SANS | GIAC CERTIFICATIONS

2026 Cybersecurity
Workforce Research Report

The Evolving Cyber Workforce:

AI, Compliance, and the Battle for Talent

Table of Contents

A Note on Survey Data

This report draws from 947 global respondents. Percentages exclude "Unknown/Unsure" responses unless noted. Questions permitting multiple selections (e.g., "select up to 3") may total more than 100%.Individual graphs specify their methodological basis for precision.

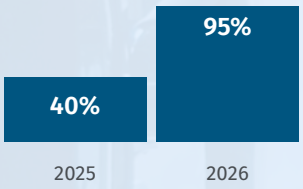
Key Findings

The cybersecurity workforce is undergoing a fundamental transformation. Organizations are rebuilding their teams from the top down as artificial intelligence (AI) disrupts traditional entry points while regulatory compliance demands create new frameworks for skills validation. This convergence is producing a widening skills gap that organizations struggle to close, even as they increasingly recognize that having the right abilities matters more than simply adding headcount.

Data from the 2026 Cybersecurity Workforce Survey by SANS | GIAC reveals stark shifts compared to past years. Workforce Framework adoption grew significantly, as organizations turn to structured role definitions. Regulatory pressure drives dramatic changes in hiring: the need for specialists in new roles nearly doubled year-over-year, while additional hiring for existing skills increased substantially.

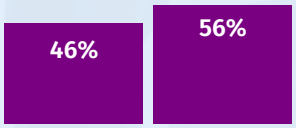
Most striking, while skills gaps emerged as the dominant workforce concern for the first time in 2025, that trend has accelerated for 2026. When isolating the core question, the skills gap now dominates at 60% (up from 52% in 2025), compared with 40% for staffing shortages. Career progression simultaneously emerged as a major concern after barely registering in previous years, more than tripling in importance.

Significant Regulatory Impact on Hiring:



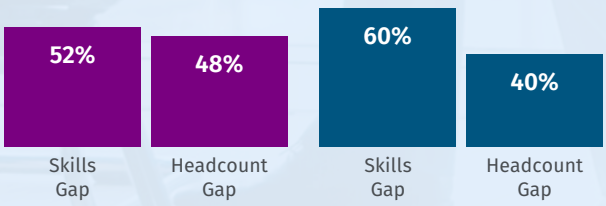
↑ 55-point increase

Organizations Using NICE or ECSF:

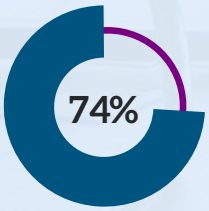


↑ 10-point increase

Skills Gap is Growing



2025 (4-point gap) **2026** (20-point gap)



of Cyber Teams Are Changing Team Size & Role Structures Due to AI

Four Key Dynamics Define Current Transformations:

1. AI is Restructuring Entry-Level Work

While most organizations still lack comprehensive AI governance policies, AI's impact on workforce composition is already visible. Among organizations experiencing role changes, SOC and security analysts lead reductions, followed by threat intelligence analysts and incident responders. These are precisely the entry-level positions where repetitive analysis—tasks increasingly handled by AI—has traditionally served as the training ground for junior cybersecurity professionals. The automation of entry-level tasks is changing the skill requirements for how junior professionals enter the field — shifting from manual analysis toward oversight, validation, and AI-augmented investigation.

2. Regulatory Compliance Drives Workforce Transformation

New requirements from regulations such as NIS2, CMMC, DORA, DoD 8140, and the SEC are reshaping hiring practices, even though many directives are less than a year old. These regulatory pressures accelerate workforce standardization through framework adoption and specialist hiring, forcing organizations to validate capabilities they may not have previously documented. The majority (68%) of organizations report moderate to extreme regulatory impact on their hiring practices, with 54% creating entirely new specialist roles to meet compliance requirements.

3. Organizations Rebuild from the Top Down

Rather than developing junior talent, organizations are hiring senior professionals to meet immediate compliance and capability needs. Senior leadership and CISOs now control the majority (53%) of hiring decisions, while expert and senior positions rank as most difficult to fill. By contrast, entry-level roles present minimal recruitment challenges.

Nearly half of organizations identify expert (27%) and senior (22%) roles as most difficult to fill, with mid-level positions (23%) close behind—collectively representing 72% of reported recruitment difficulties. This creates a career progression crisis that begins at the mid-career level and intensifies through senior and expert positions, where professionals see limited advancement opportunities while organizations struggle to build sustainable talent pipelines.

4. Skills Gap Pulls Further Ahead of Headcount Gap

The skills gap (60%) now outpaces headcount shortages (40%) as organizations' primary workforce challenge—up from 52% last year and creating a 20-percentage-point differential, compared to just 4 points in 2025. However, recognition alone hasn't driven solutions. The constraints preventing closure create a self-reinforcing cycle.

Budget limitations and time constraints dominate as obstacles. Teams caught in operational firefighting lack bandwidth for development, while budget pressures force organizations to prioritize immediate needs over long-term, broad talent development. When examining training specifically, lack of time and budget emerge as the overwhelming barriers. In response, certification has become a critical validation tool, with organizations increasingly turning to structured frameworks and trusted credentials to address capability gaps even when traditional training remains constrained.

The AI Transformation: Early But Impactful

AI has arrived in cybersecurity workforce management with measurable, practical effect — not as sweeping revolution, but as steady operational change already visible in how organizations build and staff their security teams. While most organizations are still developing governance frameworks, AI's influence on hiring practices, role composition, and team dynamics is clearly present in our data. What emerges is an industry in active adaptation: restructuring workflows, creating new role categories, and rethinking what entry-level contribution looks like alongside AI tools.

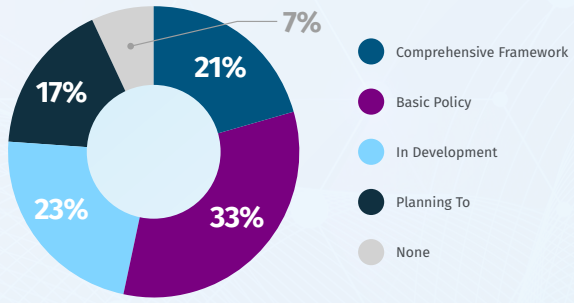
> "The industry hasn't invested yet in giving management the tools to understand what developing people means in an AI-enabled world."
>
> **Jay Bhalodia**
> **Rebuilding the Pipeline:** How Microsoft Balances AI Acceleration with Workforce Development

Governance Lags Behind Adoption

AI adoption—measured here as organizations' governance policies, training programs, and reported tool usage—reveals a significant disconnect from operational readiness. The governance data illustrates this gap clearly. 54%of organizations report having AI security policies (see graph 1). Roughly three-quarters of organizations are either implementing or still building governance structures, with only one in five having comprehensive frameworks ready. Despite this immaturity, organizations report AI influencing critical workforce decisions across the majority of these organizations.

This maturity gap manifests in observable patterns. First, policy without practice: while 54% report governance policies exist (see graph 1), only 38% provide comprehensive training (see graph 2) either for all staff or cybersecurity teams, meaning frameworks exist on paper but teams lack guidance on implementation. Second, impact without oversight: 74% **report AI affecting team size and structure** (see graph 3), yet 24% have no governance plans (see graph 1)—allowing tools to reshape operations before formal oversight exists. The survey measures the extent of impact rather than its direction; whether teams grew, shrank, or changed composition varies by organization. Third, adoption without alignment: employees use AI tools in daily work while organizations scramble to define acceptable use. Readiness failures manifest as inconsistent tool usage across teams, unclear responsibility of AI governance, and inability to track unsanctioned AI deployments—creating compliance and security risks that policies haven't yet addressed.

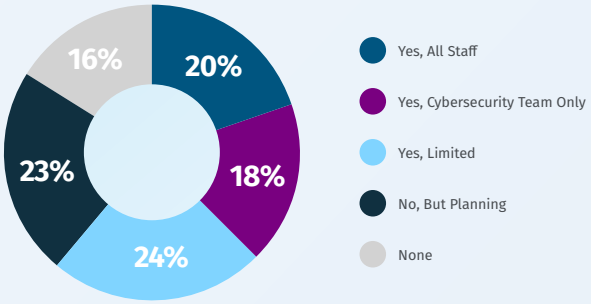
Graph 1: Does Your Organization Have an Organization-wide AI Security and Governance Policy?



Key Takeaway:
AI security governance is still in early days

Training programs show a similar gap. Only 20% provide comprehensive AI security training for all staff, while another 18% restrict training to cybersecurity teams (see graph 2). As a result, fewer than half of organizations (38%) have any form of comprehensive AI security training.

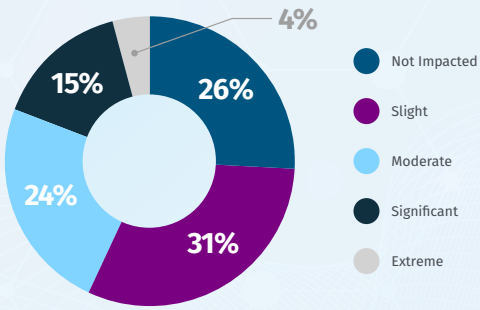
Graph 2: Does Your Organization Provide AI Security Training?



The Impact: Already Measurable

Despite governance uncertainty, AI's influence on team composition is undeniable. 74% describe some degree of AI influence on team composition — with the most common response being slight adjustment (31%), and 39% reporting moderate-to-significant restructuring. (see graph 3). Organizations are feeling AI's workforce effects before establishing the policies and training to manage that transformation.

Graph 3: AI's Impact on Cybersecurity Team Size



Key Takeaway:

AI is influencing how teams are structured — primarily through efficiency, not headcount reduction.

The Shadow AI Challenge

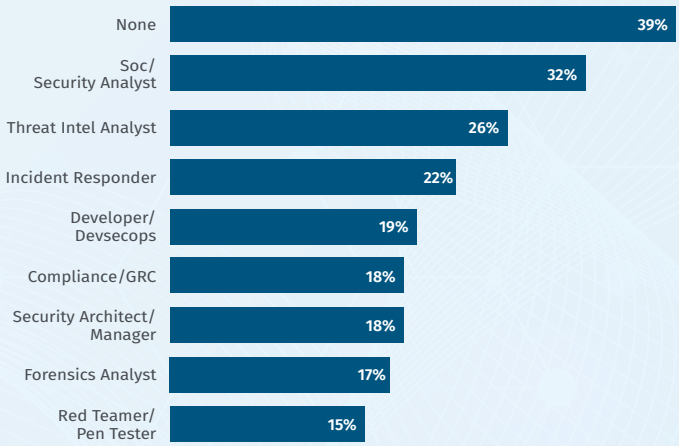
The governance uncertainty creates an immediate operational challenge. Organizations report AI reshaping team composition (74%, see graph 3) even as many lack formal governance plans (23%, see graph 1) or comprehensive training programs (only 38% provide training despite 54% having policies, see graphs 2 and 1). This gap between deployment and oversight—where AI tools influence operations before frameworks exist to manage them—creates compliance and security risks that organizations are addressing reactively rather than proactively.

Role Transformation: Who Gets Reduced, Who Gets Created

Organizations report early effects on team composition that reveal a clear pattern. While 39% report no role reductions, among those experiencing changes, SOC and security analysts lead reductions (32%), followed by threat intelligence analysts (26%), incident responders (22%), and developer/DevSecOps roles (19%). These are positions where repetitive analysis and pattern recognition form significant workload components (see graph 4).

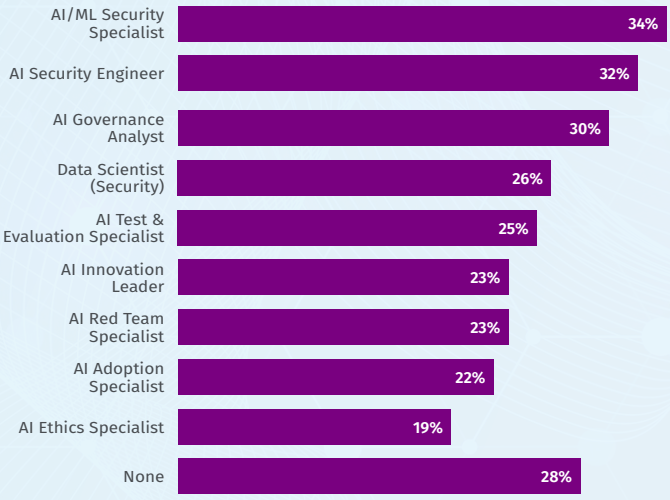
Graph 4: Roles Where AI Is Changing Task Composition (Among organizations reporting role changes)

(Respondents selected all that applied)



Simultaneously, organizations are creating new AI-focused security positions. Among those adding roles, 34% have filled AI or machine learning (ML) security specialist positions, 32% added AI security engineers, and 30% employed AI governance analysts. Specialized positions, such as security-focused data scientists (26%), AI red team specialists (23%), and AI ethics specialists (19%), signal that organizations aren't simply automating existing work (see graph 5)—they're creating entirely new expertise domains.

