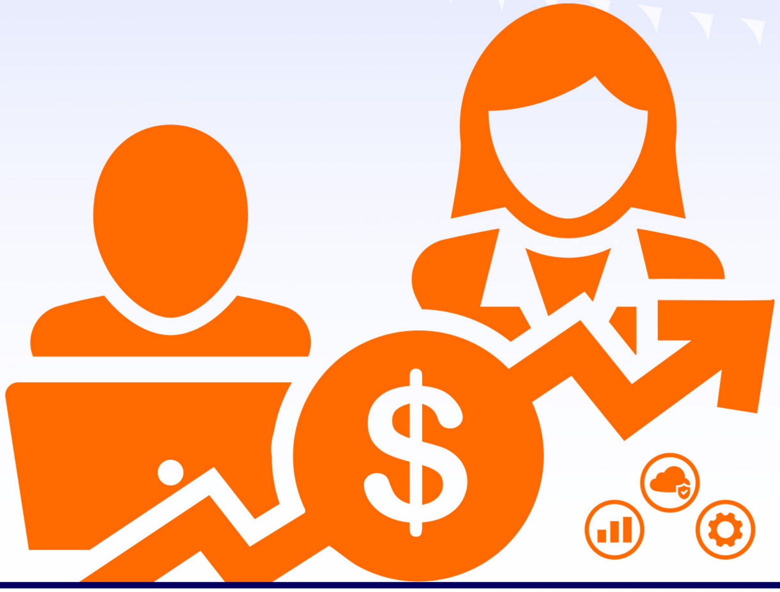
IANS + ARTICO



2025 Cybersecurity Staff Compensation

Summary Report

This summary report provides high-level insights from our 2025 Cybersecurity Staff Compensation Benchmark Report.

The complete 2025 Cybersecurity Staff Compensation Benchmark Report is a comprehensive, 30-page breakdown that offers a more detailed set of data and is available to IANS clients through the IANS Portal or to non-clients upon request by contacting us at info@iansresearch.com.

Table of Contents

Executive Summary

Talent shortages have long plagued the cybersecurity sector, leaving CISOs grappling with understaffed teams to execute critical security initiatives. Demand for skilled professionals continues to outpace supply, particularly in specialized and technical roles. This imbalance pressures CISOs to offer more competitive compensation, yet many find their standard salary bands inadequate. Given that many employees are considering a job change within the next 12 months, CISOs must remain vigilant, as their teams are highly susceptible to poaching by competitors.

To retain and attract top talent, CISOs require infosec-specific market compensation rates, as well as a clear understanding of staff satisfaction drivers and the critical skill areas for high-demand roles.

The second annual staff compensation and career survey

To provide firsthand insight into staff compensation, critical skill areas and satisfaction, IANS and Artico Search fielded their annual Staff Compensation and Career survey for which we captured responses from more than 525 cybersecurity staff across a range of industries and company types in the U.S. and Canada. This report presents insights from the survey, including staff compensation data, day-to-day responsibilities, common career paths and job satisfaction.

Key findings

Cybersecurity roles are extremely heterogeneous in titling and without clear role boundaries

Over 75% of respondents reported unique titles representing management, functional staff and specialized roles. With many security organizations shorthanded, staff often support multiple functions within the cyber domain. Among respondents, 61% work across multiple infosec domains, often combining responsibilities in areas such as SecOps and governance, risk management and compliance (GRC), or application security (AppSec) and product security. The data also shows overlap across day-to-day responsibilities, with cloud responsibilities, threat and vulnerability management, and detection and monitoring among the daily tasks of security analysts, architects and engineers.

Compensation varies widely by role, region and level of expertise

Security architects and engineers based in the U.S. earn the highest average annual cash compensation (annual base salary plus on-target bonus) at $206,000 and $191,000, respectively, while mid-level security analysts with about five years' experience earn, on average, $133,000 annually. Pay scales jump considerably with skill level; respondents considered experts in their field earn two-and-a-half times more than peers who are new to their role. Regional differences are significant, with staff in the U.S. West region earning the highest pay, followed by the U.S. Northeast.

The IT domain provides essential experience for key functional roles

Over 70% of security engineers and more than half of security analysts and security architects acknowledge their IT background was crucial for their current positions. Within IT, professionals in these roles most frequently cite systems admin, network/infrastructure engineering and general IT experiences as must-have skill sets. Many of them also have a background in infosec, often as security analysts or in SecOps. Nontechnical backgrounds are less common for most cybersecurity roles.

