2025

Enterprise Cybersecurity Talent Index

Are enterprises attracting the best candidates or blocking their own success?

Executive summary

One of the main topics of conversation in cybersecurity is the perceived cybersecurity talent gap. Some argue that it's not a talent gap but rather a skills gap. Others assert that there's neither a lack of talent nor skills, but rather a lack of *focus* on who they actually need protecting their environments.

One thing is for certain: enterprise security teams are in crisis. A number of factors are at play: demand for experienced personnel is up, cybersecurity risk is rising, the threat landscape is expanding, and talent dynamics are evolving faster than most hiring strategies. These conditions create a volatile mixture that could affect the security resilience of global enterprises.

So where does the fault lie? Talent? Skills? Strategy?

We gathered and analyzed ***over 5,000 cybersecurity or cybersecurity-adjacent job postings from Fortune 100 companies.*** And from this data, we concluded that the primary issue lies in the *hiring strategy*, rather than any sort of perceived (or real) talent or skills shortage. Our view is that these enterprises are misaligned with both market conditions and candidate expectations.

The result? The enterprises that desperately need cybersecurity personnel are inadvertently alienating candidates and pushing talented professionals to seek out career paths outside of security, often in emerging fields like the nascent observability industry. Thus, ironically, the strategy gap that originates within enterprises is actually contributing to the perceived talent shortage that they're suffering from.

> **These conditions create a volatile mixture that could affect the security resilience of global enterprises.**

Why did we do this? To equip organizations to find and recruit top cybersecurity talent.

This report will dive into a number of important trends.

- **There's a remote work paradox.** Only 8% of enterprise cybersecurity roles offer remote work, yet 43% of the remote roles in our study attracted over 100 applicants.
- **Despite a clear burnout crisis, mental health is still overlooked.** Only 10% of cybersecurity job listings mention wellness or burnout support.
- **Degree requirements are fading.** Only 23% of cybersecurity roles mention needing a four-year degree.
- **Cybersecurity roles pay less and offer fewer perks than those in adjacent areas.** Cybersecurity roles have a lower average pay ($152.7K annually) than roles in related areas. Equity packages are only mentioned in 4% of the analyzed cybersecurity job postings.
- **AI isn't a senior-level priority yet.** Half of all analyzed job descriptions reference AI, but 0% of director-level or higher jobs require AI knowledge or experience.
- **Observability is the new frontier.** Observability roles lead cybersecurity in average annual pay ($165.4K), flexibility, and applicant interest. (Observability is just one example of a field where security professionals can successfully leverage their technical expertise.)

While nothing is certain, we hypothesize that enterprises that consider these findings when building their hiring strategies will set themselves apart and have an easier time drawing in the high-caliber talent they seek. The perception of a "talent shortage" or "skills gap" will fade away, as top applicants seek and find open job roles, and enterprises carry on building a resilient defense around their most valuable data and assets.

Contents

Research methodology and important definitions

Expel conducted this research in partnership with Method Research. Method sourced global job postings (including contractor opportunities) for the Fortune 100 companies within the Information Technology job category with an emphasis on cybersecurity, security, observability, IT security, and DevOps keywords.

Method sourced the data from LinkedIn and Indeed job postings between March 6 and March 9, 2025. After cleaning and deduping, **the dataset contained 5,026 records.**

This larger dataset allowed us to focus on cybersecurity and cybersecurity-adjacent personnel throughout the organizational chart, versus other great studies that have historically focused strictly on senior leadership. With the broader aperture, we hoped to compare and contrast various trends across the different levels of the business. And we feel we accomplished just that.

Important definitions

This study approaches the issue of identifying the right cybersecurity hiring strategy from a number of different angles and often finds itself using similar but not interchangeable job groupings. The appropriate groups will be explicitly identified within the appropriate places, to avoid confusion.

The overall goal of this study is to equip organizations **to find and recruit top *cybersecurity* talent**.

> **The overall goal of this study is to equip organizations to find and recruit top cybersecurity talent.**

Throughout the study, you'll see cybersecurity roles contrasted with various IT security roles. We found it interesting that enterprises used different nomenclature for these positions. We don't know why that is; it could be that the IT security roles sit within an IT team, and cybersecurity roles are on a specific cybersecurity team. Or it could simply imply that some enterprises are using legacy "IT security" job titles, while others choose to be more specifically in the "cybersecurity" camp.

No matter the reason, we chose to highlight some of the differences that exist in the data between the two roles throughout the report. Doing so could shed light on the different philosophies of certain organizations, based on their job title nomenclature preferences. It could also account for some of the salary differences we see as a result later in our analysis.

A third term discussed in the study is *observability*, which is entirely separate from (though similar to) security-related disciplines. Observability is defined as the ability to understand the internal state of a system or systems by collecting, analyzing, and correlating data from logs, metrics, and traces—enabling faster detection, diagnosis, and resolution of issues.

You can see a robust list of job titles for each of these groupings in Appendix A.

Sample "cybersecurity" job titles

Cyber Strategy & Risk Sr. Consultant, Sr. Manager - Security Incident Response Team, Senior Compliance TPM, Senior Information Systems Security Officer

Sample "IT security" job titles

Application Security Engineer, Security Governance Specialist, Security Engineer I, Senior Systems and Infrastructure Engineer

Sample "observability" job titles

Senior Site Reliability Engineer, Senior Full Stack Engineer, Cloud Engineer, Senior Developer Experience Engineer, Technical Consulting Engineer

CHAPTER 1:

Where the jobs are (and where they're not)

You'd be hard-pressed to find someone who's unaware of the ongoing debate around return-to-office (RTO) mandates versus the work-from-home (WFH) alternative. It'd be even harder to find someone without an opinion on said debate.