Graph 5: AI-Related Cybersecurity Roles That Have Been Newly Created or Filled *(Respondents selected all that applied)*

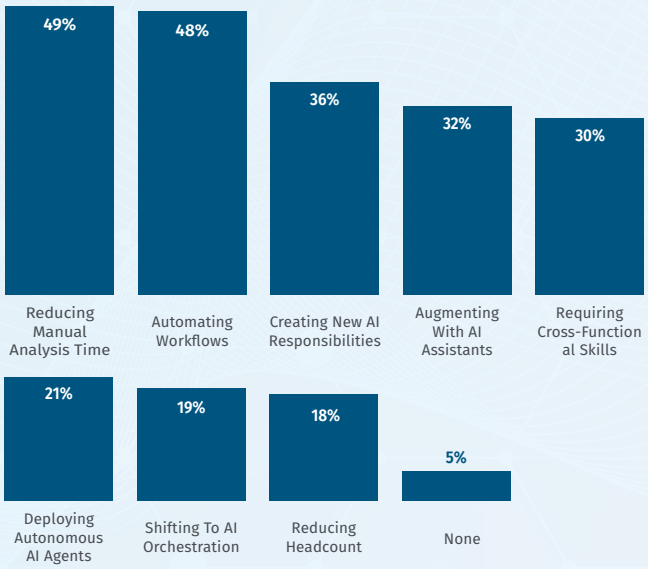


As organizations automate analysis and create AI-centric roles, they report acute skills needs layered on top of existing shortages. AI governance, risk, and compliance capabilities top required competencies, followed by data security for AI, securing AI systems, and AI-powered threat detection. These specialized requirements represent a compounding challenge: organizations must staff for both traditional cybersecurity and an entirely new AI-security domain.

AI's Impact: Efficiency Gains and Evolving Roles

Organizations report impacts that reveal nuance beyond simple workforce reduction. AI's value is concentrated in efficiency gains, with 49% highlighting reduced manual analysis time and 48% pointing to workflow automation, versus only 16% citing workforce reduction. However, deeper changes follow: 36% are creating new AI-specific responsibilities, 32% are augmenting teams with AI assistants, 30% require new cross-functional skills, 21% are deploying autonomous AI agents, 19% are shifting toward AI orchestration roles, and 16% are reducing headcount (see graph 6).

Graph 6: Top Impacts of AI on Cybersecurity Teams *(Respondents selected up to 3)*



This data signals a fundamental shift in how cybersecurity work gets done. For many organizations, the job is shifting toward directing AI systems rather than performing every task manually—requiring different skills, workflows, and organizational structures.

> "The real risk isn't the AI itself—it's using AI to automate these growth pathways instead of focusing on accelerating them."
>
> **Jay Bhalodia**
> **Rebuilding the Pipeline:** How Microsoft Balances AI Acceleration with Workforce Development

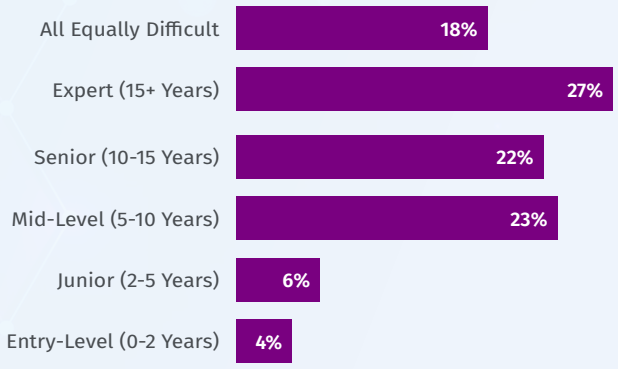
The Junior Pipeline Disruption: An Emerging Hypothesis

These patterns suggest a structural challenge for workforce development, one that several data points collectively indicate. Entry-level roles—SOC analysts, threat intelligence

analysts, junior incident responders—have traditionally served as training grounds where new professionals develop fundamental skills through repetitive, hands-on work. This apprenticeship model has been foundational to cybersecurity workforce development for many years. Analyzing alerts, investigating routine incidents, processing threat intelligence feeds: this is how junior practitioners build the pattern recognition and technical judgment on their path to more advanced positions.

The data reveals an emerging pattern that may threaten this traditional pathway. Organizations report that manual analysis and workflow execution tasks are increasingly automated—49% report reduced manual analysis time, 48% report automated workflows (see graph 6). Organizations report role reductions concentrated in these positions: SOC and security analysts (32%), threat intelligence analysts (26%), and incident responders (22%)—roles that have traditionally been junior-level steppingstones. This suggests a troubling paradox: while entry-level positions are among the easiest to fill (only 4% cite them as most difficult to recruit), organizations struggle significantly with experienced hires—27% identify expert roles as most challenging, 22% point to senior positions, and 23% cite mid-level roles. Collectively, these experienced roles represent 72% of recruitment difficulties while junior and entry-level positions account for just 10% (see graph 7).

Graph 7: Most Difficult Cybersecurity Level to Recruit



Key Takeaway:

Senior and Expert talent are hardest to find.

Organizations have traditionally relied on junior talent developing foundational skills through hands-on analytical work. As AI handles more of that routine analysis, the nature of entry-level work is evolving — requiring earlier exposure to AI-augmented workflows rather than manual-first approaches. Simultaneously, organizations are creating new specialized AI security roles that require cross-functional expertise, opening new career pathways that didn't exist three years ago. The combined effect on junior talent development is still emerging; the data suggests a structural shift in how skills are built, not a closure of the pipeline.

This transformation has only begun. With With three-quarters of organizations still developing AI governance approaches and training programs, AI's full impact on workforce structure remains to be seen. That said, early indicators point toward a clear direction: AI isn't solving the cybersecurity talent shortage directly — it's changing the nature of the problem. The efficiency gains are real and measurable. So is the structural shift in what skills matter at each career stage. The field is reorganizing around AI-augmented work, not replacing professionals with AI. What follows reveals how this plays out in practice: through regulatory pressure that demands new expertise, through organizational choices about where to invest in talent, and through the resulting skills gap that organizations are scrambling to address. Current impacts concentrate in productivity gains—automated workflows and reduced analysis time—rather than immediate headcount reduction, yet these operational shifts signal the beginning of deeper structural changes in how cybersecurity work gets done.

Regulatory Compliance: The Accelerator

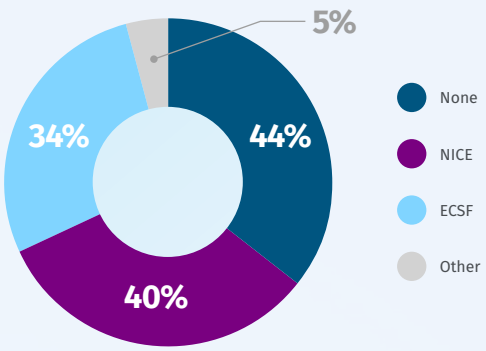
While AI disrupts traditional entry pathways into cybersecurity, a parallel force is fundamentally reshaping workforce requirements from the opposite direction. Regulatory compliance—once viewed as a bureaucratic necessity—has emerged as a powerful accelerator of workforce standardization, forcing organizations to adopt structured frameworks, hire specialized talent, and rebuild teams around clearly defined roles and competencies.

The Framework Revolution

Workforce framework adoption is on a steady upward trajectory. In one year, the percentage of organizations using NICE or ECSF to define cybersecurity role descriptions and job requisitions grew from 46% to 56% (Graph not included). NICE is now adopted by 40% of organizations and ECSF by 34%. While this 10% increase reflects gradual rather than explosive growth, the individual framework adoption rates tell a similar story: NICE adoption jumped 11 points and ECSF increased 8 points, signaling a meaningful shift toward structured, competency-based workforce planning.

Organizations are increasingly turning away from the ad hoc job descriptions that long characterized the industry, opting instead for standardized frameworks that provide clearer role definitions and career pathways (see graph 8).

Graph 8: Which Framework Does Your Organization Use to Define Cybersecurity Role Descriptions
(Respondents selected all that applied)



Key Takeaway:

NICE and ESF lead the way when it comes to framework adoption.

This isn't organic growth driven by best practices alone. The data suggests a clear correlation between framework adoption and regulatory pressure. The ECSF, now at 34% adoption—just 6 points behind NICE's 40%, despite NICE's longer market presence and prevalence in U.S. organizations—appears to be benefiting from its integration into European directives. When compliance mandates tie directly to specific frameworks, adoption follows, transforming frameworks from optional guidance into operational necessity.

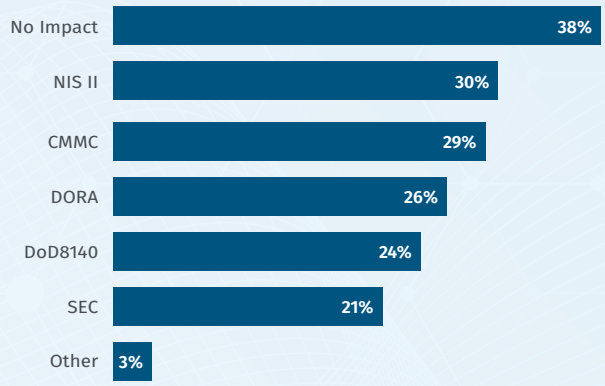
Directive-Driven Transformation

The catalyst behind framework adoption becomes clearer when examining which regulatory directives are reshaping hiring practices. NIS2 leads at 30%, followed closely by CMMC at 29% and DORA at 26%. DoD 8140 affects 24% of organizations, while SEC regulations impact 21% (see graph 9).

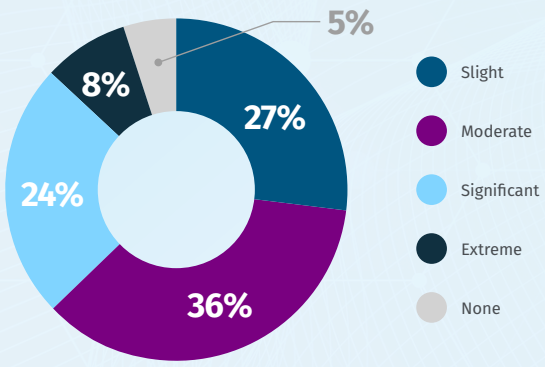
These findings are particularly striking given how sector-specific most directives are. NIS2 applies to critical sectors in the European Union (EU). DORA applies exclusively to financial services in the EU. CMMC applies to US Department of Defense contractors. DoD 8140 affects U.S. military personnel and DoD contractors. That these narrowly focused regulations show such strong representation in a global survey reveals the depth of their impact within affected sectors.

Organizations subject to these directives aren't experiencing mild compliance adjustments. Instead, they report substantial workforce impact, with many creating entirely new specialist positions to meet regulatory requirements.

Graph 9: Directive and Regulations That Have Impacted Hiring
(Respondents selected all that applied)



Graph 10: Impact on Hiring Due to Regulatory Compliance



Key Takeaway:
Multiple regulations are driving hiring decisions, not just one.

Key Takeaway:
Regulatory compliance is causing a widespread impact on hring.

The extent of impact reinforces this interpretation. When asked how significantly directives have affected hiring, 68% of organizations report moderate to extreme impact. Another 27% report slight impact. Only 5% say their hiring remains entirely unaffected by regulatory requirements (see graph 10).

This represents a substantial shift from 2025, when only 40% of organizations reported that directives were affecting their hiring practices. In 2026, that figure jumped to a whopping 95%. The transition from regulatory uncertainty to measurable workforce impact happened faster than many anticipated, leaving organizations scrambling to build compliance-ready teams under compressed timelines.

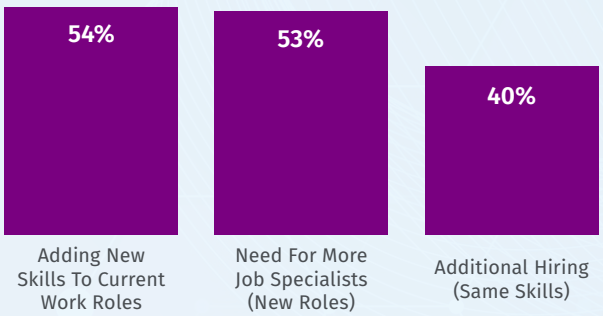
The Specialist Imperative

Regulatory pressure manifests most visibly in a dramatic surge in specialist hiring. **Organizations reporting a need for more job specialists to handle new roles jumped from 23% in 2025 to 53% in 2026—a 30% increase** that reflects how compliance requirements are creating entirely new workforce skillsets within organizations.

This growth outpaces even the rise in additional hiring for existing roles, which increased from 26% to 40%. While 54% of organizations are adding new skills to current work roles (up modestly from 51%), the dominant story is specialist role creation, not skill expansion (see graph 11).

While the survey doesn't specify which roles organizations are creating, the timing and scale of this surge—occurring alongside sector-specific regulatory mandates—suggests these are likely compliance-focused positions designed around directive requirements. Organizations subject to

Graph 11: Top Impacts of Directives and Regulations
(Respondents selected all that applied)



Key Takeaway:
Regulations are creating a need for new roles and skills.

DORA need operational resilience expertise, NIS2 creates demand for incident reporting coordination. CMMC requires DoD contractor validation capabilities. DoD 8140 formalizes specific work roles tied to military missions.