Job satisfaction is mediocre, with many staff actively considering a change

Only a third of respondents are likely to recommend their employer, and over 60% are contemplating switching jobs within the next 12 months. Among those considering a change, dissatisfaction with career progression stands out as a key issue, while work-life balance is less of a concern. Dissatisfaction with career progression is highest among functional department heads—professionals already in senior roles—underscoring the importance of clear pathways for continued growth in improving retention.

Return-to-office mandates clash with staff preferences

Many organizations are revisiting work-from-home policies, but cybersecurity professionals overwhelmingly prefer remote or hybrid arrangements. Currently, 52% work remotely and 43% are in hybrid setups, with 59% expressing a strong preference for fully remote work and only 1% favoring on-site roles. Forcing a shift back to the office in this talent-scarce field risks disengagement, increased turnover and recruitment difficulties. Offering flexible work arrangements is critical to meeting employee expectations and staying competitive in the tight cybersecurity talent market.

Why CISOs Should Read This Report

This report provides insights into cybersecurity staff roles that extend beyond any single organization, with the sample representing a broad range of company types of different sizes and sectors, with a range of ownership structures.

This report uses data and analysis that can help CISOs compare their current and planned staff roles inside their own security organizations and provide guidance to security leaders as they prepare to embark on a search. The information below includes:

Responsibilities by role

These include the set of day-to-day tasks the main security functions carry out, as well as the overlap among key domains.

Staff compensation data

Key compensation metrics and ranges included for key roles—security architects, security engineers, security analysts and risk/GRC specialists.

Key factors that impact compensation

These include experience level, region and education, including by how much these factors influence comp.

Satisfaction levels among staff

This gives an indication of which groups may have a higher likelihood of looking for a job change and provides suggestions to reduce attrition risk.

Expert perspectives on the data

These come from prominent CISOs and from executives at Artico Search based on their 15-plus years of CISO recruiting and career guidance, including Steve Martano, IANS Faculty member and partner in Artico Search's cyber practice, and Matt Comyns, Artico Search's co-founder and president.

Cybersecurity Staff Wear Multiple Hats

We identified the core responsibilities of cybersecurity staff (functional department heads, managers/team leads, functional staff and specialists), both in terms of the functions they support, as well as their day-to-day activities.

Looking at the key cybersecurity functions—SecOps, GRC, architecture and engineering, AppSec, product security, and identity and access management (IAM)—we found most staff (61%) work across multiple functions, dedicating at least 30% of their time to more than one domain. The remaining share (39%) focuses exclusively on a single domain.

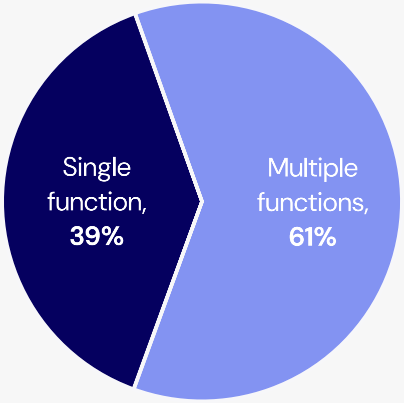
FIGURE 2

Source: IANS & Artico Search

Cybersecurity Staff Commonly Support Multiple Security Functions

Which of the functional areas below accounts for at least 30% of your time?

Functions that account for at least 30% of a role's time



Common combinations of functions that staff support at least 30% of the time

	SecOps	GRC	A&E	AppSec	Product security	IAM
SecOps						
GRC	41%					
A&E	27%	18%				
AppSec	22%	16%	26%			
Product security	49%	40%	48%	70%		
IAM	33%	34%	23%	29%	26%	

Less than 25% | 25% – 40% | 41% – 54% | 55% – 99% | 100%

Among cybersecurity staff who support multiple domains (with each domain receiving at least 30% of their time), certain combinations are particularly common. These include AppSec and product security, as well as SecOps and GRC. Additionally, product security and, to a lesser extent, IAM frequently overlap with other domains.

This situation often occurs in smaller organizations that lack the budget to hire dedicated specialists across all domains. It can also occur in larger firms where comprehensive security tools reduce the need for dedicated staff; instead, versatile team members who can manage responsibilities across multiple functions are required. Temporary vacancies may also lead to redistributed responsibilities among existing staff.

Some cybersecurity domains inherently share responsibilities and skill sets, enabling the creation of combined roles. For example, application security and product security often pair due to their shared goals of securing software and systems throughout the development process. Similarly, SecOps and GRC are commonly linked, as SecOps focuses on operational defense, while GRC ensures adherence to policies, regulations and compliance standards.