RTO hawks say that being together in a traditional office environment creates connection between coworkers and spurs collaboration that's simply unsustainable in remote workforces.

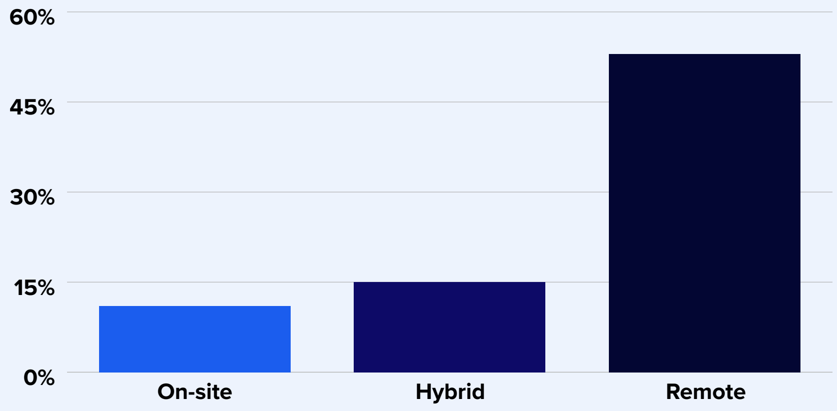
However, those who favor remote working would argue the opposite—that video conferencing gets the job done just fine, thank you very much. WFH advocates argue that this work arrangement better fits their lifestyles, making them more productive and overall happier in their roles.

When it comes to job location preferences, our research found that there's a clear disconnect between enterprises and the cybersecurity personnel they're trying to recruit. Remote work accounted for only 8% of open cybersecurity roles, while the rest specified on-site or hybrid (a mix of working from home and from an office) requirements.

Despite being a small percentage of open cybersecurity roles, remote jobs were the most sought after by far. Forty-three percent of those remote cybersecurity roles had 100 or more applicants. By contrast, only 11% of onsite roles and 15% of hybrid roles had 100 or more applicants.

Remote roles attract significantly more applicants in cybersecurity

Percentage of cybersecurity roles receiving 100+ applications by work location



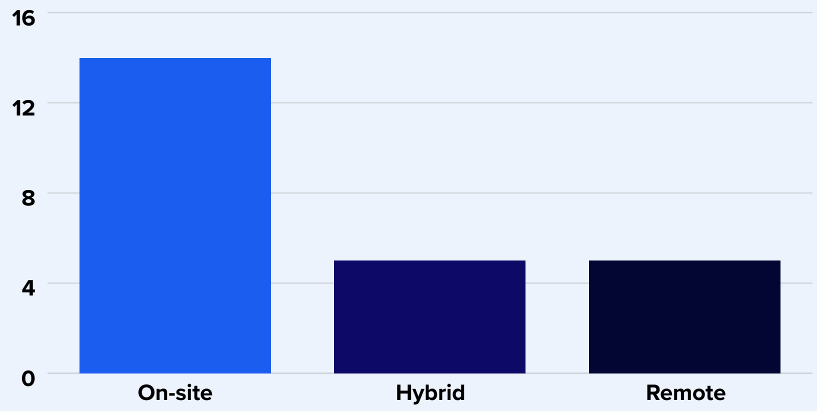
KEY INSIGHT

Remote work accounted for only 8% of open cybersecurity roles. Despite this, 43% of remote cybersecurity roles attracted 100+ applicants, compared to only 11% of on-site roles and 15% of hybrid roles. This indicates a clear demand for remote opportunities within cybersecurity.

To clarify, we can only speculate as to *why* these numbers look the way they do. It could be that the workers applying for remote roles don't live close enough to an onsite location, so commuting is impossible, or it could be the preference for working from home because it's simply more convenient. The data is interesting nonetheless.

Remote and hybrid roles fill faster

Percentage of roles remaining open for over one month



KEY INSIGHT

On-site positions take nearly 3x longer to fill than remote/hybrid roles, indicating stronger candidate interest in flexible work arrangements.

This data indicates that enterprises who offer remote cybersecurity roles are receiving a higher number of candidates, and thus have a better selection of talent for those open jobs. And the data shows that on-site positions take nearly **three times longer** to fill than remote/hybrid roles.

Application

Listen, we get it. Veering away from the corporate stance on remote hiring may seem like a longshot. But if you want a fully staffed security org filled with the best and brightest, enterprises should take a hard look at their location requirements. If you want to attract a large pool of candidates and a better selection of cybersecurity talent, perhaps you can grant an exception.

CHAPTER 2:

What about burnout?

As we know, burnout is a huge issue in cybersecurity, and it has a long-tail impact on organizations large and small. In fact, we looked in-depth at the vicious cycle of alert fatigue → burnout → turnover that afflicts so many organizations, and it's often the result of unrealistic expectations placed on security personnel. We also know that burnout can have a negative impact on physical and mental health.

Of course, having mental health resources or support doesn't magically solve burnout, which is a complex problem that can be caused by a lot of factors. But having some sort of structure in place for mental health can certainly be an indicator that the organization hiring for the role has an interest in addressing workplace stressors.

Enterprises have vast threat landscapes, with dozens if not hundreds of security applications working at once to protect different elements of the tech stack. All of these applications produce alerts, which in many security operations centers (SOCs) are handled by security analysts, who investigate those alerts to find real incidents.