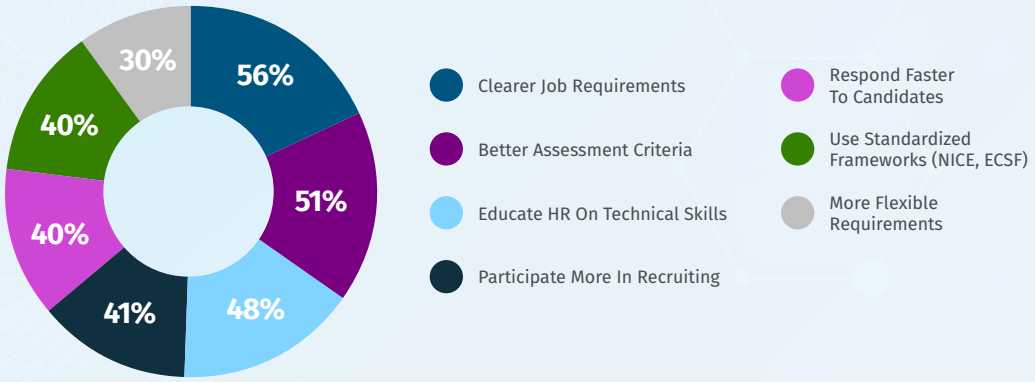
The data indicates organizations are building new skills sets and specialties rather than simply expanding existing teams, a pattern consistent with compliance-driven specialization.

> "Our cybersecurity officers are accountable for ensuring that local regulations are met. The standardized foundation handles the majority of requirements, and they deliver that final piece."
>
> **Dr. Kevin Jones**
> **Skills Over Hierarchy:** How Bayer Builds Cybersecurity Careers for an AI-Driven Future

Frameworks as Organizational Blueprint

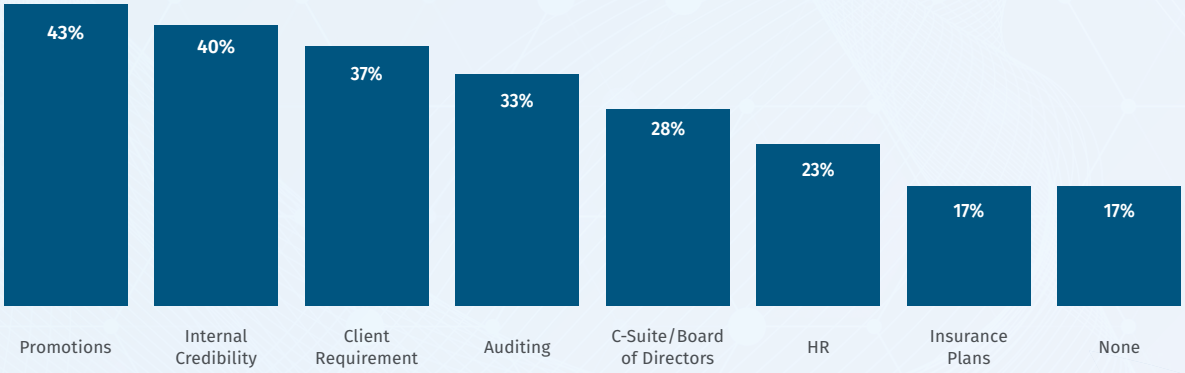
The practical value of frameworks extends beyond regulatory checkboxes. While 56% prioritize clearer job requirements and 51% advocate for better assessment criteria, 40% identify use of standardized frameworks as a critical support mechanism—a ranking that reflects the structural solution frameworks provide within broader hiring challenges (see graph 12).

Graph 12: How Can Cybersecurity Managers Better Support HR?
(Respondents selected all that applied)



External pressures are also reshaping skills validation requirements. Auditing requirements (33%), executive mandates (28%), and client demands (37%) are starting to getting close to promotions (43%) and credibility (40%). Certification is increasingly shifting from nice-to-have to business necessity (see graph 13).

Graph 13: Where Certification Matters Most



This regulatory transformation sets the stage for a critical challenge explored in the following section: as directives mandate specialized capabilities and frameworks provide the structure to build them, competition for senior talent who can fill these specialized roles intensifies dramatically. Organizations aren't just hiring more people—they're rebuilding teams from the top down.

Rebuilding From the Top: Senior Hiring Dominance

Faced with AI's transformation of how entry-level analytical work gets done — and regulatory frameworks demanding specialized expertise — organizations are restructuring how they build and develop cybersecurity teams. The patterns explored earlier — where AI is reshaping entry-level analytical work and compliance is creating specialized demands — converge in a distinct shift toward senior hiring. Rather than developing expertise internally through junior pipelines, organizations are increasingly attempting to acquire it directly through experienced hires.

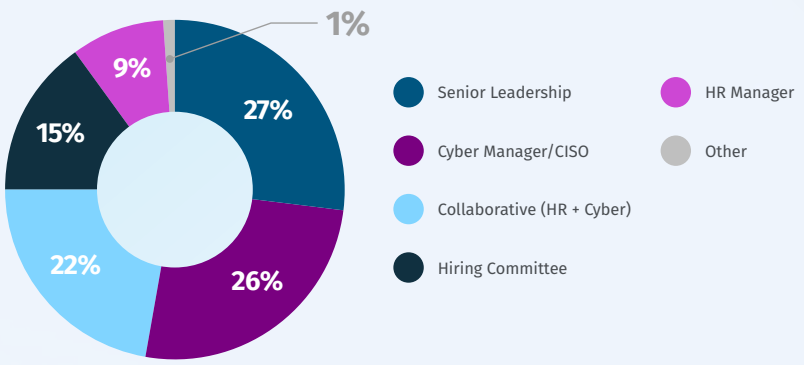
Decision Authority Migrates Upward

The power dynamics of cybersecurity hiring have shifted markedly toward senior leadership. **Senior executives and CISOs now control 53% of hiring decisions** (see graph 14), **consolidating authority that was previously distributed across collaborative teams, hiring committees, and HR managers.**

This concentration of authority coincides with substantial regulatory pressure on workforce planning. With 68% of organizations reporting moderate to extreme regulatory impact on hiring (see graph 10) and 54% creating new specialist roles to meet compliance requirements (see graph 11), the data suggests these trends may be connected—senior leadership involvement potentially reflecting the strategic nature of compliance-driven hiring.

As hiring decisions become more strategic and compliance-driven, they also become more concentrated at executive levels, creating distinct patterns in recruitment difficulty across experience levels.

Graph 14: Final Hiring Decision Authority



Key Takeaway:
Decision authority stays at the top.

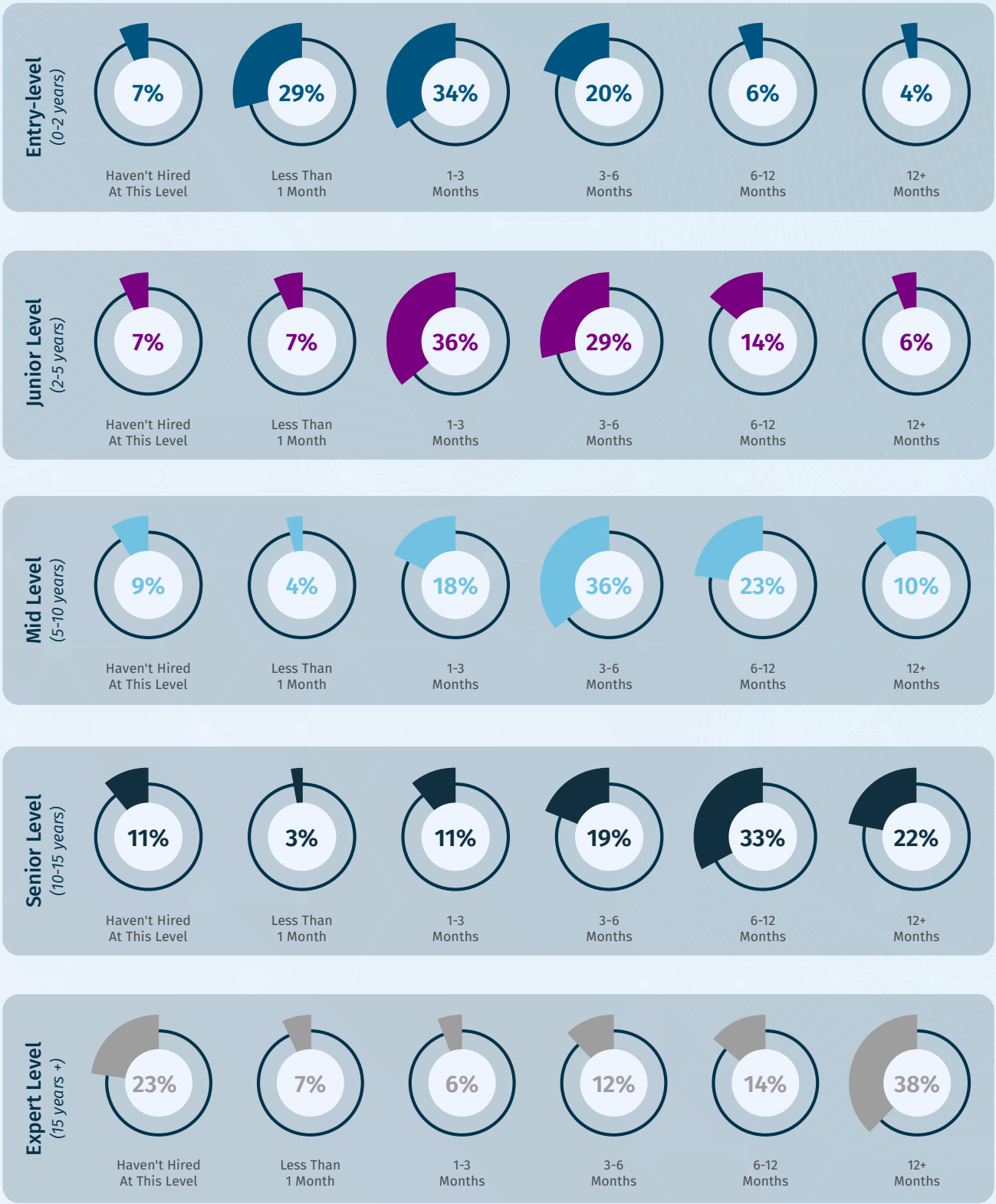
The Senior Talent Squeeze

Organizations report starkly different experiences recruiting across seniority levels. Nearly half identify expert and senior positions as being the most difficult to fill—27% cite expert roles (15+ years of experience) and 22% point to senior positions (10–15 years) as their greatest recruitmentchallenge. In contrast, only 4% report difficulty filling entry-level roles (see graph 7).

These recruitment challenges are compounded by extended time-to-fill metrics.55% of senior hires require six months or longer to fill, revealing sustained pressure at experienced levels, while junior positions fill relatively quickly (see graph 15).

Graph 15: Average Time to Fill Open Cybersecurity Roles

What is the average time (Posting to hired) to fill open cybersecurity roles?



Key Takeaway: The higher the role, the longer it takes to fill.

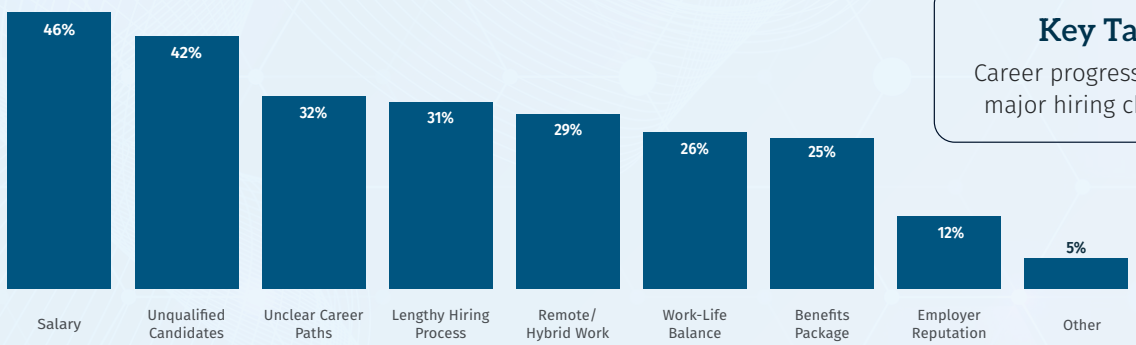
The Career Progression Crisis

The consequences of top-down rebuilding manifest most clearly in a striking shift among hiring challenges. Unclear career progression now ranks as the third-largest obstacle, cited by 32% of organizations (see graph 16)—more than triple the 9% reported last year. This 23% surge suggests career development is becoming increasingly difficult as organizations rebuild their teams.

The data points to a structural tension. As AI automates entry-level analysis and regulatory frameworks drive demand for specialized expertise, traditional progression pathways (e.g., SOC analysts advancing through detection, incident response, and threat hunting over several years) may be fragmenting. Organizations appear caught between immediate specialist needs and the long-term necessity of developing internal talent pipelines.

> "If we can't develop people to operate the business, then it's not a sustainable business. Long-term growth means I need to build the people to replace me."
>
> **Jay Bhalodia**
> **Rebuilding the Pipeline:** How Microsoft Balances AI Acceleration with Workforce Development

Graph 16: Top Hiring Challenges For Organizations
(Respondents selected up to 3)



Key Takeaway:
Career progression emerges as a major hiring challenge in 2026.