> “When companies hire individuals with versatile skill sets, it not only offers managers flexibility when priorities shift, but it also exposes team members to broader parts of the security function that may benefit them in their career development. With broader mandates, managers can flag high performers who may have the aspirations and skill sets to manage multiple functions over time.
>
> —
>
> *Steve Martano*

Cybersecurity Staff Compensation

We combined respondents' self-reported annual base salaries and on-target bonuses to arrive at their annual cash compensation. To ensure a fair comparison, this analysis includes only compensation figures from U.S.-based staff (95% of the sample).

Security architects and security engineers earn above-average annual cash compensation, averaging $206,000 and $191,000, respectively. Additionally, around one-third of respondents in both roles received annual equity grants as part of their compensation packages.

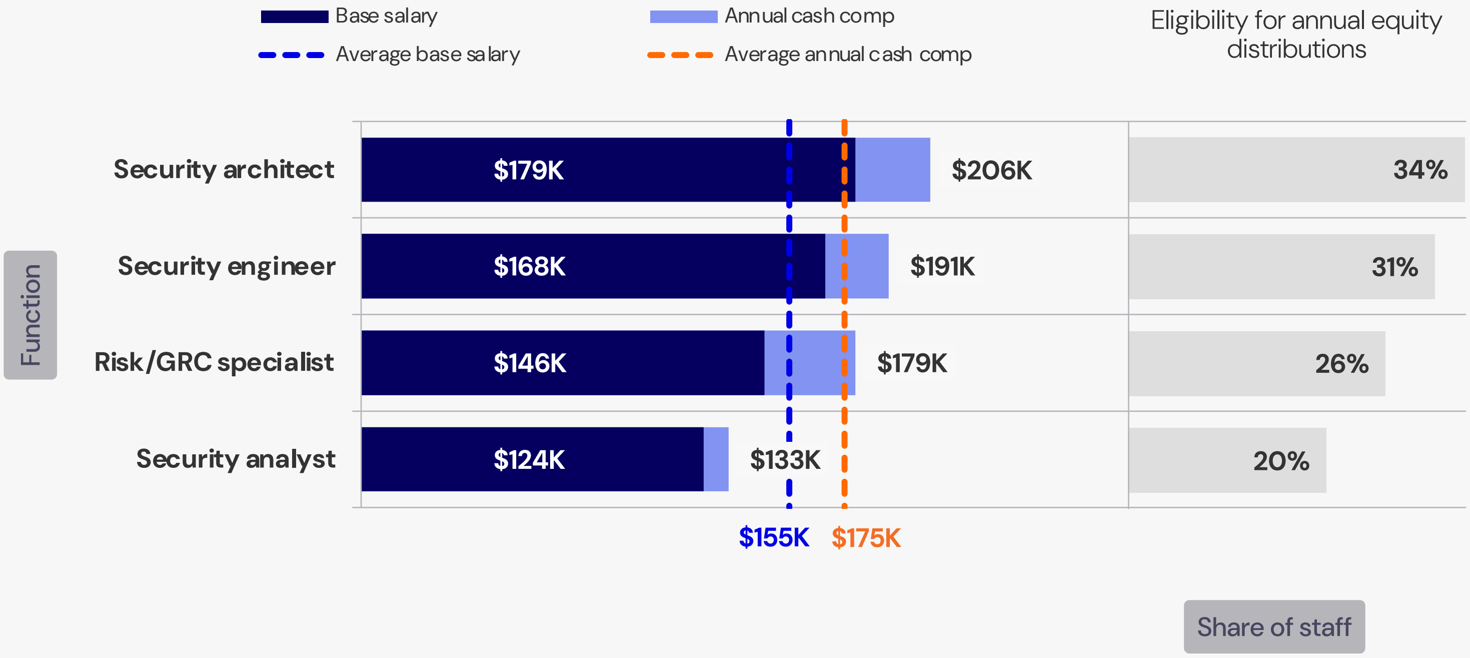
Risk/GRC specialists report an average cash compensation of $179,000, with 26% indicating they receive annual equity grants.

In contrast, security analysts have the lowest average cash compensation at $133,000, with 20% eligible for equity grants.

FIGURE 4 *Source: IANS & Artico Search*

Compensation for U.S.-Based Functional Staff, by Role

Base salary and annual cash compensation (base salary and target bonus), in USD



Pay differences by region

Regional pay differences are driven by factors such as cost of living, demand for talent, industry presence and local economic conditions. Using data on respondents' work location, we compared the average compensation across four U.S. regions—Northeast, Southeast, Central and West—as well as Canada.