While estimates of precisely how many alerts a SOC receives vary, a 2020 analysis from Forrester places the volume north of 11,000 alerts per day. A Trend Micro report finds that more than half of SOC analysts are "overwhelmed" by the volume of alerts. And another survey says "more than half of respondents spend more than 20% of their time deciding which alerts should be dealt with first."

> **A Trend Micro report finds that more than half of SOC analysts are "overwhelmed" by the volume of alerts. And another survey says "more than half of respondents spend more than 20% of their time deciding which alerts should be dealt with first."**

It's been said before: attackers have unlimited chances to infiltrate an organization, but operators need to be able to block every single attempt. That puts a tremendous burden on security teams, who must often manually gather information about each alert, and then use that data to make an informed decision on whether to close it out or escalate it. One wrong move by a defender, and the attacker slips by, ready to do untold damage.

As one large data intelligence company CISO put it, "It's not feasible for a human to look at 10,000 log lines a day. And you need to overlay threat intelligence and known attack patterns if you want humans to make sense of alerts."

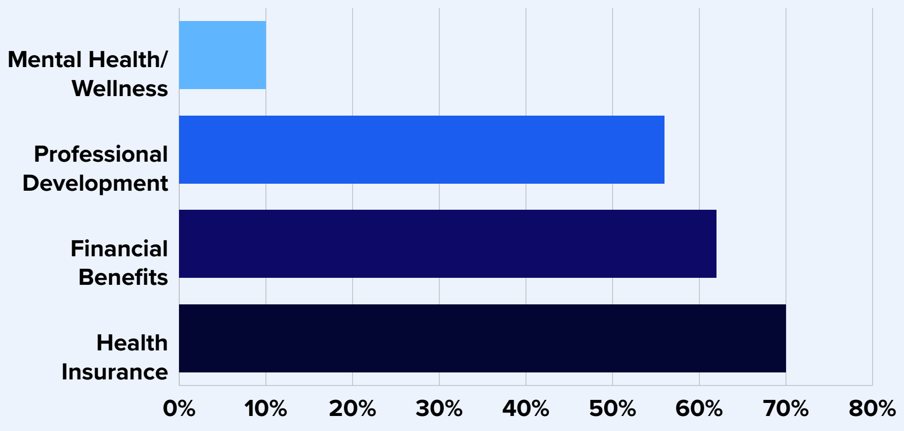
> **As one large data intelligence company CISO put it, "It's not feasible for a human to look at 10,000 log lines a day. And you need to overlay threat intelligence and known attack patterns if you want humans to make sense of alerts."**

And yet, the majority of Fortune 100 cybersecurity job descriptions fail to mention anything about mental health and burnout. Further, a recent Forrester blog post on controlling burnout in cybersecurity mapped the relationship between engagement and burnout into multiple segments. Fifty-nine percent of survey respondents were categorized as "Tired Rockstars," which is defined as "highly engaged employees experiencing some level of exhaustion." This segment of security pros was in danger of slipping into the "Red Zone," which is employees who have reached the end of their rope, and are so disengaged that they leave their jobs—and perhaps the industry entirely.

Shouldn't enterprises want to do everything in their power to retain top talent, including devoting time and dollars to keeping them in the right headspace?

Mental health support severely underrepresented

Benefit mentions in cybersecurity job descriptions



KEY INSIGHT

Despite widespread burnout in cybersecurity, only 10% of job postings mention mental health support—far below health insurance (70%) and financial benefits (62%).

Application

We at Expel maintain that burnout may be the most critical issue facing cybersecurity. However, the term has been used so much that its weight and value is eroding.

We recommend a different term to better describe the specific impact that this phenomenon has on our industry: **cyber strain**. We feel that this term better captures the physical and mental toll that cybersecurity pros experience from enduring the low-level, manual, repetitive yet absolutely critical tasks that are at the core of their work.

When it comes to attracting top talent at your enterprise, your job descriptions should make it clear that you care about your people and dedicate resources to helping your internal teams combat cyber strain. Then, of course, you have to walk the talk, else you risk attrition—and potentially souring bright security talent towards the industry altogether. In your job descriptions, also consider including quotes or testimonials from internal security personnel around your mental health programs to assure an already skeptical audience that you mean business. And if you have tools in place that help reduce the strain caused by alert fatigue, say so. It could be what helps attract your ideal candidate.

CHAPTER 3:

Money isn't everything (but it is something)

So the Fortune 100 companies have a clear preference on *where* they want their cybersecurity employees to work, but what about the other important details of their employment, like compensation packages? Unfortunately, cybersecurity roles pay less in both salary and equity than the other roles we examined.

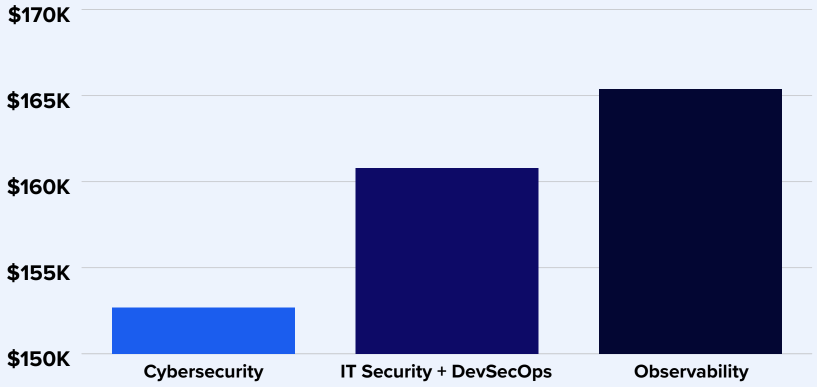
Cybersecurity positions had an average annual salary of $152,700. This might seem high to those reading this report, but remember that this is specific to Fortune 100 enterprises. Additionally, not every state requires job postings to include salary ranges—so we used the data that was available to us. That figure is, in fact, lower than other similar roles we analyzed within Fortune 100 companies. IT security and DevSecOps roles offered an average annual salary of $160,800, and observability roles had an average annual salary of $165,400.