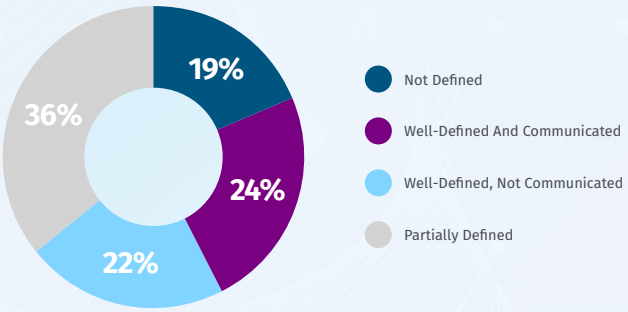
This challenge extends beyond hiring into retention. Unclear career pathing ranks as the third-largest retention obstacle at 31% (see graph 17), while lack of career growth emerges as a significant obstacle for 32% of teams (see graph 16). The data reveals a reinforcing cycle: organizations struggle to retain junior talent without visible advancement pathways, thus reinforcing the impulse to hire experienced professionals requiring less development investment.

Graph 17: Top Employee Retention Challenges
(Respondents selected up to 3)

At the same time, only 24% of organizations report providing well-defined and clearly communicated cybersecurity career paths (see graph 18). Most appear to recognize the problem exists but have not yet built systematic solutions.

Organizations now face competing imperatives: immediate specialist needs driven by regulatory demands and AI transformation versus long-term workforce sustainability. The combination of concentrated hiring authority, senior recruitment pressure, and career progression challenges across both hiring and retention suggests these short-term responses may be creating conditions for deeper skills distribution challenges—a pattern that becomes clearer when examining how skills gap manifests across teams.

Graph 18: How Defined Are Your Organization's Cybersecurity Career Paths



The Widening Skills Gap: A Perfect Storm

The cybersecurity workforce challenge has fundamentally shifted. **In 2025, for the first time, organizations identified skills gaps as a greater concern than headcount shortages—52% cited "not having the right staff," compared with 48% pointing to "not enough staff."** This year's data reveals that trend accelerating. When isolating the core question of skills versus headcount, the skills gap now dominates at 60%, compared with 40% for staffing shortages (see graph 19).

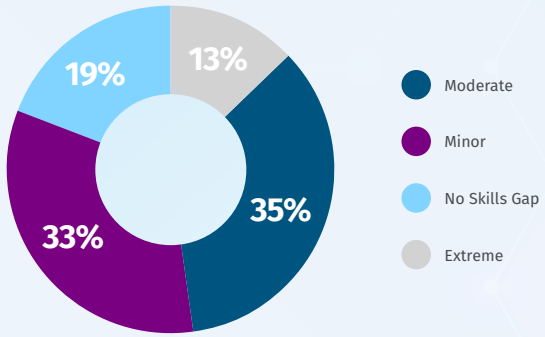
Graph 19: Which Is a Greater Challenge for Your Organization?

The industry's central problem is no longer simply filling seats. It's ensuring the people in those seats have the capabilities required to navigate an increasingly complex threat landscape.

This shift aligns with the compounding effects explored earlier in this report. Organizations report reductions in traditional junior-level roles as routine analysis becomes increasingly automated, potentially narrowing the learning environment where foundational skills were once developed. Regulatory frameworks demand specialized expertise that can't be acquired overnight. Organizations rebuild from the top through senior hiring, potentially creating skill concentrations at leadership levels while gaps persist across broader teams.

The result is a workforce where nearly half of organizations report moderate to major skills gaps—35% face moderate gaps spanning 10-29% of required skills, while 13% struggle with major gaps exceeding 30%. Only 19% of organizations report their teams are fully skilled (see graph 20).

Graph 20: How Significant Is Your Skills Gap?



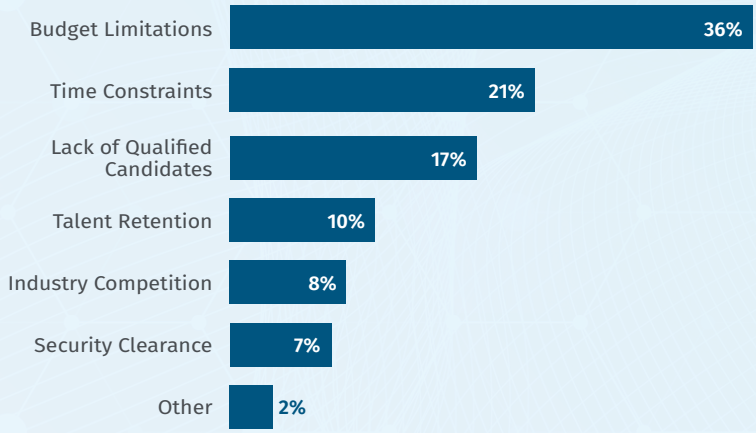
> "No longer is it about the number of people or the size of budget that you manage. We're really looking for people with the skills who can help drive outcomes."
>
> **Dr. Kevin Jones**
> **Skills Over Hierarchy:** How Bayer Builds Cybersecurity Careers for an AI-Driven Future

The Constraint Paradox

Organizations recognize the skills gap exists, yet the very constraints preventing them from closing it create a self-reinforcing cycle.

When asked to identify their primary obstacle to addressing workforce skills gaps, budget limitations top the list at 36%, followed closely by teams lacking time for skill development at 21%. Together, these account for 57% of primary constraints—a stark contrast to the 17% citing inability to find qualified candidates or the 10% struggling to retain talent (see graph 21).

Graph 21: Top Challenges in Addressing Skills Gaps

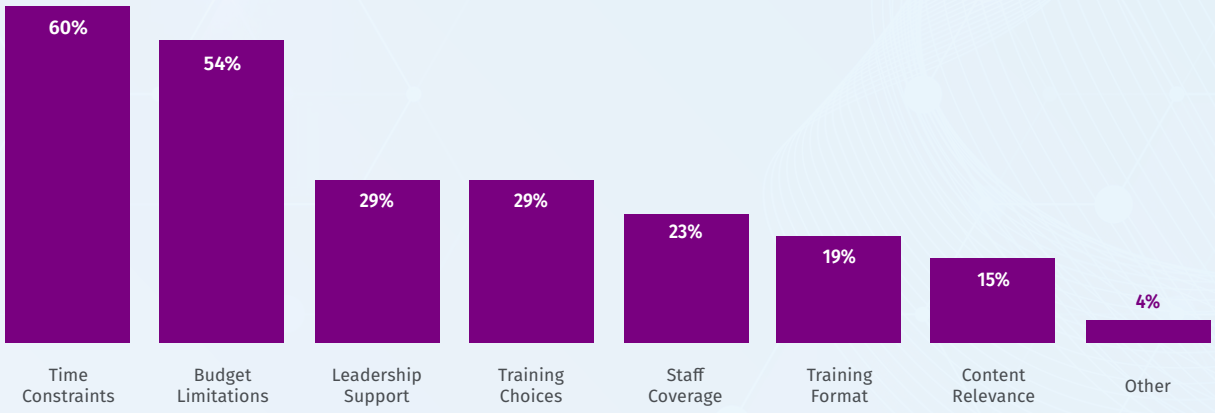


The narrative that dominates industry headlines—that cybersecurity can't find enough people—misses the more fundamental challenge. Organizations have people, But those people are overwhelmed, under-resourced, and unable to develop the skills they need because they're too busy executing today's security operations.

This paradox becomes clearer when examining training obstacles. Lack of time due to workload emerges as the single greatest barrier at 60%, with budget constraints following at 54%. The same constraints that prevent addressing skills gaps also block the training that could close them. Teams caught in operational firefighting mode lack the bandwidth to pursue skill development, while budget pressures force organizations to prioritize immediate security needs over long-term workforce capabilities. Leadership support, which could help resolve both time and budget challenges, ranks third at 29%, suggesting that in many organizations, workforce development remains secondary to other priorities (see graph 22).

Graph 22: Top Training Obstacles

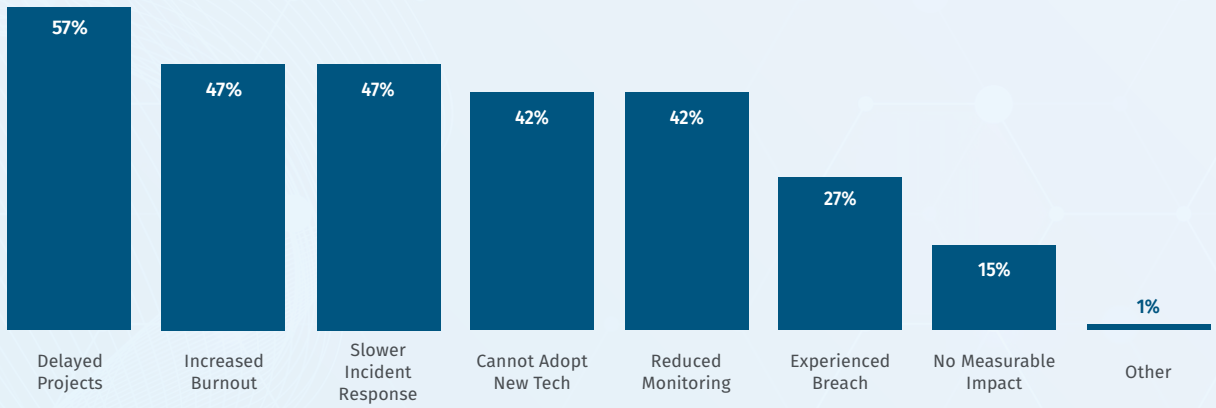
(Respondents selected up to 3)



The cascading effects of persistent skills gaps manifest across security operations. Organizations report that skills shortages lead to delayed projects in 57% of cases, increased team burnout in 47%, and slower incident response in another 47%. The inability to adopt new technologies affects 42% of organizations, while reduced monitoring capabilities impact another 42%. Perhaps most concerning, 27% of organizations report experiencing breaches as an impact of workforce skills gaps (see graph 23).

These aren't theoretical problems—they represent measurable operational impacts that accumulate over time, degrading both security posture and team sustainability.

Graph 23: Impacts of The Skills Gaps Within the Cybersecurity Industry
(Respondents selected all that applied)

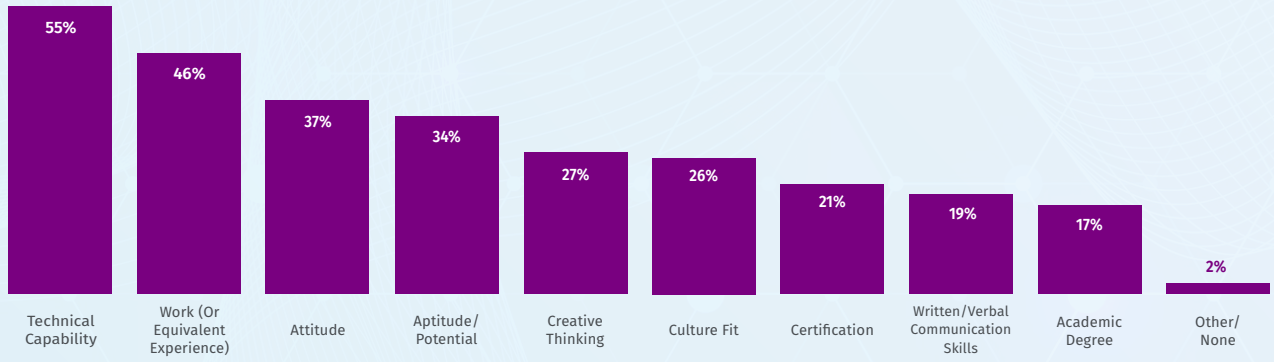


Shifting Hiring Priorities: Technical Capability Takes Center Stage

Organizations reveal clear priorities when evaluating cybersecurity candidates. Technical capability emerges as the dominant hiring criterion, cited by 55% of organizations as among their most important considerations when hiring—establishing a notable lead over work experience at 46%. Attitude (37%), aptitude (34%), creative thinking (27%), and culture fit (26%) round out the top priorities (see graph 24).

This emphasis on demonstrated capability reflects the compounding pressures explored throughout this report. As AI automates traditional learning pathways and regulatory frameworks demand specialized expertise, organizations increasingly prioritize candidates who can prove they possess required skills. The question shifts from "What credentials do you hold?" to "Can you demonstrate competency?" This is where the gap between what organizations seek and how they validate it becomes critical.