Across the sample, staff in the U.S. West region report the highest average cash compensation, followed by the Northeast, with a $51,000 gap. The West region's higher compensation ties back to higher cost of living in many west coast cities, as well as a large concentration of tech companies, which typically offer premium pay to attract experienced cybersecurity professionals.

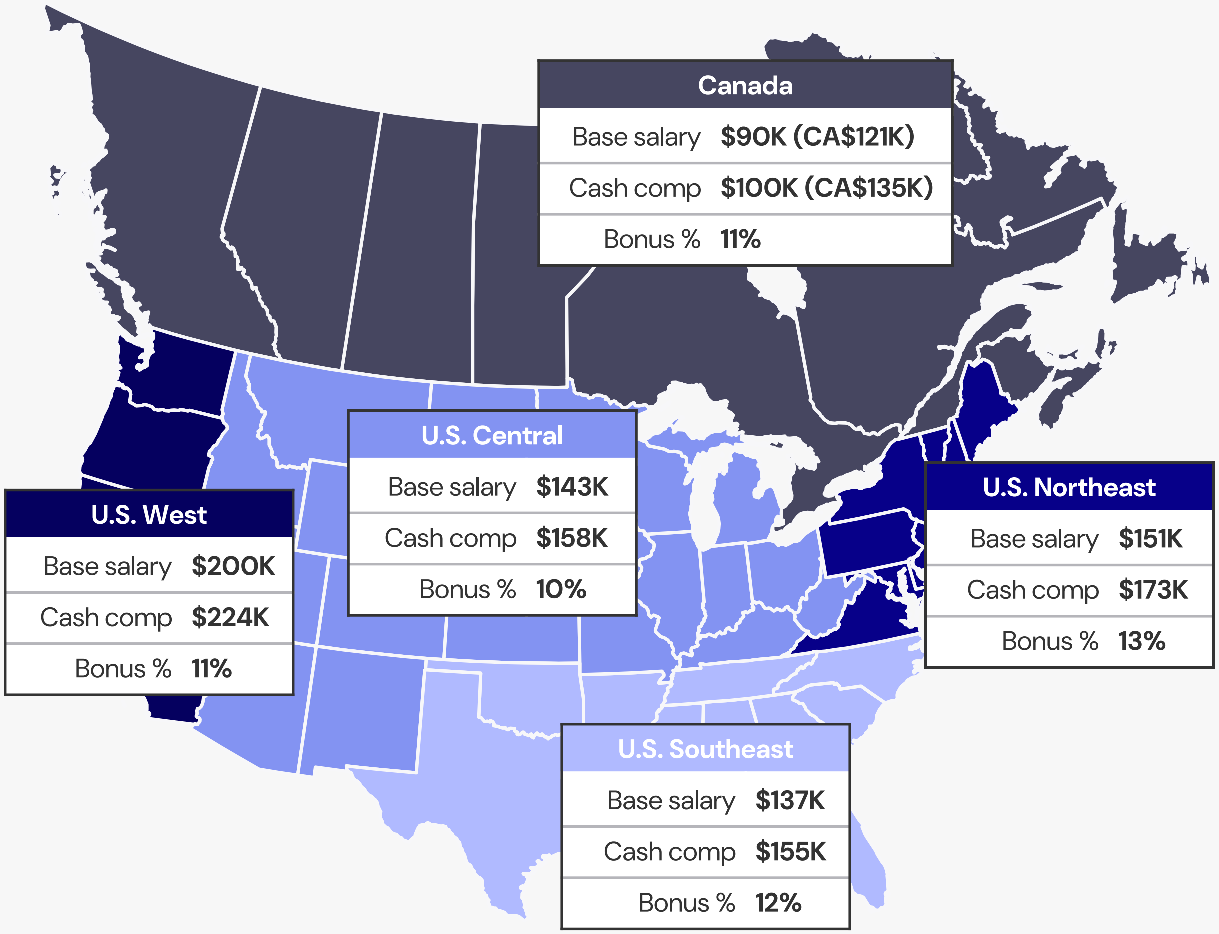
The Northeast region, especially New York City, is home to many major financial institutions, including banking and investment firms. The region also has many biotech, pharma and health insurance organizations. Both the finance and healthcare sectors operate under stringent regulatory requirements and face persistent cyber threats, leading to a high demand for skilled infosec professionals. This explains the higher compensation in the Northeast compared to the Southeast and Central regions.