A point to remember: just because a job description includes a salary range doesn't mean that the hire will be made within those ranges. Lots of security leaders have hired personnel outside the range created by human resources. Compounding this issue is the aforementioned confusion around job titles. Bottom line: if these average salaries—tied to questionable data and confusing job titles—are posted in job descriptions, it could cause some qualified professionals to look elsewhere.

Furthermore, only 4% of cybersecurity roles in Fortune 100s mentioned anything about equity as part of the compensation package, compared to 10% of IT security and DevSecOps roles and 15% of observability roles.

Cybersecurity roles offer lower compensation

Average annual salary by role type (Fortune 100 companies)

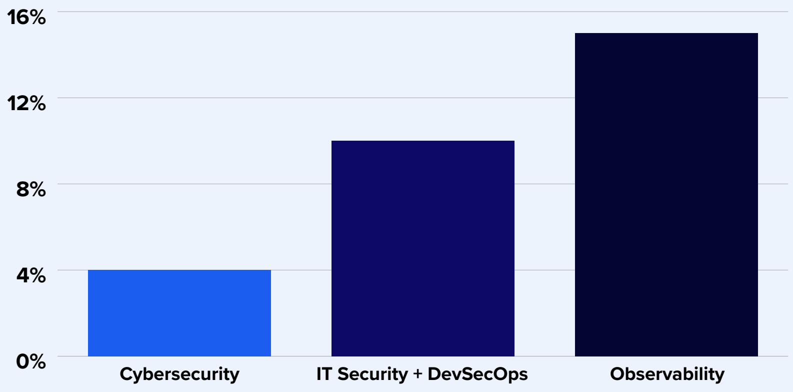


KEY INSIGHT

Cybersecurity roles pay $12,700 less than observability positions on average, potentially driving talent toward adjacent fields with similar skill requirements.

Cybersecurity roles rarely offer equity

Percentage of job postings mentioning equity compensation



KEY INSIGHT

Only 4% of cybersecurity roles mention equity, compared to 15% for observability positions—nearly 4x less likely to offer long-term financial incentives.

So, while burnout is often cited as one of the leading causes of attrition in cybersecurity, these compensation figures shouldn't be discounted either. When combined, higher rates of burnout, weaker relative compensation packages, and expectations to work from an office location could be pushing cybersecurity professionals (both on the hunt for a new role and in-seat) to seek opportunities that leverage their talents in other adjacent industries.

As we all know, compensation is just part of the package that employers offer, so we researched and analyzed some other perks that Fortune 100 orgs are offering, too. Unsurprisingly, 70% of cybersecurity job listings mentioned healthcare. Also, it's not all doom-and-gloom for cybersecurity roles. More than half (56%) of the cybersecurity job listings mentioned professional development, which outpaced both IT security and observability, where 47% and 32% of their respective listings mention professional development.

Cybersecurity was also far ahead of the other categories in terms of family leave. Twenty percent of cybersecurity roles mention family leave, compared to only 12% of IT security and 11% of observability roles.

Application

Push those salary numbers and equity shares higher, and you'll likely attract more candidates and retain your analysts longer. And, for the record, we're not advocating that you offer outrageous and unsustainable compensation packages. Use this research, as well as salary-specific data from other third parties, to help determine competitive compensation levels. Expel does this as part of our pay transparency policies.

If your company offers additional benefits—especially ones that help your roles stand out above the competition—don't be shy about touting them. Some perks, like unlimited PTO (that's genuinely encouraged and supported by leadership), generous healthcare coverage, or professional development opportunities, can set your open roles apart.

CHAPTER 4:

No diploma, no problem

When it comes to choosing candidates, experience is a big part of an applicant's story. But another traditional staple of resumes and CVs is education—and, more specifically, a four-year college degree. However, historically, we know that cybersecurity is a space where a four-year degree isn't always required. In fact, most of the security-specific positions we have at Expel don't require a degree. We're more interested in the skills, experience, and traits that candidates bring to the table.

So how did this net out for Fortune 100 companies?

In our research, both IT security and cybersecurity had 23% of job descriptions mentioning a four-year degree requirement, proving that the large majority of these roles are flexible when it comes to formal education.

Why does this matter? Mentioning a four-year degree is yet another way these orgs are artificially limiting their talent pool. It potentially weeds out people who've earned certifications, completed intensive bootcamps or training programs, offer transferable skills and experience, are seeking a mid-career transition, or simply have a good story to tell.

> **Mentioning a four-year degree is yet another way these orgs are artificially limiting their talent pool.**

Now the research isn't telling us that the jobs that mention a four-year degree actually **require** one. It may be listed as a preference or in another context. But it can still keep qualified candidates from applying, thus limiting the potential pool of qualified applicants. So enterprises should do themselves a favor and be clear on education requirements. If a bachelor's degree is a "nice to have," make sure the lack of one isn't preventing otherwise strong candidates from applying.