Graph 24: Technical Capability Dominates Hiring Priorities

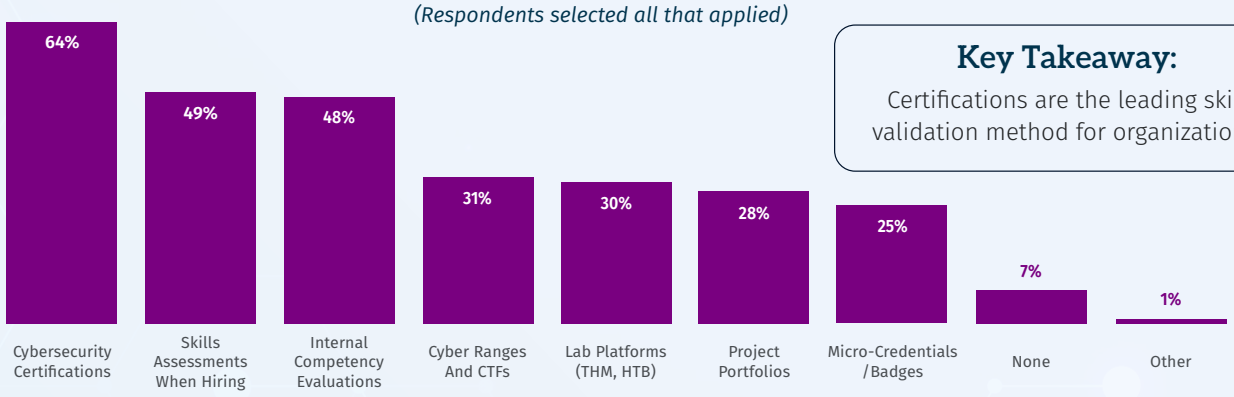


Certification as Critical Validation

In an environment where skills gaps widen and resources tighten, organizations increasingly turn to certifications as a practical mechanism for validating capabilities and making informed development investments. **Cybersecurity certifications rank as the most utilized validation method at 64%, significantly ahead of skills assessments during hiring at 49% and internal competency evaluations at 48%** (see graph 25). This preference suggests that certifications provide both standardized proof of knowledge and a structured framework for skill development. The importance organizations place on certifications becomes evident in hiring priorities. **When evaluating cybersecurity staff, 58% of organizations consider certifications either very important or extremely important.** Only 5% dismiss certifications as unimportant (see graph 26). This emphasis translates directly into organizational programs. Certification exam reimbursement leads all training offerings at 51%, followed closely by training course and platform subscription reimbursement at 48% (see graph 27).

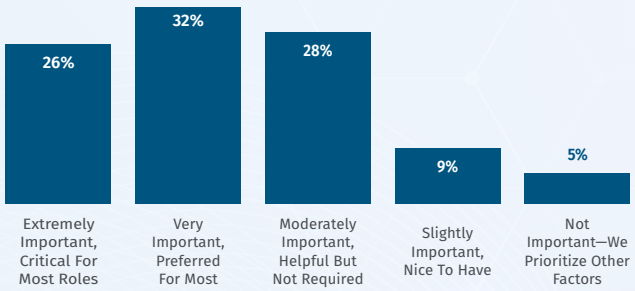
> "Certification validates that someone has achieved a certain skills and knowledge level."
>
> **Jay Bhalodia**
> **Rebuilding the Pipeline:** How Microsoft Balances AI Acceleration with Workforce Development

Graph 25: Top Skill Validation Methods
(Respondents selected all that applied)

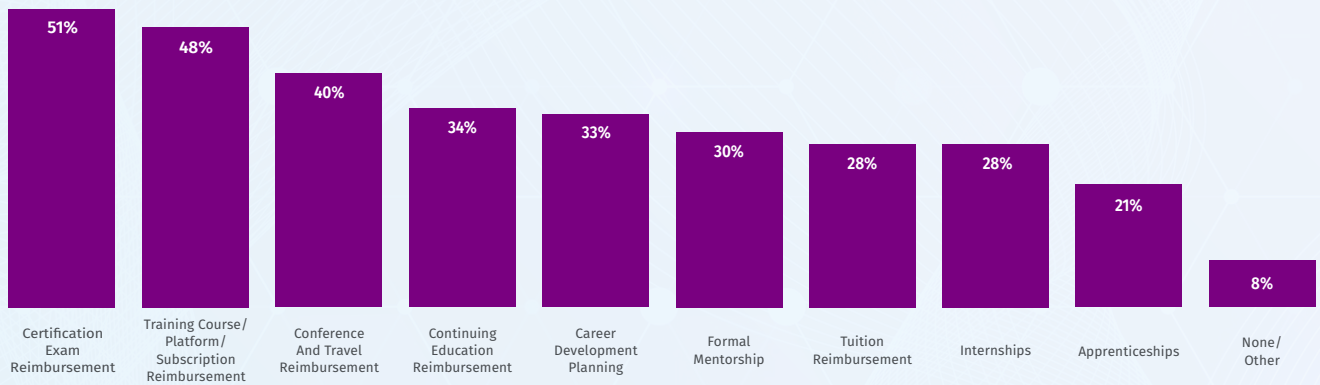


Key Takeaway:
Certifications are the leading skill validation method for organizations.

Graph 26: Certifications Critical for Most Organizations



Graph 27: Organizations Invest in Certification and Training



Organizations put their budgets where their validation needs are—investing in tangible credentials that verify team capabilities.

The strategic value of certification extends beyond individual development. Organizations require skills validation for multiple business-critical purposes, with 43% using it for promotion decisions and 40% for establishing internal credibility. Consulting and client requirements drive validation needs for 37% of organizations, while auditing purposes account for 33%. Even C-suite and board-level requests factor in at 28% (see graph 13).

The data indicates that certifications function as a mechanism for communicating technical capabilities to stakeholders who may lack deep technical expertise—transforming individual knowledge into demonstrable organizational competency.

The Path Forward

The cybersecurity workforce is experiencing simultaneous transformation from multiple directions.

AI disrupts traditional entry pathways while automating the junior roles that once served as learning grounds, thus eliminating the foundation of career progression. Regulatory compliance accelerates professionalization, driving framework adoption and creating entirely new specialist categories that didn't exist two years ago. Organizations respond by rebuilding from the top—hiring into senior roles to meet immediate expertise demands—yet this strategy fragments career pathways and concentrates decision authority at leadership levels.

The result compounds into a widening skills gap where teams lack the abilities required for evolving threats, constrained by the very time and budget pressures that training could address.

Yet the data also reveals pathways forward.

Framework adoption provides structural clarity for role definitions and requirements. Certification offers validated proof of capabilities that work within resource constraints. Organizations that strategically invest in structured skill development—leveraging certifications, hands-on training, and clearly defined career pathways—can build the adaptive, validated capabilities today's threat landscape demands while rebuilding the junior pipelines that ensure long-term sustainability.

> "Ultimately, it is whether an individual has the right skills, aptitude, and attitude, and is able to contribute, that matters."
>
> **Kok Wee Ong**
> **Building Cybersecurity from Two Directions:** Singapore's National Approach to Workforce Development

Key Recommendations

The 2026 Cybersecurity Workforce Research Report by SANS | GIAC reveals actionable strategies for organizations looking to strengthen their cybersecurity teams in today's challenging talent landscape. Based on the comprehensive global research undertaken for this study, we recommend the following approaches:

- ✔ Develop an AI governance program and provide baseline AI security training for all employees. Begin with essential policy frameworks and prioritize teams with highest AI exposure, scaling systematically as resources permit.
- ✔ Build a pipeline of entry-level talent that develops the skills needed to work effectively alongside AI tools. Structured mentorships and on-the-job training rotations remain the highest-ROI approaches — and the data suggests organizations that maintain junior development programs are better positioned as AI capabilities evolve. As capacity grows, expand into more formal programs like internships, academies, or cyber range initiatives as resources allow. Organizations can design residency-style programs that systematically develop junior talent, adapting the approach to their scale and budget.
- ✔ Leverage established frameworks and best practices—such as NIST CSF 2.0, CIS Critical Security Controls v8.1, MITRE ATT&CK, etc.—as guides to support compliance and regulatory alignment.
- ✔ Use workforce frameworks such as the NICE Framework, the European Cybersecurity Framework (ECSF), or the Saudi Cybersecurity Workforce Framework (SCyWF) as examples in building job qualifications and requisitions.
- ✔ Develop a cyber incident response plan beforehand and involve stakeholders beyond the security team, including communications, legal, HR, finance, and executive leadership in this process.
- ✔ Educate the Board, C-suite, and senior leaders on cybersecurity fundamentals and overall posture. Provide periodic updates—especially as regulations increasingly affect the entire enterprise. Regularly include cybersecurity leadership in Board and executive discussions.
- ✔ Create and strengthen career paths for security team members and individual contributors.
- ✔ Validate and document security team skills to meet regulatory and internal requirements. Establish a plan to close identified skills gaps across the team.

"Once you start thinking about skills, not about job titles, you can really bring good teams together to deliver a powerful outcome."

Dr. Kevin Jones
How Bayer Builds Cybersecurity Careers for an AI-Driven Future

Thank you for reading the **2026 Cybersecurity Workforce Research Report** by SANS | GIAC. This global workforce study delivers actionable insights to help cybersecurity leaders develop and sustain high-performing teams in an evolving threat landscape. Grounded in SANS research and real-world case studies, the report outlines practical strategies to strengthen resilience, close skills gaps, and prepare teams for tomorrow's demands.

Appendix A. Case Studies

Microsoft

Rebuilding the Pipeline: How Microsoft Balances AI Acceleration with Workforce Development

An Interview with:

Jay Bhalodia
Federal Managing Director
Customer Success, Microsoft

David Caswell
Federal Security AI Leader, Microsoft

> "If we can't develop people to operate the business, then it's not a sustainable business,"

says Jay Bhalodia, Federal Managing Director Customer Success at Microsoft. Yet AI is automating the exact work that traditionally develops those people—alert triage, initial investigation steps, the pattern recognition that builds foundational security skills. It's the dilemma facing every security leader in 2026, but Microsoft's position as both a major AI developer and a massive cybersecurity operation gives the organization an uncomfortably clear view of what's at stake.

Bhalodia leads Customer Success for Microsoft Federal's cybersecurity organization of over 100 professionals. His concern isn't theoretical. When organizations use AI to eliminate the routine work that junior analysts perform, they risk destroying the learning ground where the next generation of security leaders develops. "The real risk isn't the AI itself," he explains. "It's using AI to automate these growth pathways instead of focusing on accelerating them. If we take away the work that allows our junior folks to learn pattern recognition and investigation skills, we reduce our ability to build that pipeline moving forward."

Microsoft has made an intentional choice. Rather than viewing AI as a replacement for junior-level work, the organization frames it as an acceleration tool—a co-pilot that helps people learn faster, reason more effectively, and move through skill development at increased speed. The distinction shapes everything from hiring decisions to training investments to whether the organization will have the leadership bench it needs five years forward.

Short-Term Survival Versus Long-Term Strategy

David Caswell, who leads Microsoft Federal's work at the intersection of cybersecurity and AI, sees the tension playing out across the industry. "There are a lot of organizations doing short-term thinking right now—how do I survive the next two years—rather than asking how they're going to create long-term sustained business growth," he observes. "Long-term growth means I need to build the people to replace me, which means I need to start with people getting out of college right now who don't have extensive credentials yet."

That long-term commitment became formal policy when Microsoft launched its Secure Future Initiative in 2023, making security the organization's first priority above all other business objectives. The company's dedicated security workforce grew from roughly 8,000 professionals to over 30,000 as product engineers across the organization were deputized into security roles. More significantly, security became measurable criteria in annual performance reviews for every business leader. "We will delay features to ensure what we ship is secure," Bhalodia explains, echoing CEO Satya Nadella's mandate that security comes first. That executive-level commitment creates the foundation for investment in workforce development even when short-term automation might seem more efficient.

Hiring at Scale with Human Judgment

Building that pipeline starts with hiring—and the volume has become staggering. Where Bhalodia's team once received 20 applications per open position, they now regularly see 200 or more. AI becomes essential not for making hiring decisions, but for managing the scale of evaluation required. "We have to find ways to reason over this data effectively," Bhalodia explains. "I can't scale my productivity ten to twenty times, and if I wait, those candidates won't be available."

Microsoft uses AI extensively in hiring—but with clear boundaries. The technology helps reduce bias, improve job descriptions, and analyze resumes for relevant experience rather than simply matching keywords. When crafting requisitions, teams use AI to check whether language is accessible to candidates from diverse backgrounds, whether junior applicants would understand the requirements, and whether Microsoft-specific jargon might exclude qualified candidates. "We don't offload cognition and we don't offload assessment," Bhalodia emphasizes. "AI reduces friction and bias, but interviewing, judgment and accountability stays fully human."

Caswell points to a deeper challenge the industry hasn't solved. "We have bots writing resumes and bots reading resumes—this is a failed process that won't scale," he argues. Traditional mechanisms for verifying credentials and confirming identity break down when resume preparation becomes automated and application volume explodes. Background checks for academic credentials alone can cost $20 per person—prohibitive when multiplied by hundreds of applications. "We need robust ways to confirm that someone is who they claim to be and has the experience they claim to have," Caswell says. "That's not just a hiring problem—it's a security problem."

The Management Gap

Bhalodia's challenge isn't finding enough people—it's finding the right mix of skills at the appropriate career stage. An unexpected problem emerged: highly qualified candidates willing to accept roles below their experience level. "We've seen turnover because we hired people who were overqualified but willing to take the position," Bhalodia notes. "We now assess whether someone is at the right career stage for the role and whether the growth opportunities align with where they are professionally."