Canada generally offers lower compensation than all U.S. regions. This is not unique to infosec; it extends to most other sectors as well. Even in Canadian business centers like Toronto and Vancouver, salaries tend to lag behind those in the U.S., reflecting broader economic conditions and cybersecurity maturity.

FIGURE 7 *Source: IANS & Artico Search*

Regional Differences in Functional Staff Compensation

All figures are based on the staffers' primary location of work. Figures are averages, in USD (unless otherwise specified), and rounded to thousands.



Canada	
Base salary	$90K (CA$121K)
Cash comp	$100K (CA$135K)
Bonus %	11%

U.S. West	
Base salary	$200K
Cash comp	$224K
Bonus %	11%

U.S. Central	
Base salary	$143K
Cash comp	$158K
Bonus %	10%

U.S. Northeast	
Base salary	$151K
Cash comp	$173K
Bonus %	13%

U.S. Southeast	
Base salary	$137K
Cash comp	$155K
Bonus %	12%

Job Satisfaction and Attrition Risks

Many organizations use net promotor score (NPS) to gauge the satisfaction and loyalty of both customers and employees—providing insight into how likely they are to recommend the organization/workplace to others. For CISOs and cyber leadership, employee NPS can serve as an insightful indicator of engagement and retention:

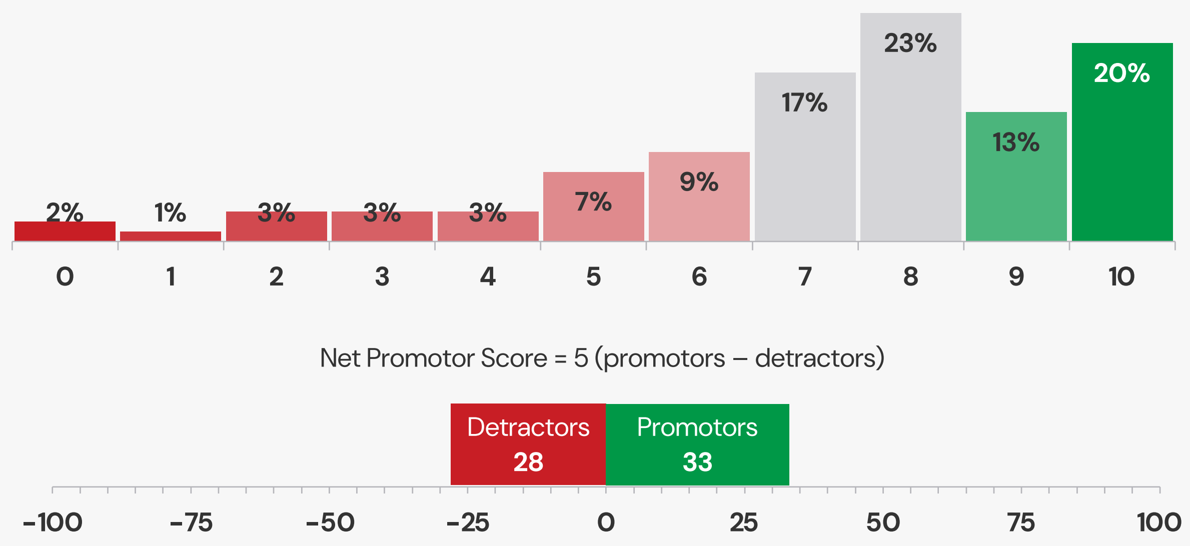
- A low NPS (less than 0) may signal a higher risk of employee attrition.
- A high NPS (30 or higher) often correlates with stronger satisfaction, lower attrition and a greater likelihood of employee referrals.

Our research shows one-third of cybersecurity staff and management are promotors—scoring a 9 or 10 when asked if they would recommend their current workplace to others. Meanwhile, 28% fall into the detractors category, scoring 6 or lower. The resulting NPS score is 5 (33% promotors minus 28% detractors).

FIGURE 12 *Source: IANS & Artico Search*

One-Third of Cybersecurity Staff Would Recommend Their Employer vs. 28% Who Wouldn't

Would you recommend your current workplace to others?



When examining NPS by role, functional staff report the highest level of workplace advocacy, with an NPS of 11 and the lowest level of detractors at 23%. In comparison, functional department heads have a negative NPS of -2, indicating detractors outnumber promotors in this group. Security middle management falls in between these two groups with an NPS of 2, reflecting slightly more-balanced levels of satisfaction.