Application

If your enterprise currently *does* require a four-year degree, ask yourself if it really matters as much as it once did, especially considering all the alternate paths that security professionals can take for educational development. Would certain types of experience or the completion of intensive training programs do the job just as well?

CHAPTER 5:

AI on the rise

AI is seemingly everywhere. Countless trade show booths, articles in cybersecurity and tech media, conference sessions, podcasts, blog posts, whitepapers, and more have talked about the impact that AI will have on the security industry. AI promises in cybersecurity range from quick summaries of security events to full incident auto remediation, and even to scenarios of automated cyber warfare between nations. With such varied claims, it's difficult to determine AI's true impact on SOCs.

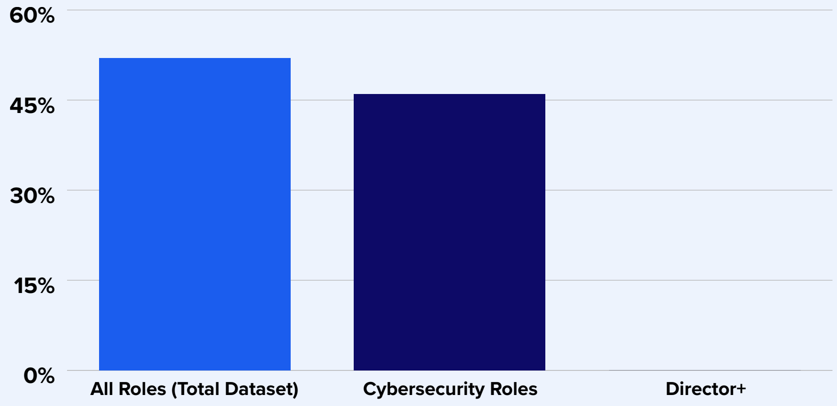
Given the hype around AI, we wanted to see what Fortune 100 enterprises were looking for in terms of AI experience and skills. And we found some pretty interesting data.

When cycling through our job role data, we found:

- 2,605 roles mentioned AI knowledge or experience (~52% of the total dataset)
- 46% of cybersecurity roles mentioned AI knowledge or experience
- **0% of directors and above required AI knowledge or experience**

AI experience mentions across key categories

Percentage of roles mentioning AI knowledge or experience



KEY INSIGHT

While approximately 52% of the total dataset mentioned AI knowledge or experience, only 46% of cybersecurity roles mentioned it. Crucially, 0% of director-level or higher jobs required AI knowledge or experience.

This data indicates that Fortune 100 employers are putting AI applications and expertise in the hands of their rank-and-file employees and supervisors. Perhaps the thought process is as follows: those closest to the day-to-day operations best know the areas and gaps where AI can add the most value and create the most efficiencies.

It's worth pointing out that "AI" takes a lot of different forms. Generative AI is by far the most popular and well-known, but that's just one AI-related term we focused on. We also looked at the terms "machine learning" (or "ML"), [standalone] "AI," "large language model" (or "LLM"), and "automation."

In cybersecurity roles, generative AI only came up 1% of the time, which was the lowest of the five terms. Automation appeared 27% of the time for cybersecurity roles and was the most frequent term. That said, we know "automation" isn't a purely AI-specific term, but AI-driven outcomes in the SOC are often the result of some automated processes, so we felt it important to include here.

What industries want AI experience? Of all the jobs that mention an AI experience requirement, 43% were in the technology and cloud space, and 21% were in financial services. Insurance and retail made up 14% each, while 7% of the roles requiring AI experience were in healthcare. Interestingly, none of the roles were in the aerospace and defense industry.

Application

It simply appears that explicit AI experience isn't a priority for senior leaders' job descriptions—despite familiarity with AI best practices and strategy being a widely understood imperative. But perhaps it should be. Otherwise, leaders run the risk of not setting a clear strategy around AI use, which could be a security risk in and of itself. At the very least, leaders should have experience in overseeing the implementation of AI in security settings and/or how their current security tools use AI to achieve outcomes or improve efficiencies.

But perhaps this present moment represents an opportunity for those leaders that actually have deep AI experience—and may even provide a path for those security professionals looking to make the progression from team member to leadership. Experience in AI—especially in how it can help make security workflows more efficient (like alert research and triage)—could be a way for these folks to set themselves apart from the competition.

And it appears that the tide may be turning on this front. Microsoft recently directed managers to include how their reports use AI tools in their performance reviews.

CHAPTER 6:

Observability, the new frontier

We've mentioned observability roles in this report a few times now, but what is it? Observability is the ability to understand the internal state of a system or systems by collecting, analyzing, and correlating data from logs, metrics, and traces—enabling faster detection, diagnosis, and resolution of issues. In today's software landscapes and cloud environments, observability is critical for maintaining the reliability, performance, and security of both applications and infrastructure.

With the surge in software system complexity, the rise of microservices, and the dependency on distributed architectures, observability has become a more prominent discipline.

Observability enhances traditional monitoring systems by enabling teams to pinpoint the root causes of issues. It empowers stakeholders to address application and business inquiries, including predictions and forecasts of potential problems. The diverse array of tools and technologies available creates a complex deployment landscape.

Why compare cybersecurity to observability? The disciplines are somewhat related, and many of the skills needed to be an effective cybersecurity operator or leader could transfer to observability roles. Another reason is that we saw these roles enough times in our research to warrant some comparison. And what we found was a little alarming.