For specialized skills—operational technology expertise, threat emulation capabilities—the market remains constrained. But for the broader security workforce Microsoft needs, volume isn't the issue. Retention reflects the organization's development focus. Over the past year, Bhalodia's team lost six to eight people—but only one left Microsoft entirely. "We're not going to compete on cost," Bhalodia says. "If we're constantly buying each other's talent, that's not a sustainable model. We have to develop and cultivate our own."

That development starts with hiring for different attributes than traditional requisitions demand. Caswell sees a fundamental shift in what matters. "I prioritize creativity and tenacity over specific technical credentials now," he explains. Security professionals driven by curiosity naturally explore new AI tools in their own time, discover what works, and bring those efficiency gains back to their day jobs. That pattern—individual exploration leading to operational improvement—only functions when organizations hire for those traits rather than checking boxes for specific technical skills or years of experience. "The tools and the work itself are evolving rapidly, but management and hiring practices haven't kept pace," Caswell observes.

> **"The opportunity isn't in retraining the workforce—it's in equipping managers to think differently about what they're asking of people and how they develop them. The industry hasn't invested yet in giving management the tools to understand what developing people means in an AI-enabled world."**

Beyond hiring, that development happens through structured support. Microsoft established an AI Center of Excellence designed not to solve AI problems for teams, but to advise them in solving their own. "I've got this AI problem that I'm going to solve, and you'll advise me on what I need to do. But I have to physically build the thing," Bhalodia explains. "People across the organization are at different points—some learning basic prompting, others coding full agentic systems. The COE helps accelerate that journey without removing the learning experience itself."

When Certification Matters

Microsoft provides extensive internal training on AI application and security—a significant advantage for a services organization supporting external customers. Bhalodia takes a pragmatic approach to skill validation.

For using AI to increase personal productivity, he doesn't require certifications—he cares whether someone maximizes their impact. For customer-facing security expertise, the calculation changes. "SANS classes give you perspective—you're sitting with IT directors, analysts, people from different companies," he explains. "That cross-industry context is valuable for our team's ability to resonate with customers. Certification validates that they achieved a certain skills and knowledge level."

Microsoft's approach ultimately rests on an intentional choice: view AI as an accelerator for human capability rather than a replacement for it. The organization's scale and position as an AI developer create advantages most organizations don't have. But the underlying philosophy—that sustainable security operations require continuous investment in developing the next generation—applies regardless of size. As organizations navigate AI's transformation of security work, the critical question isn't whether to adopt AI tools. It's whether they're using those tools to eliminate the pathways that build tomorrow's workforce, or to accelerate the development of the professionals who will lead security operations for the next decade.

> **"The real risk isn't the AI itself—it's using AI to automate these growth pathways instead of focusing on accelerating them."**
>
> **-Jay Bhalodia**
> Federal Managing Director Customer Success, Microsoft

The views expressed in this report are the personal view of each respondent and not necessarily represent the views of their employers, past or present, or any other party.

Skills Over Hierarchy: How Bayer Builds Cybersecurity Careers for an AI-Driven Future

An Interview with:

Dr. Kevin Jones
Global CISO, Bayer

Meg Waloschek
Strategy Director Cyber Security, Bayer

In a global organization of 90,000 people operating across pharmaceuticals, consumer health, and crop science, Bayer has undertaken a radical transformation over the past two years. The change goes far beyond cybersecurity—moving from traditional hierarchy to a skills-based model that redefines career progression, team structures, and how work gets done. "We're really looking for people with fungibility, the flexibility to adapt and drive outcomes across different domains," says Dr. Kevin Jones, Global CISO at Bayer. That focus on adaptability marks a profound shift in how the organization approaches talent.

The change began with a company-wide operating model called Dynamic Shared Ownership (DSO), which collapsed management layers down to five or six across the organization. "It's a philosophy around the way Bayer operates as a company, ensuring that the right decisions are taken at the right level of the organization," Jones explains. For IT, this meant moving to 34 platforms across the company, with five dedicated to cybersecurity.

These five platforms span the full security lifecycle: Cybersecurity Assurance handles governance, risk, and compliance; Cyber Defense Center manages threat intelligence, hunting, and incident response; Cybersecurity Technologies deploys preemptive controls; Cybersecurity Architecture & Innovation sets global standards and drives DevSecOps and offensive security; and Cybersecurity Culture & Enablement is cyber security's footprint in local markets and leads security culture adoption. Each platform operates as a full-stack capability team, combining engineering, operations, and delivery rather than splitting these functions across departments. But removing hierarchical layers created an immediate challenge: How do you measure value and enable career progression when traditional management structures disappear?

Measuring Impact, Not Management Scope

Bayer's answer is a customized skills-based framework, that draws on established models, including SANS, CIISEC and Gartner, and fundamentally redefined what career advancement means.

> "No longer is it about the number of people or the size of budget that you manage,"

Jones says. "We're really looking for people with the skills who can help drive the outcomes." Under this model, progression is measured by four types of impact: skills impact (increased skill level), impact on outcomes or business results, impact on (developing) others, and impact on bringing innovation into the program.

The framework is one solution to a persistent retention challenge across the cybersecurity industry. "This model is very powerful for retention, because it means you don't need to go down a management path to prove your value and impact," Jones notes. Technical experts can advance their careers based on the depth of their expertise and the business outcomes they drive, without being forced into management roles. The organization is implementing this framework across its entire 90,000-person global workforce, not just IT or cybersecurity, creating consistent career pathways throughout Bayer.

The skills-based approach enables the organization to build teams with unprecedented speed by pulling talent based on required capabilities rather than job titles or departmental boundaries. Meg Waloschek, Strategy Director for Bayer's cybersecurity organization: "I think the best example of this is when an information protection squad was spun up literally over a weekend because our assurance platform leader had wider access to people."," she says. The team went live in days and delivered key outcomes by the end of the year. Jones estimates the alternative approach would have taken substantially longer: "At least a year and a half, if not two years for those outcomes."

That speed comes from thinking differently about where expertise lives. "Bringing the right skills in doesn't always mean they have to come from cybersecurity," Jones adds. "Cybersecurity is a team sport, we pull in experts from various other departments." The result is multidisciplinary teams that combine cybersecurity specialists with psychologists hired to support culture change programs, professionals with business backgrounds, and risk specialists from other domains. Waloschek herself moved from marketing and sales through digital transformation and IT strategy before landing in cybersecurity—what Bayer calls a "squiggly career." This concept is actively encouraged through an internal talent marketplace where employees list their skills and find opportunities across the company. "Once you start thinking about skills, not about job titles," Jones observes, "you can really bring good teams together to deliver a powerful outcome."

Embedding Compliance in Platform Design

Operating across the highly regulated sectors of pharmaceuticals and crop science, Bayer faces overlapping global, regional, national, and domain-specific regulations. Pharmaceuticals and agriculture are both considered critical national infrastructure, adding additional compliance layers. Without coordination, each division or even country could run separate regulatory projects.

That is why Bayer standardizes 90% of its cybersecurity program globally, then handles country-specific or sector-specific requirements through what Jones calls "last-mile delivery"—the final customization needed to meet local regulations. This approach operates through a network of over 25 regional security offices. "Our cybersecurity officers are accountable for ensuring that local regulations are met," Jones explains. "The standardized foundation handles the majority of requirements, and they deliver that final piece."

Each of the five cybersecurity platforms is built to be auditable by design, embedding regulatory requirements directly into operations rather than treating compliance as a separate, reactive activity. This approach allows the skills-based workforce model to function across regulatory environments—knowledge can move between platforms and geographies because the compliance foundation is already built in.

Elevating Roles in an AI-Driven Future

Like many organizations, Bayer is actively automating Level 1 security operations tasks. But the organization frames this as role transformation rather than replacement. "We will elevate the role of analysts to manage agents that are doing a lot of the repetitive work," Jones explains.

> "It's not necessarily a replacement, it's a pure shift in terms of what we could do. And that enables us to do more."

The shift is driven by necessity. "That's a necessity for the future of the security world where the attackers have AI," Jones says. "It's the only way we can be fast enough to respond on the defense side." The role of the human operator shifts from being "in the loop"—executing every task manually—to being "on the loop," providing oversight and context while automated systems handle repetitive work. The distinction is significant. It demands different skills—not just technical ability, but a higher order of cognitive decision-making.

Training reflects this reality. The approach is blended: formal AI courses available through internal platforms, on-the-job cross-training, and an expectation embedded in the skills model that senior professionals actively develop others. A monthly virtual huddle brings the cybersecurity organization together to share program outcomes, external knowledge, and technical updates. Bayer's cybersecurity academy extends further, planning hackathons for skills like vibe coding, bringing in external experts, and offering development opportunities well beyond technical security—from inclusive language training to deep knowledge of Bayer's product lines. "People are responsible for their own training and development," Jones says. "But the expectation is that you also help develop others. That's part of the impact we measure."

Looking ahead, Jones envisions a future defined not by individual security tools but by an integrated "security fabric" where platforms communicate and act autonomously through AI. This leads to the concept of a Cyber Resilience Center, an evolution of the traditional SOC where AI takes autonomous action, and humans provide strategic direction and oversight. Jones sees a future where the battle shifts fundamentally. "In a few years' time, it's highly probable that a lot of the attacker-defender landscape will be AI versus AI," Jones predicts. The skills organizations need will shift accordingly—less about operating tools manually, more about leveraging AI and managing autonomous agents effectively. “This requires a workforce with deep domain knowledge, whether in risk assessment, IT security, or psychology, combined with the ability to direct AI systems.” The skills-based framework Bayer implemented positions the company to deploy that expertise where needed, regardless of traditional departmental boundaries or hierarchical structures.

The views expressed in this report are the personal view of each respondent and not necessarily represent the views of their employers, past or present, or any other party.

Building Cybersecurity from Two Directions: Singapore's National Approach to Workforce Development

An Interview with:

Kok Wee Ong
Assistant Chief Executive (Policy & Corporate Development), Cyber Security Agency of Singapore

The Cyber Security Agency (CSA) of Singapore faces a challenge most organizations don't: building its own cybersecurity workforce while also strengthening talent capacity across the nation. As Singapore's national authority, CSA competes with private technology companies for cybersecurity professionals to meet its own operational needs. At the same time, it works closely with industry partners to develop the broader cybersecurity ecosystem, running programs that have trained over 22,000 individuals across government and industry since 2020. This dual role shapes everything from hiring philosophy to workforce development strategy.

"It is critical for Singapore to cultivate a robust cybersecurity talent pipeline for both government and private sectors," explains Kok Wee Ong, Assistant Chief Executive for Policy & Corporate Development at CSA. That national responsibility translates into practical constraints. CSA faces inherent challenges in compensation competitiveness, hiring speed, and market perception compared to private industry. Its rigorous selection process takes three to four months—comparable to global averages but longer than many private companies. Yet CSA maintains competitive hiring outcomes not through salary alone, but through something private employers cannot easily replicate: the opportunity to protect national digital infrastructure while building the workforce that will secure it for decades to come.

Skills Over Credentials in Public Service

CSA's hiring philosophy reflects a fundamental shift happening across the cybersecurity industry, but with a distinctly public service orientation.

> **"Ultimately, it is whether an individual has the right skills, aptitude, and attitude, and is able to contribute, that matters"**

While academic qualifications, professional certifications, and work experience provide baseline assessment criteria, CSA prioritizes candidates who demonstrate the technical capability to address sophisticated cyber challenges alongside commitment to serving Singapore's national cybersecurity interests.

That assessment happens through technical evaluations and structured interviews designed to test real-world application of knowledge, especially for technical roles. The agency weights these criteria strategically: entry-level positions place slightly higher emphasis on academic qualifications and demonstrated interests, given limited work history, while midlevel and senior roles prioritize hands-on skills and demonstrated experience. But across all levels, CSA looks for what Ong describes as essential differentiators—a strong sense of public purpose coupled with the attitude and aptitude for thriving in cybersecurity's constantly evolving threat landscape.

This approach enables CSA to build teams through multiple pathways simultaneously. Experienced professionals bring established expertise and immediate operational capability. Career changers offer fresh perspectives from adjacent industries and diverse problem-solving approaches that challenge conventional thinking. Fresh talent—developed intentionally through CSA's programs—represents the agency's investment in the future.

> "As Singapore's national cybersecurity agency, we have a responsibility to develop cybersecurity talent not just for CSA but also for our national ecosystem"

This balanced strategy finds practical expression in CSA's workforce development programs. The Cybersecurity Development Programme exemplifies the approach: a 12-month initiative targeting fresh graduates and mid-career professionals transitioning into public sector cybersecurity. The program provides fully sponsored technical training with industry-recognised certifications and hands-on experience within CSA. Upon completion, participants either continue developing their cybersecurity expertise in CSA or are deployed to other government agencies to support broader cybersecurity outcomes.

CSA extends its skills-based approach to how it defines roles. The agency references Singapore's Skills Framework for Infocomm Technology, developed jointly with SkillsFuture Singapore and the Infocomm Media Development Authority. This framework clearly defines cybersecurity roles, required skills and competencies at different levels, and progression pathways.

When operational technology (OT) cybersecurity emerged as a critical focus area, CSA developed the OT Cybersecurity Competency Framework, mirroring the existing Skills Framework architecture to ensure employers, training providers, and professionals could easily understand career opportunities and progression in this specialized domain.