These findings highlight challenges of promoting skilled functional staff into people-leadership roles without the proper expectations and/or training.

To further pin down potential causes, we delve deeper into satisfaction in the next two sections.

Low NPS foreshadows attrition

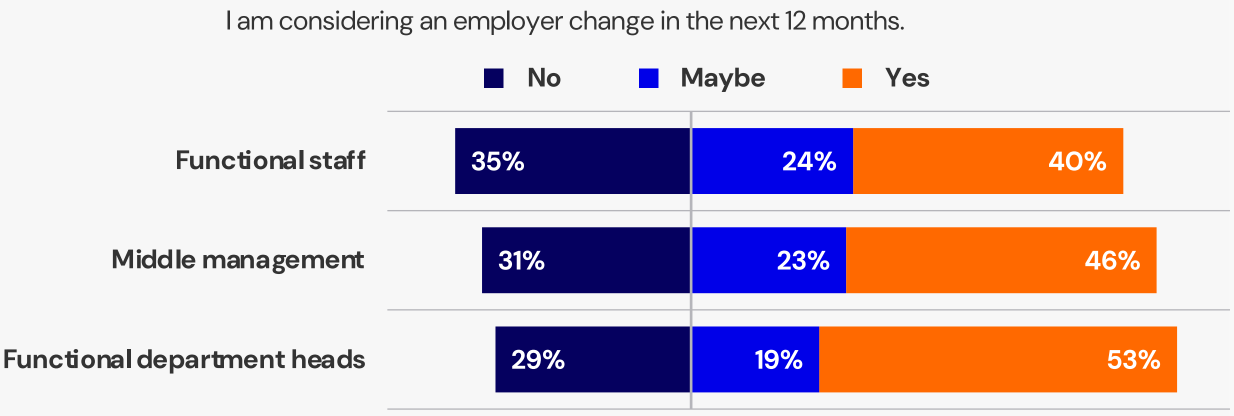
NPS ratings closely align with employees' considerations of changing employers. Among functional department heads, 53% indicate they are contemplating a change in the near future, compared to 46% of middle management and 40% of functional staff.

While these considerations do not always translate directly into actual attrition, they signal potential motivational challenges and underlying dissatisfaction with certain aspects of the job. Notably, only 9% of respondents reported having changed employers in the past 12 months, highlighting that, while actual turnover has been low, the expressed intent to leave may reflect latent engagement issues that warrant attention.

FIGURE 13 *Source: IANS & Artico Search*

Most Staff Contemplate a Change in Employers

Do you agree with the statement, "I am considering an employer change in the next 12 months"?



Percentages may not total 100% due to rounding.

Career progression concerns

To understand the concerns of staff considering a job change, we analyzed their responses to a set of satisfaction-related questions. Among respondents who answer “yes” to the question “Are you considering an employer change in the next 12 months?” more than 60% expressed satisfaction with their work-life balance, so this is likely not a primary driver of dissatisfaction.

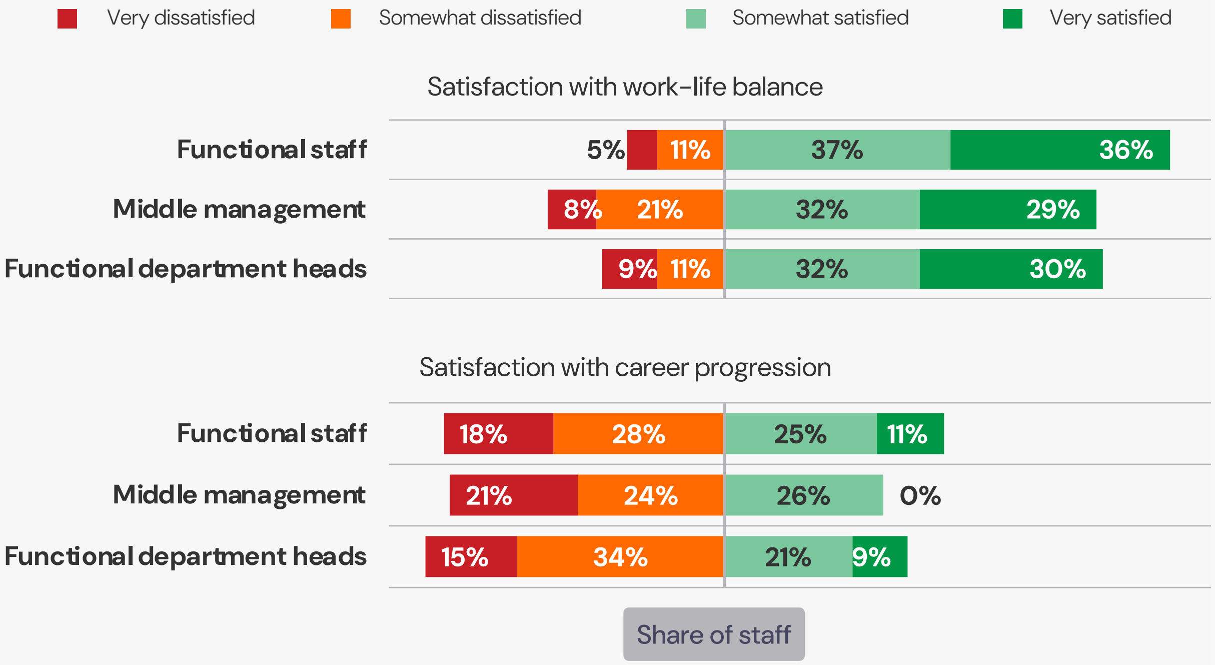
The same is not true of career progression. Fewer than 40% of respondents considering an employer change reported being satisfied with their career advancement, while more than 45% expressed dissatisfaction.