Observability roles had an average annual salary of $165,400. This is noticeably higher than cybersecurity's average annual salary of $152,700. Fifteen percent of observability roles offer equity, which is nearly four times the number of cybersecurity roles that offer equity.

> **Observability roles had an average annual salary of $165,400. This is noticeably higher than cybersecurity's average annual salary of $152,700. Fifteen percent of observability roles offer equity, which is nearly four times the number of cybersecurity roles that offer equity.**

These generous compensation packages could be helping drive applicants. We found that observability roles were driving more applicants than cybersecurity roles (for example, 22% of observability roles had more than 100 applicants vs. 16% of cybersecurity roles), and only 12% of observability roles were posted for more than a month or more (slightly less than the 14% of cybersecurity roles).

It’s important to note that we’re not saying that observability is stealing cybersecurity talent. It’s just one category where security professionals can find roles that fit their skills and interests. But when similar jobs offer better compensation, orgs looking for talents should sit up and pay attention.

Application

Always be aware of cybersecurity-adjacent fields where candidates can use similar skills to carry out often less-stressful job responsibilities (like product and engineering roles). Use these adjacent disciplines as motivation to fight for comparable compensation for your cybersecurity personnel on the front lines. And ask your own people who may be interested in these emerging fields why they may want to consider a career change to one of these disciplines. Take these answers as feedback on how you can make your current working environment healthier and more satisfying.

CHAPTER 7:

Summary and conclusion

Our comprehensive analysis of over 5,000 cybersecurity job postings across Fortune 100 companies reveals a critical insight: the perceived "cybersecurity talent shortage" might be largely self-inflicted. Enterprise hiring strategies are fundamentally misaligned with market realities and candidate expectations, creating artificial barriers that push qualified professionals away from security roles and toward adjacent fields. It's also possible that companies simply don't know what sort of expertise they actually need, or how to articulate it.

The data paints a clear picture: enterprises are inadvertently sabotaging their own security talent acquisition efforts through inflexible work policies, inadequate compensation, and a failure to address the very real challenge of burnout—or as we suggest reframing it, "cyber strain."

Key findings and recommendations

Remote work flexibility

With only 8% of enterprise cybersecurity roles offering remote options, yet 43% of those remote positions attracting over 100 applicants, the message is clear. Organizations that embrace flexible work arrangements will gain a significant competitive advantage in attracting top talent. Leadership should model the behavior they expect—if supervisors must be on-site, executives should demonstrate the same commitment.

Addressing cyber strain

The fact that only 10% of cybersecurity job listings mention mental health or burnout support is alarming, especially given the documented crisis facing security professionals. Organizations must **implement and highlight** meaningful support systems—think employee resource groups (ERGs), generous time off, and more—to prevent burnout and turnover.

Competitive compensation

With cybersecurity roles offering lower average compensation ($152.7K) than both IT security ($160.8K) and observability positions ($165.4K), enterprises must reassess their compensation strategies. The minimal equity offerings (only 4% of cybersecurity roles) further disadvantage these positions compared to adjacent fields. Companies should conduct regular compensation analyses to ensure they remain competitive.

Education requirements

Only 23% of cybersecurity roles explicitly require a four-year degree, indicating a positive shift toward skills-based hiring. Organizations should continue this trend, focusing on capabilities and certifications rather than traditional educational credentials that may unnecessarily limit their talent pool.

AI integration

There is a significant disparity in AI requirements across organizational levels. Out of ~52% of job descriptions that had some sort of AI knowledge requirement, none were director-level and above roles. Leadership must develop AI competency to effectively guide implementation and leverage these technologies for operational advantage.

The observability challenge

The emerging observability field offers higher compensation, better work-life balance, and similar technical challenges, making it an attractive alternative for security professionals. Security leaders should recognize this competitive threat and adapt their value propositions accordingly.

But observability is just an example of other fields where security professionals can successfully leverage their technical expertise, all while making more money and not dealing with cyber strain. This isn't an observability issue specifically—it's about ensuring that organizations understand the value that security professionals bring and properly supporting them.

Looking forward

The solution to the cybersecurity talent challenge lies not in lamenting a shortage but in fundamentally rethinking how enterprises attract, develop, and retain security professionals. Organizations that recognize security talent as a strategic investment rather than a cost center will build more resilient teams and stronger security postures.

By implementing the recommendations in this report, Fortune 100 companies can transform their approach to security hiring—offering meaningful work, reasonable expectations, competitive compensation, and genuine wellness support. In doing so, they'll not only fill their open positions but build sustainable security operations capable of defending against evolving threats.

The cybersecurity talent gap isn't inevitable—it's a choice. Forward-thinking enterprises that align their hiring strategies with market realities will find themselves with robust, effective security teams while their competitors continue to struggle with chronic understaffing and the vulnerabilities that result.