The Dual Mission: National Ecosystem and Internal Capacity

CSA's workforce responsibility extends far beyond its own hiring needs. The agency conducts regular cybersecurity landscape studies and consultations with industry stakeholders to identify manpower gaps, then develops initiatives to address those gaps across Singapore's entire cybersecurity ecosystem.

Since 2020, the SG Cyber Talent initiative has impacted over 22,000 individuals through programs including cybersecurity bootcamps, career mentoring, career conversion programs, and leadership education.

The national scope creates intentional talent flows between CSA and the broader ecosystem. CSA Academy provides cybersecurity professionals in government and Critical Information Infrastructure sectors with intermediate and advanced courses not readily available commercially. This tripartite collaboration approach—involving government, industry, and academia—ensures initiatives address actual market needs rather than theoretical gaps.

Building a robust cybersecurity talent ecosystem generates compounding benefits that extend beyond addressing immediate workforce shortages. It creates value for the broader ecosystem while strengthening Singapore's overall cybersecurity posture. CSA maintains a collaborative consultation process when designing initiatives, inviting stakeholders from government, industry and academia to provide feedback. The agency also supports ground-up initiatives from academic institutions and the cybersecurity community through sponsorships, recognizing that effective workforce development requires multiple approaches from multiple sources.

Retention Through Purpose and Development

In Singapore's competitive market, retention demands more than competitive compensation. CSA anchors retention on three foundations: meaningful national impact, structured career pathways, and continuous upskilling investment.

Officers receive exposure to complex cyber operations and opportunities to rotate across domains, building both depth and breadth while sustaining long-term career growth.

CSA's annual posting exercise provides rotation within CSA, secondments to other government agencies, or attachments to private organizations. These experiences broaden perspectives, build cross-functional expertise, and ensure officers remain adaptable in an evolving cybersecurity landscape.

CSA adopts a comprehensive talent development approach through bonded scholarships and sponsorships supporting formal education, advanced training, and professional certifications in critical and emerging domains. By enabling officers to customize their learning journeys at different career stages and rapidly acquire new capabilities aligned with technological shifts, CSA sustains engagement, strengthens retention, and ensures its workforce remains future-ready.

Clear performance and competency indicators provide transparency in career progression. CSA has established different career pathways for talent development, while supervisors and HR engage in regular career conversations to understand aspirations, assess capabilities, and identify development opportunities aligning with both personal

goals and organizational needs. Development opportunities include job postings within CSA and across government agencies, formal training, certifications, and stretch assignments preparing officers to become leaders who are technically competent, operationally experienced, and ready for greater responsibilities.

Beyond career development, CSA fosters workplace culture through comprehensive engagement initiatives. Regular recognition of achievements—including celebrating officers who win external awards—reinforces a culture of excellence. HR curates opportunities for officers to lead interest groups, creating networks that extend beyond daily work and foster collaboration across teams. The agency also prioritizes officer well-being through thoughtful welfare initiatives.

Cultural Values as the Foundation

CSA's team culture centers on values that reflect both organizational principles and cybersecurity work's collaborative nature.

Inclusiveness is fundamental—the agency values diverse views and builds environments where varied perspectives drive positive outcomes. In cybersecurity, this diversity of thought proves crucial for understanding complex threat landscapes and developing comprehensive defense strategies protecting all segments of society.

Professionalism ensures CSA delivers its mission with integrity, operating in a culture of trust with both internal teams and external constituents. This encompasses technical excellence, ethical conduct, and maintaining high standards in all interactions with government agencies, private sector partners, and international counterparts.

Boldness empowers team members to seek innovative approaches and communicate ideas while striving to do the right thing. In an ever-evolving threat environment, this value encourages proactive thinking, challenges conventional approaches, and enables calculated risk-taking necessary to stay ahead of sophisticated adversaries.

Commitment reflects dedication to protecting Singapore's cyberspace, with team members taking pride in serving as Singapore's cyber defenders. This value ensures individuals invest in the mission and maintain continuous vigilance that cybersecurity demands.

The principle that "cybersecurity is a team sport" reinforces that effective cyber defense cannot be achieved in isolation. Within CSA, this means fostering seamless cooperation across technical, policy, and operational teams. Externally, it extends to partnerships with local and global organizations across government and private sectors, recognizing that Singapore's cybersecurity posture depends on collective effort.

These values create a culture where individual expertise contributes to collective strength, and where diverse and professional teams boldly tackle complex challenges together. In this environment, CSA effectively fulfills its mission of securing Singapore's cyberspace through both internal excellence and external collaboration.

As CSA continues building both its own workforce and Singapore's broader cybersecurity capacity, these foundational values ensure the agency remains effective in recruiting, developing, and retaining the talent needed to address evolving challenges in an increasingly digital world.

The views expressed in this report are the personal view of each respondent and not necessarily represent the views of their employers, past or present, or any other party.

Appendix B: Additional Insights

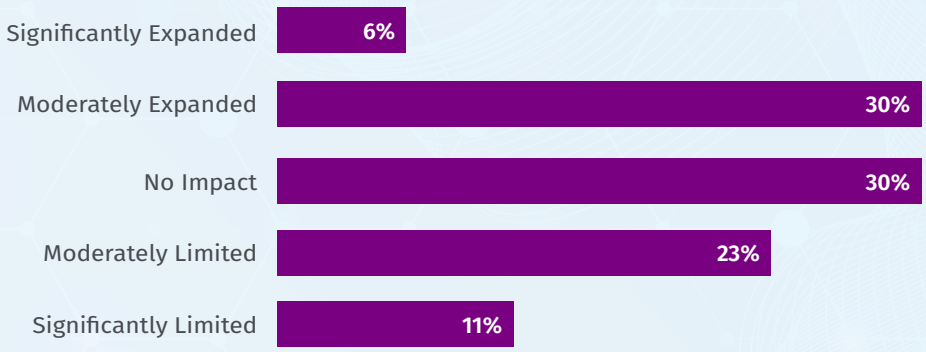
The following section presents supplemental findings from the 2026 survey that provide additional context on workforce trends not central to the primary narrative but offer valuable perspective.

Remote Work Policies

Organizations continue experimenting with work arrangements. Hybrid schedules (2-3 days in office) are most common at 28%, while 23% require 4 or more days on-site. Fully remote options remain limited: 9% allow work from anywhere, 9% permit remote work within specific regions, and 13% require full on-site presence (graph not included).

Among organizations excluding those unsure of impact, 36% report that remote policies expanded their candidate pool, 34% experienced limitations, and 30% saw no noticeable impact (see graph 28).

Graph 28: Impact of Remote Work Policy on Candidate Pool

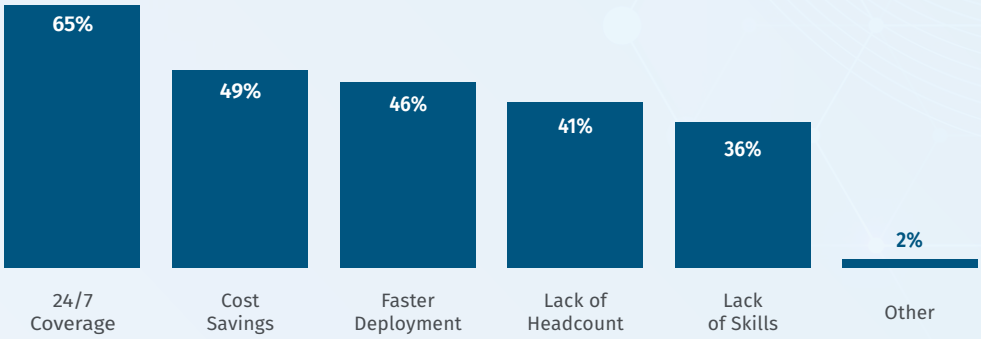


MSSP/MSP Usage Drivers

Among organizations using managed security service providers (MSSP) or managed service providers (MSP), 24/7 coverage drives adoption (65%), followed by cost savings (49%) and faster deployment (46%).

Skills gaps (41%) and headcount shortages (36%) rank lower, suggesting MSSPs/MSPs address operational needs beyond staffing challenges (see graph 29).

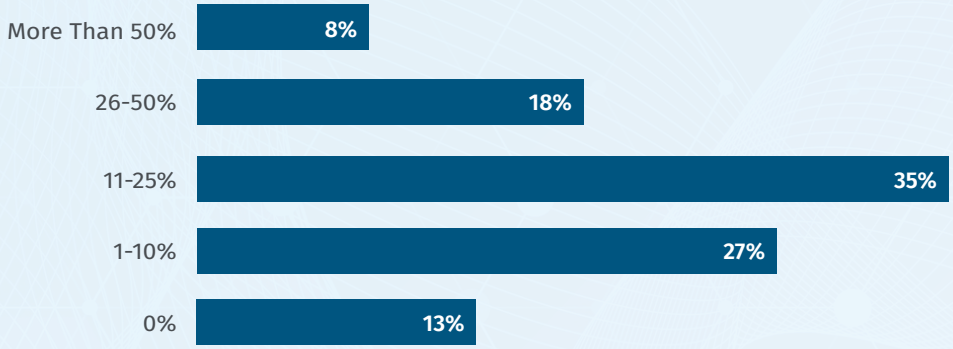
Graph 29: Primary Drivers for MSSP/MSP Adoption



Non-Traditional Hiring

Most organizations report modest adoption of non-traditional candidates: 62% indicate that 1-25% of recent hires came from non-traditional backgrounds (27% in the 1-10% range and 35% in 11-25% range). Only 8% report that more than half of hires originated from non-traditional paths, while 18% made no such hires (see graph 30).

Graph 30: Non-Traditional Background Hires



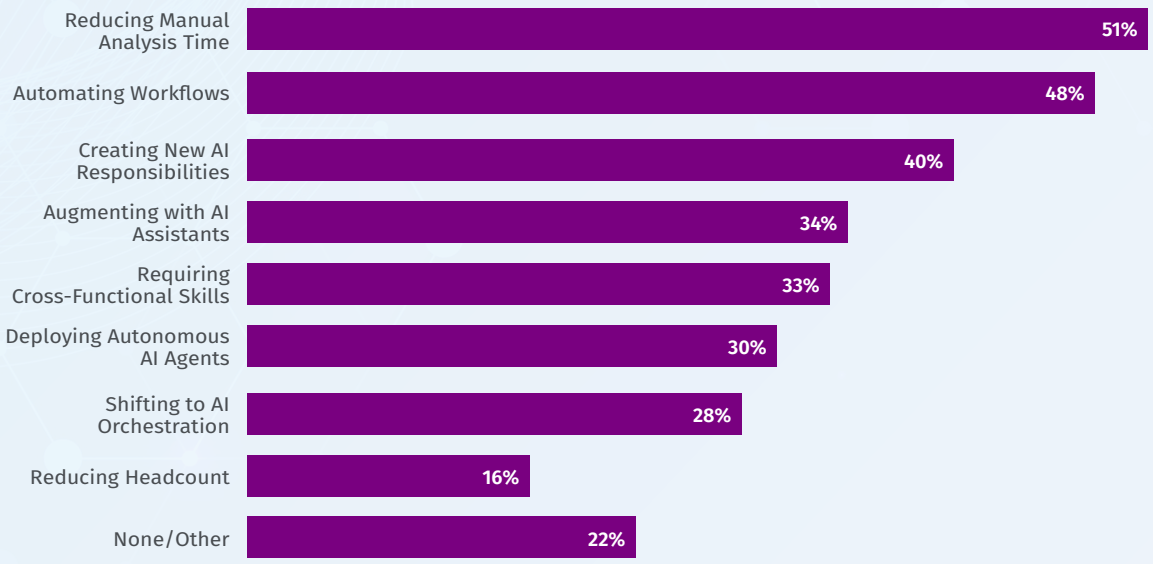
AI Implementation in Cybersecurity Teams

Current AI usage focuses primarily on productivity tools—conversational AI, data analysis, and workflow automation—with more transformational applications like autonomous agents and model training still emerging. Among teams using AI, conversational AI/chat leads (49%), followed by data analysis (47%) and workflow automation (44%).

Advanced applications like autonomous agents (24%) and AI model training (28%) remain less common (graph not included).

The biggest impacts center on reducing manual analysis time (51%) and automating workflows (48%), while reducing headcount ranks lowest at 16% (see graph 31). New AI-focused security roles — AI/ML security specialists, AI security engineers, AI governance analysts — are being created at a rate that may offset role changes in traditional analytical positions. Among organizations actively building out AI security functions, the majority have filled at least one new AI-focused role.