These findings suggest that while people are being promoted to higher-level roles, they often feel impatient and believe they are ready for the next step—typically, the CISO role for functional department heads.

FIGURE 14 *Source: IANS & Artico Search*

Staff Career Progression Satisfaction Lags Behind

Satisfaction with work-life balance and career progression among staff who indicated they are considering a job change



Percentages do not add up to 100% because "neutral" responses are not included in the chart.

> “CISOs should always be thinking about their highly valued and high-performing employees’ engagement level. Some managers and leaders may outgrow the roles an organization can offer, which can increase the risk of attrition. Instead of letting this happen without addressing it, plan ahead. Let high performers know what may be next for them and give them a voice to advocate for what challenge they may wish to take on next. If there’s simply no room for growth, the best CISOs advocate for their high performers in the market so they can land a great job elsewhere and continue to serve as a sounding board for their former boss and advocate for their previous company in a positive way.
>
> *Steve Martano*

Recommendations for CISOs to Attract and Retain Staff

Given the competitive market for cybersecurity talent, organizations should prioritize three areas to maintain stability and support growth of their infosec teams: retaining existing talent, attracting new talent and fostering the success of both current and new employees.

Based on the research outlined in this report, our panel of experts at IANS and Artico Search provides the following recommendations to address these priorities.

Retaining current staff

The research revealed significant retention challenges, with many infosec staff and leaders considering a job change, coinciding with dissatisfaction with their career progression. To address this, organizations must prioritize creating clear career advancement pathways, enhancing communication about growth opportunities and implementing leadership development programs. Additionally, regular performance reviews and personalized career planning can help employees feel valued and supported, reducing turnover risks and fostering long-term loyalty.

Attracting new staff

In budgeting for and crafting comp packages designed to attract strong cybersecurity talent, leaders must align compensation and opportunities with market realities. Most professionals in the field possess diverse experience across functions like SecOps, AppSec and GRC, making them highly adaptable but also highly sought after. To compete effectively, organizations should offer compensation packages that reflect expertise and proficiency levels, recognizing top-tier talent often commands a premium of up to 40% more at each successive skill level. Additionally, regional pay disparities, with the West and Northeast demanding higher rates, should inform recruitment strategies. By offering competitive pay, emphasizing career growth and showcasing opportunities for impactful, multifunctional work, organizations can attract top talent in a competitive market.

Fostering staff success

The research highlighted the importance of prior IT and infosec experience in shaping the success of cybersecurity professionals, particularly in technical roles like analysts, architects and engineers. To foster success, organizations should focus on providing targeted training that builds on these critical skills while addressing any gaps in knowledge. Offering mentorship opportunities with seasoned professionals and encouraging collaboration between IT and security teams can further enhance skill development and adaptability. By aligning professional development initiatives with the key experiences that contribute to success, organizations can empower their staff to excel in their roles and drive meaningful contributions to the security function.