APPENDIX A:

Job titles by group

Group 1: Cybersecurity

- Comcast Cybersecurity: Sr Manager, Security Incident Response Team
- Cyber Strategy & Risk Sr Consultant
- Senior UEBA Security Engineer
- Systems Engineer - CCA
- Cloud Solution Architect Manager - Cybersecurity - CTJ
- Compliance Technical Specialist
- Manager, Identity and Access Management
- LEAD CYBERSECURITY - Encryption at Rest and Secrets Management
- Lead, Infrastructure Security Engineer - Data Protection
- Cyber Trust SAP Jr Consultant
- IDC Security Engineer
- Advanced Technology and Innovation Advisor
- Advanced Technology and Innovation Advisor
- Senior Compliance TPM
- Software Development Engineer, Tech Lead
- Data Loss Prevention Policy Engineer Professional (Hybrid - 3 Days in Office)
- Information Systems Engineer II - Onsite
- Principal Information System Security Manager (ISSM) - McKinney, TX
- Principal Information System Security Manager (ISSM) - Portsmouth, RI/Marlborough, MA
- Senior Information Systems Security Officer (ISSO) - Marlborough, MA

Group 2: IT security

- Distinguished Application Security Engineer
- Senior Network Engineer, Information Security
- (USA) Staff, Systems And Infrastructure Engineer, Information Security
- (USA) Staff, Systems And Infrastructure Engineer, Information Security
- Analyst III, Technology Operations (Project Management)
- (USA) Principal, Systems and Infrastructure Engineer, Information Security
- (USA) Senior Systems and Infrastructure Engineer, Information Security
- Senior Systems And Infrastructure Engineer, Information Security
- Security Governance Specialist, Security Governance
- Security Engineer I, Security Incident Response Team (SIRT)
- Sr. Security Governance Specialist, Security Governance
- Application Security Engineer, Amazon Application Security
- Security Engineer, Security Incident Response Team (SIRT) Security Engineer I, Stores Security Pen Test
- Security Engineer II, Offensive Security Penetration Testing
- Security Engineer - Detection Engineering, Customer Logistics Security (CLS) Detection Engineering

Group 3: Observability

- Senior Site Reliability Engineer - Cisco ThousandEyes
- Senior Full Stack Engineer
- Senior Site Reliability Engineer I, Efficiency and Performance
- Senior Site Reliability Engineer II, Efficiency and Performance
- Site Reliability Engineer - Performance Testing
- Principal Site Reliability Engineer, Datastores (ThousandEyes)
- Cloud Engineer
- Software Engineer - Full stack developer
- Lead Site Reliability Engineer, Engineering Enablement - REMOTE
- Senior Developer Experience (DevEx) Engineer - REMOTE
- Site Reliability Engineer
- Technical Consulting Engineer - SP Networking
- Senior Full Stack Engineer
- Senior Site Reliability Engineer, Datastores
- Senior Technical Consulting Engineer - SP Networking
- Senior Site Reliability Engineer, Datastores

APPENDIX B:

Sample best practice job description

Senior Detection and Response Analyst

Location: Remote (US-based) | **Department**: Cybersecurity | **Reports to**: Security Operations Manager

About This Role

Join our cybersecurity team as a Senior Detection and Response Analyst where you'll play a critical role in protecting our organization from evolving cyber threats. We're committed to building a sustainable security operation that prioritizes both operational excellence and employee wellbeing.

Starting Salary Range: $155,000 - $175,000 annually + equity participation + comprehensive benefits

What You'll Do

- Lead threat detection and incident response activities across our security infrastructure
- Analyze security alerts and events to identify genuine threats and minimize false positives
- Develop and refine detection rules and playbooks to improve our security posture
- Mentor junior analysts and contribute to team knowledge sharing
- Collaborate with cross-functional teams to implement security improvements
- Leverage AI and automation tools to enhance detection capabilities and reduce manual workload
- Participate in threat hunting activities and security research initiatives

What We're Looking For

Required Experience:

- 4+ years of hands-on experience in security operations, incident response, or threat detection
- Strong understanding of security frameworks, threat intelligence, and attack methodologies
- Experience with security platforms, EDR tools, and security orchestration technologies
- Proficiency in scripting languages (Python, PowerShell, or similar) for automation
- Knowledge of cloud security principles and technologies (AWS, Azure, or Google Cloud)
- Experience with AI/ML security tools and automation platforms

Preferred Qualifications:

- Relevant security certifications (GCIH, GCFA, CySA+, or equivalent)
- Bachelor's degree in Computer Science, Information Security, or related field ***OR*** equivalent professional experience and certifications
- Experience in threat hunting and malware analysis
- Familiarity with DevSecOps practices and tools

Our Commitment to Your Wellbeing

We recognize that cybersecurity can be demanding, and we're committed to preventing "cyber strain" through:

- **Mental Health First**: Comprehensive mental health benefits including therapy coverage, wellness programs, and stress management resources
- **Sustainable Workload**: Intelligent alert prioritization and automation to reduce manual overhead
- **Team Support**: 24/7 follow-the-sun coverage model to prevent individual burnout
- **Regular Check-ins**: Monthly one-on-ones focused on workload management and career development

["Our security team has transformed how we approach work-life balance. The automation tools and mental health support have made this the most rewarding security role I've had." - Current Team Member]

Comprehensive Benefits Package

- **Health & Wellness**: Premium medical, dental, and vision coverage (100% company-paid)
- **Financial Security**: 401(k) with 6% company match + equity participation program
- **Professional Growth**: $3,000 annual learning budget for certifications, conferences, and training
- **Time Off**: Unlimited PTO policy + 12 weeks paid parental leave
- **Work-Life Balance**: Flexible remote work with home office stipend
- **Additional Perks**: Mental health app subscriptions, fitness reimbursement, and quarterly team retreats

Why Choose Us?

- **Innovation Focus**: Access to cutting-edge security technologies and AI tools
- **Career Advancement**: Clear paths for technical and leadership growth
- **Inclusive Culture**: Diverse team with commitment to psychological safety
- **Impact**: Protect critical infrastructure serving millions of customers
- **Recognition**: Regular peer recognition programs and performance bonuses

Application Process

We value diverse perspectives and encourage applications from candidates with non-traditional backgrounds. We're committed to skills-based hiring and welcome candidates who demonstrate relevant experience through bootcamps, certifications, or self-directed learning.