Graph 31: Biggest AI Impacts on Cybersecurity Teams *(Respondents selected up to 3)*

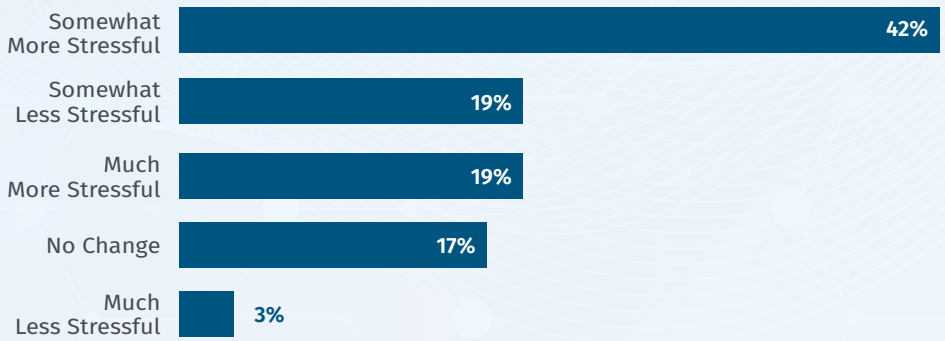


Team Stress Levels

Stress within cybersecurity teams continues to rise. 61% of organizations report increased stress levels over the past two years (42% somewhat more stressful, 19% much more stressful). Only 20% report decreased stress levels (see graph 32).

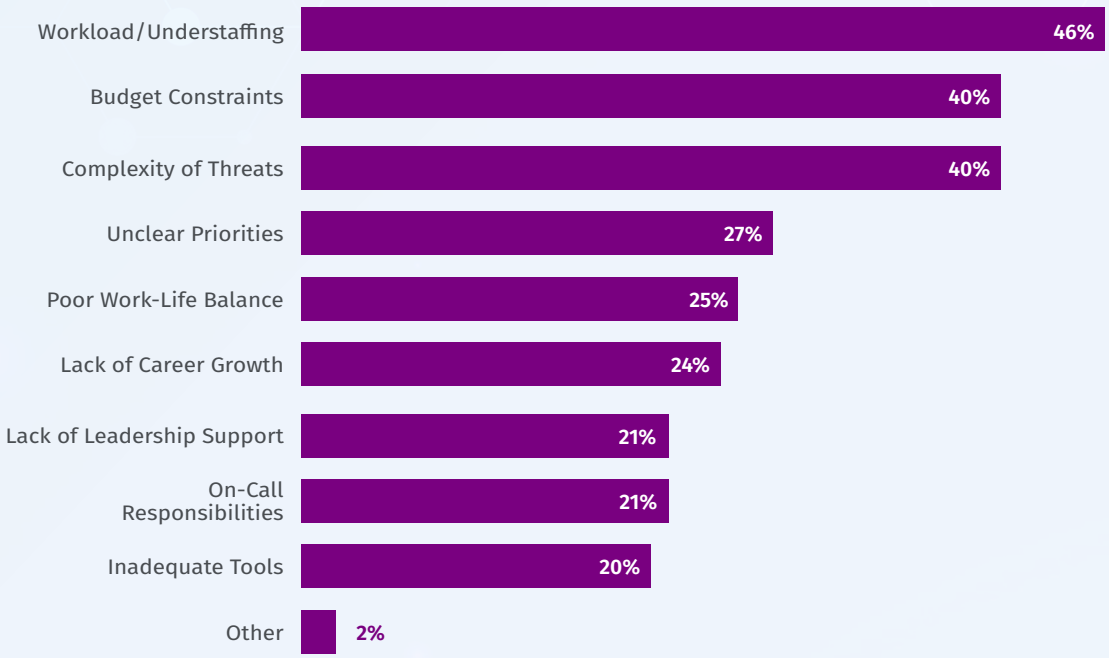
The top sources of stress mirror core workforce challenges: workload and understaffing lead at 46%, followed by budget constraints (40%) and threat complexity (40%). Other significant stressors include unclear priorities (27%), poor work-life balance (25%), and lack of career growth opportunities (24%) (see graph 33).

Graph 32: Team Stress Level Changes



Graph 33: Primary Sources of Team Stress

(Respondents selected up to 3)



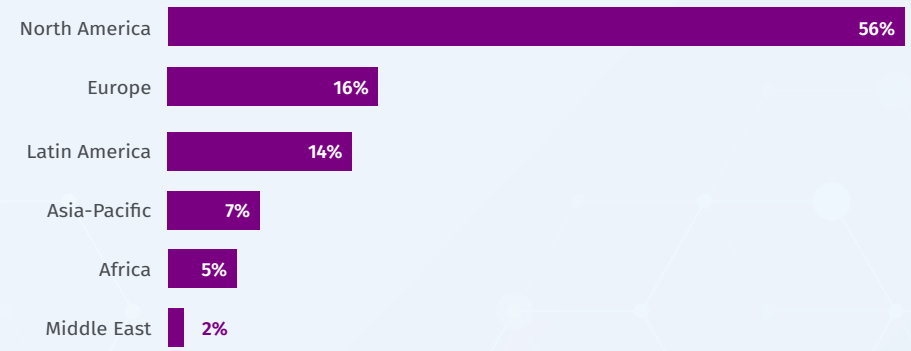
Appendix C: Demographics

A Global Perspective

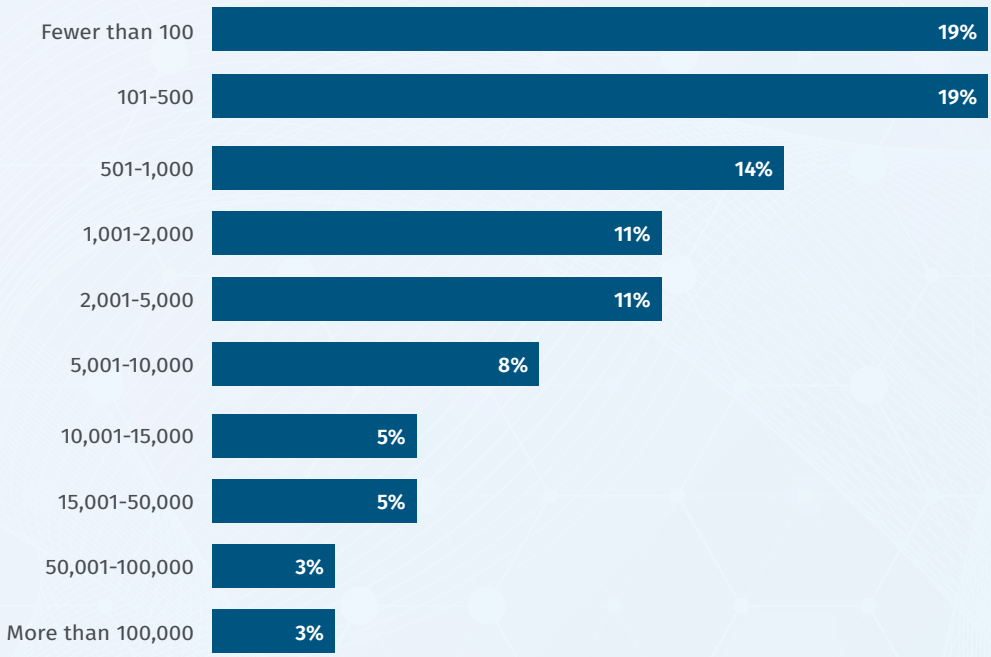
The 2026 Cybersecurity Workforce Research Report gathered insights from over 900 respondents across six global regions. The largest representation comes from North America with 56%, followed by Europe (16%), Latin America (14%), Asia-Pacific (7%), Africa (6%), and the Middle East (2%) (see graph 34).

These organizations span the full spectrum of company sizes, from small businesses with fewer than 100 employees to enterprises with over 100,000 staff members. The distribution across size categories shows 19% representing small businesses (fewer than 100 employees), 33% represent mid-sized organizations (101-1,000 employees), and 47% represent large enterprises (over 1,000 employees) (See graph 35).

Graph 34: Regional Distribution of Respondents



Graph 35: Company Size of Respondents (Headcount)



Cross-Industry Insights

This broad representation extends across industries as well. Technology (12%), consulting/professional services (11%), and banking/financial services (11%) lead the distribution. Additional representation includes healthcare (10%), government (8%), education (6%), manufacturing (5%), and energy/utilities (4%) (See graph 36).

This geographic, organizational, and industry mixture provides a comprehensive view of cybersecurity workforce development across different business contexts.

Graph 36: Industry Type

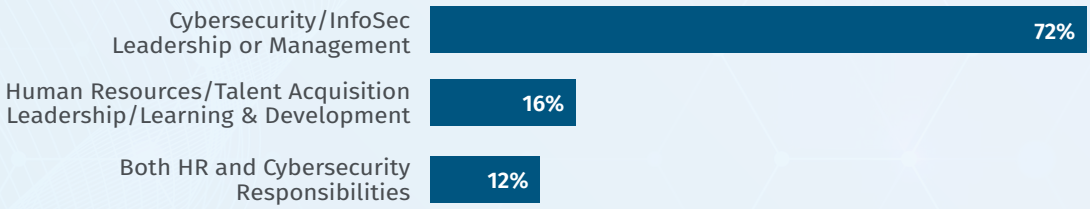
Team Composition and Experience

Within these organizations, the study captures perspectives from cybersecurity/InfoSec leadership (72%), HR/talent acquisition professionals (16%), and respondents with both HR and cybersecurity responsibilities (12%). This representation provides insights into how different stakeholders approach talent management challenges.

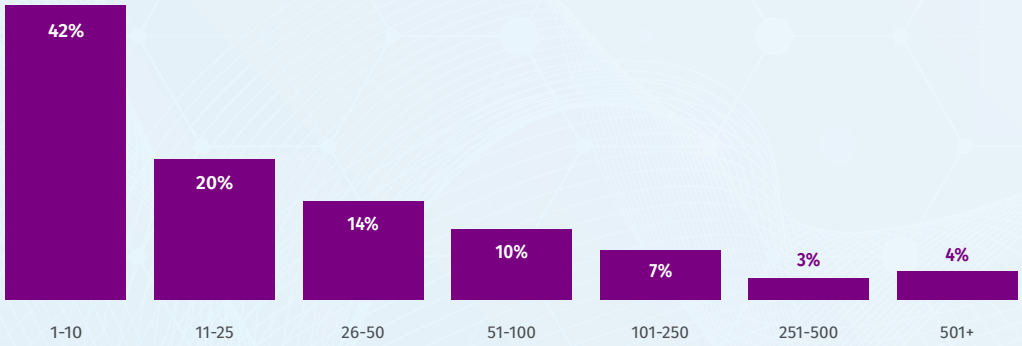
Most participating organizations (62%) maintain cybersecurity teams of 25 or fewer professionals, with 42% operating with teams of 1-10 staff members and 20% with teams of 11-25. Larger security operations include 14% with teams of 26-50, 10% with 51-100, and 11% with teams exceeding 100 professionals (See graph 38).

The respondents themselves demonstrate substantial industry experience, with 29% having worked in cybersecurity for 6-10 years and 24% for 2-5 years. Seasoned professionals with 11-15 years of experience comprise 16%, while those with 16-20 years and over 20 years represent 9% and 10% respectively. Entry-level professionals with less than 2 years of experience account for 13% of respondents (see graph 39).

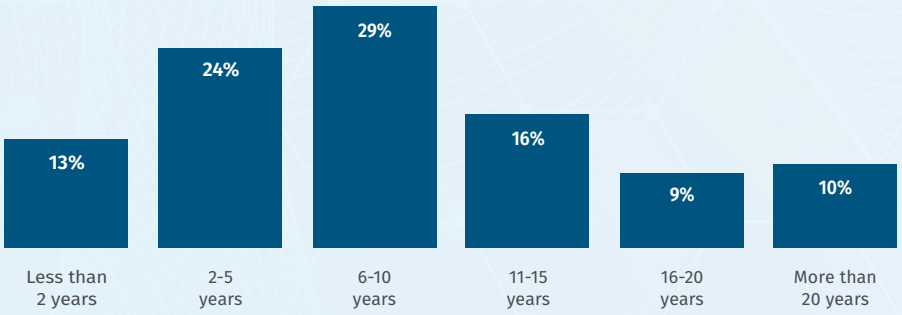
Graph 37: Professional Role



Graph 38: Cybersecurity Team Size Distribution



Graph 39: Years of Experience



Acknowledgments

2026 Cybersecurity Workforce Research Report
by SANS | GIAC

Community Awareness:

A special thank you to the following individuals:

Jay Bhalodia
Microsoft

David Caswell
Microsoft

Kerry-Ann Barrett
Organization of American States (OAS)

Deidre Diamond
CyberSN

Jessica Porter
RSA Conference

Linda Gray Martin
RSA Conference

Britta Glade
RSA Conference

Dr Kevin Jones
Bayer

Meg Waloschek
Bayer

Kim Loohuis
Independent Copywriter

Fabio DiFranco
ENISA

Evangelos Ouzounis
ENISA

Danielle Santos
NICE

Davina Mentle-Pruitt
NICE

Karen Wetzel
NICE

Rodney Petersen
NICE

Jack Poller
Paradigm Technica

Elizabeth Regan
Cyber Guild

Debbie Sallis
Cyber Guild

Lynn Dohm
WiCyS

Liz Lacey
SHRM

Nick Schacht
SHRM

Confidence Staveley
CyberSafe Foundation

Elise Yacobellis
ISSA

David Koh
Cyber Security Agency of Singapore

Kok Wee Ong
Cyber Security Agency of Singapore

Tin Jun Kong
Cyber Security Agency of Singapore

www.sans.org

SANS | GIAC CERTIFICATIONS

www.giac.org