilities, from frontline security roles to senior executives. Participants were from 5 continents providing a global perspective.

Individuals Represented

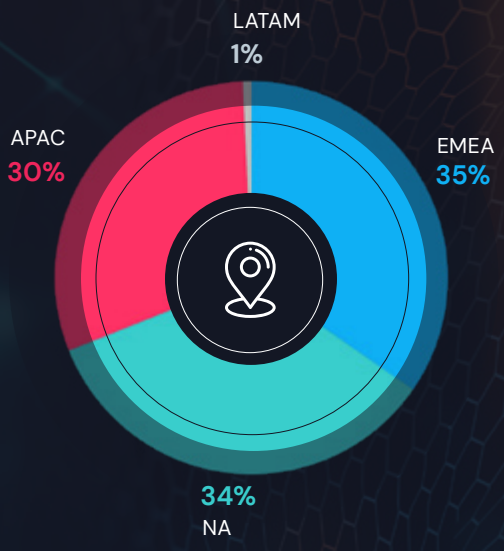




Companies Represented



Regions Represented



SWIMLANE

The following definitions were used in the context of the survey and report:

Heavy scripting security automation
Refers to an automation solution that requires the extensive use of coding or scripting languages to create the automation. This often requires dedicated coding experts who are capable of creating complex workflows and processes using scripting languages, such as Python.

No-code security automation
Refers to an automation solution that offers a codeless approach to security automation utilizing menu options, taskbar buttons, and drag-and-drop capabilities to create the automation.

Low-code security automation
Refers to an automation solution that primarily utilizes menu options, taskbar buttons, selectable items, and drag and drop to create the automation. It also enables more customization and expansion with the option to use coding or scripting languages to create more sophisticated automation.

About Swimlane

Swimlane is the leader in cloud-scale, low-code security automation. Swimlane unifies security operations in-and-beyond the SOC into a single system of record that helps reduce process and data fatigue, overcome chronic staffing shortages, and quantify business value.

The Swimlane Turbine platform combines human and machine data into actionable intelligence for security leaders. For more information, visit **swimlane.com**.

About Dimensional Research

Dimensional Research provides practical market research for technology companies. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business. Our researchers are experts in the applications, devices, and infrastructure used by modern businesses and their customers. For more information, visit **www.dimensionalresearch.com**.

SWIMLANE