Ready to join our mission-driven security team?
Apply with your resume and a brief note about what excites you most about detection and response work.

We are an equal opportunity employer committed to diversity and inclusion. We do not discriminate based on race, gender, age, religion, sexual orientation, or any other protected characteristic.

Contact: careers@company.com
Learn more about our security team culture at company.com/security-careers

APPENDIX C:

Supplemental information

Figure 1: Breakdown of job descriptions analyzed, by industry

Industry	% of total companies analyzed
Aerospace & Defense	5%
Apparel	1%
Automotive & Energy	4%
Energy	1%
Financial Services	14%
Food & Processing	6%
Healthcare	10%
Insurance	8%
Manufacturing	8%
Media	1%
Oil & Gas	8%
Pharmaceuticals	4%
Retail	11%
Technology & Cloud	11%
Telecommunications	4%

Figure 2: How long the job had been posted at the time of analysis

How long the role has been posted for	All roles
A week	28%
A month	60%
Over a month	13%

Figure 3: How long the job had been posted at the time of analysis, by industry

Industry	All	A week	A month	Over a month
Aerospace & Defense	15%	9%	10%	55%
Airline	2%	2%	3%	0%
Apparel	1%	1%	1%	0%
Automotive & Energy	2%	2%	2%	6%
Financial Services	24%	27%	23%	17%
Food & Processing	5%	7%	5%	1%
Healthcare	4%	3%	5%	2%
Insurance	3%	4%	2%	6%
Manufacturing	3%	2%	4%	1%
Media	1%	0%	1%	0%
Others	0%	0%	0%	0%
Pharmaceuticals	2%	4%	2%	1%
Retail	15%	16%	16%	3%
Technology & Cloud	21%	21%	24%	2%
Transportation	1%	1%	1%	7%

Figure 4: Breakdown of open roles across industries, by job category

Industry	All	Cybersecurity	IT Security + IT Security Desk + DevSecOps + Security by Design	Observability
Financial Services	24%	25%	28%	18%
Technology & Cloud	21%	12%	12%	32%
Aerospace & Defense	15%	33%	9%	11%
Retail	15%	7%	23%	11%
Food & Processing	5%	5%	5%	7%
Healthcare	4%	4%	4%	5%
Insurance	3%	2%	2%	3%
Manufacturing	3%	3%	2%	2%
Airline	2%	2%	2%	3%
Automotive & Energy	2%	1%	2%	2%
Pharmaceuticals	2%	2%	2%	2%
Transportation	1%	0%	4%	1%
Apparel	1%	0%	1%	1%
Media	1%	0%	2%	0%
Others	0%	0%	0%	0%

Figure 5: Breakdown of seniority across all analyzed open job descriptions

Role seniority	All
Non-Mgt	80%
Supervisor + Team Lead	6%
Senior Manager + Manager	10%
Senior Director + Director + VP + C-level	5%

Figure 6: Breakdown of net-new jobs versus backfill positions

Role seniority	All	The role is not new and not associated with growing the team	The role is new or associated with growing the team
Non-Mgt	80%	81%	69%
Supervisor + Team Lead	6%	6%	6%
Senior Manager + Manager	10%	8%	20%
Senior Director + Director + VP + C-level	5%	5%	4%

Figure 7: Average number of applicants for each role, by role seniority

Role seniority	Average number of applications
Non-Mgt	40.5
Supervisor + Team Lead	37.2
Senior Manager + Manager	38.6
Senior Director + Director + VP + C-level	50.3
All	40.6

Figure 8: Percentage of job applicants for each open role, by job category

Number of applications	Cybersecurity	IT Security + IT Security Desk + DevSecOps + Security by Design	Observability
Nobody	6%	3%	3%
1 to 25 people	50%	44%	41%
26 to 50 people	17%	17%	18%
51 to 75 people	7%	11%	10%
76 to 99 people	4%	5%	5%
100+ people	16%	20%	22%

Figure 9: Percentage of job applicants, by job location

Number of applicants	On-site	Hybrid	Remote
None	6%	3%	1%
1 to 25 people	46%	44%	23%
26 to 50 people	16%	21%	15%
51 to 75 people	9%	11%	12%
76 to 99 people	4%	5%	8%
100+ people	19%	17%	43%

Figure 10: Frequency of cybersecurity software mentions across job descriptions

Cybersecurity Software Mentions	
Identity	56%
AWS	44%
SSO + Single sign-on	35%
Azure	22%
Kubernetes	18%
SaaS	6%
Cloud-native	5%
SIEM + securityinformationandeventmanagement	4%
Vulnerability management	4%
EDR + endpointdetectionandresponse	4%
Malware	2%
Threat response + Threatdetection + Threatdetectionandresponse	2%
Threat hunting	2%
SOAR + securityorchestrationautomationandresponse	1%
MFA + multifactor authentication	1%

ABOUT EXPEL

Expel is the leading managed detection and response (MDR) provider trusted by some of the world's most recognizable brands to expel their adversaries, minimize risk, and build security resilience. Expel's 24/7/365 coverage spans the widest breadth of attack surfaces, including cloud, with 100% transparency. We combine world-class security practitioners and our AI-driven platform, Expel Workbench™, to ingest billions of events monthly and still achieve a 17-minute critical alert MTTR. Expel augments existing programs to help customers maximize their security investments and focus on building trust—with their customers, partners, and employees. For more information, visit our website, check out our blog, or follow us on LinkedIn.