Methodology

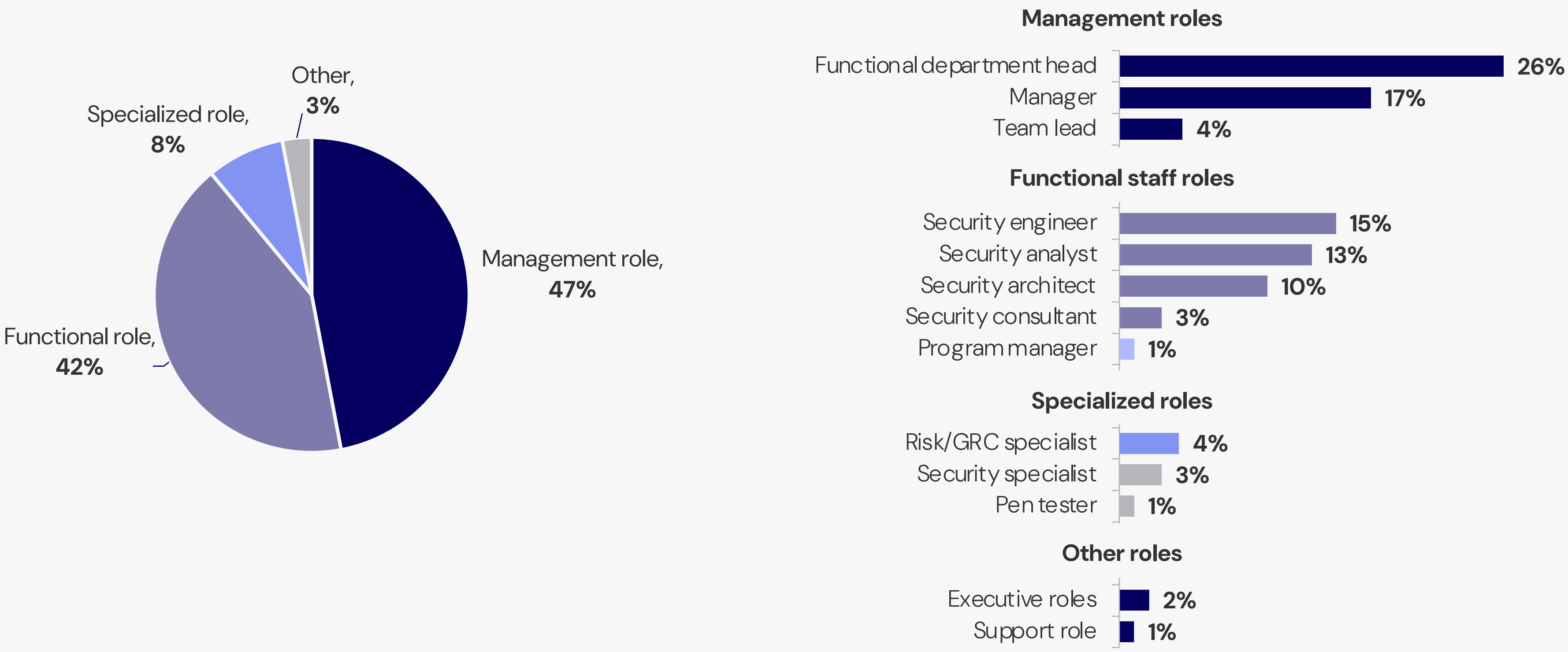
This report is produced jointly by IANS and Artico Search. Data scientists and researchers from IANS collected data, ran analyses and engaged with CISOs to identify trends and market insights. Market experts at Artico Search, including Steve Martano, IANS Faculty member and partner in Artico Search's cyber practice, and Matt Comyns, Artico Search's co-founder and president, provided actionable guidance and relevant quotes.

The data presented in this report comes from the annual Staff Compensation and Career survey, fielded from June 2024 until the end of 2024. We received survey responses from 528 security professionals that represent a wide range of roles— management (47%), functional roles (42%), specialized roles (8%) and other roles (3%). The full breakdown by role is shown below.

FIGURE 16 *Source: IANS & Artico Search*

Sample Breakdown by Role

What best describes your current role?



About Us

This publication is created in partnership between IANS and Artico Search.

Artico Search

articosearch.com

Founded in 2021, Artico Search's team of executive recruiters focuses on a "grow and protect" model, recruiting senior go-to-market and security executives in growth venture, private equity and public companies. Artico's dedicated security practice delivers CISOs and other senior-level information security professionals for a diverse set of clients.

IANS

iansresearch.com

For the security practitioner caught between rapidly evolving threats and demanding executives, IANS is a trusted resource to help CISOs and their teams make decisions and articulate risk. IANS provides experience-based insights from a network of seasoned practitioners through Ask-an-Expert inquiries, a peer community, deployment-focused reports, tools and templates, and executive development and consulting.