Cybersecurity Staff Compensation, 2023–2024

Benchmark Summary Report

Table of Contents

This summary report provides high-level insights from our Cybersecurity Staff Compensation, 2023–2024 Benchmark Report.

The complete Cybersecurity Staff Compensation, 2023–2024 Report is a comprehensive, 22-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.

Executive Summary

Infosec leaders have been dealing with a talent shortage for years. Amid growing financial demands and an increasing scope of responsibility, cybersecurity leaders are facing increased pressure to do more with less, making hiring and retention a critical topic.

After speaking with around 100 CISOs, a common theme emerged: Typical corporate bands and role categorizations often do not align with the infosec talent market. Comprehensive, infosec-specific compensation data is critical for benchmarking, as recruiting in security often requires specialized compensation packages to compete for talent and minimize attrition.

A new staff compensation and career survey

To provide first-hand insight into staff compensation, IANS and Artico Search fielded a new Staff Compensation and Career survey for which we captured responses from 563 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, staff diversity, work-from-home expectations and job satisfaction.

For added context, it includes perspectives from executives at Artico Search, in particular Matt Comyns, co-founder and president, and Steve Martano, a partner in Artico Search's cyber practice and a member of the IANS Faculty of industry experts.

Highlights from the report:

Security roles are often multifunctional: In security organizations, staff at various levels often work in multiple cybersecurity functions. Typical functional combinations within a role include architecture and engineering (A&E), application security (AppSec) and product security.

Managers and directors differ in their people management scope: Most managers oversee teams of individual contributors, while directors and senior directors have manager-level direct reports with their own teams (in other words, they serve as managers of managers).

Vast experience, specialization and advanced degrees all lead to higher pay: Professionals with 12-plus years of experience earn over 20% above the average. Expertise in AppSec, product security or IAM, or a master's degree or Ph.D., also leads to higher compensation.

Gender diversity varies across domains: Twenty percent self-identify as female, binary or other. Governance, risk management and compliance (GRC) has the highest gender diversity at 40%, followed by IAM at 25%, while A&E staff has the lowest non-male representation at 10%.

Staff recognition and job perks are associated with higher retention rates: Of four criteria we asked about, feeling valued and supported, as well as having opportunity for career advancement, show the strongest relationship to job change considerations.

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, from different sectors and sizes and 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 function
These include the set of day-to-day tasks that the main security functions carry out, as well as the overlap among key domains.

Staff compensation averages
Key compensation metrics included by cyber function and role in the security organization—directors, managers, architects, engineers and analysts.

Key factors that impact compensation
For example, people management responsibilities, experience level and education, including by how much they influence comp, up or down.

Gender diversity in cyber organizations
The report considers the overall share of non-male professionals, as well as diversity within functional areas.

Satisfaction levels among security staff
This gives an indication of which groups may have a higher likelihood of looking for a job change and suggestions to reduce attrition risk. Included in full report.

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.

This report is part of the 2023–2024 Compensation, Budget and Org report series that also includes the 2023 Security Budget Benchmark Report, the 2023 CISO Compensation Benchmark Report, the 2023 Security Organization and Compensation Study, the 2023—2024 State of the CISO Report, among others.

Cybersecurity Staff Responsibilities

Among survey respondents, 42% have responsibilities that span multiple cybersecurity domains.

Certain disciplines naturally complement each other, such as AppSec, product security and IAM. As shown in FIGURE 1, among AppSec staff, 74% also contribute to product security and 67% are involved in IAM. Within product security, 63% of staff also support IAM.

On the other hand, GRC exhibits weaker ties with other roles. About 37% of GRC staff also take on A&E responsibilities, and just 25% are engaged in AppSec work.

Steve Martano elaborates on these figures:

> *We see a clear difference between the technical track within security and the governance track. Depending on the regulatory requirements and product needs of an organization, these positions are staffed at different times in a company's security journey.*

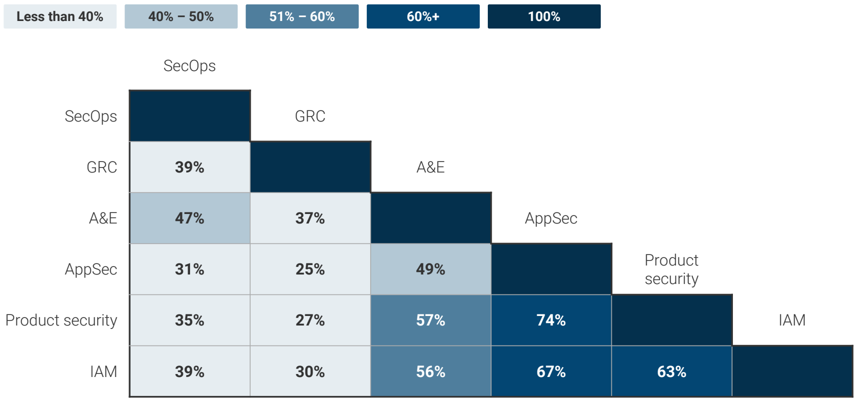
How to read FIGURE 1:

- The percentages in each cell represent the share of professionals who support both domains.
- For example: Most AppSec roles also support product security and IAM.
- Roughly half of A&E staff also support AppSec, product security and/or IAM.
- Percentages do not add up to 100% because many staff support more than two functions.

FIGURE 1

Cyber Staff Commonly Support Multiple Security Functions

Functional staff and the domains they support



	SecOps	GRC	A&E	AppSec	Product security	IAM
SecOps						
GRC	39%					
A&E	47%	37%				
AppSec	31%	25%	49%			
Product security	35%	27%	57%	74%		
IAM	39%	30%	56%	67%	63%	

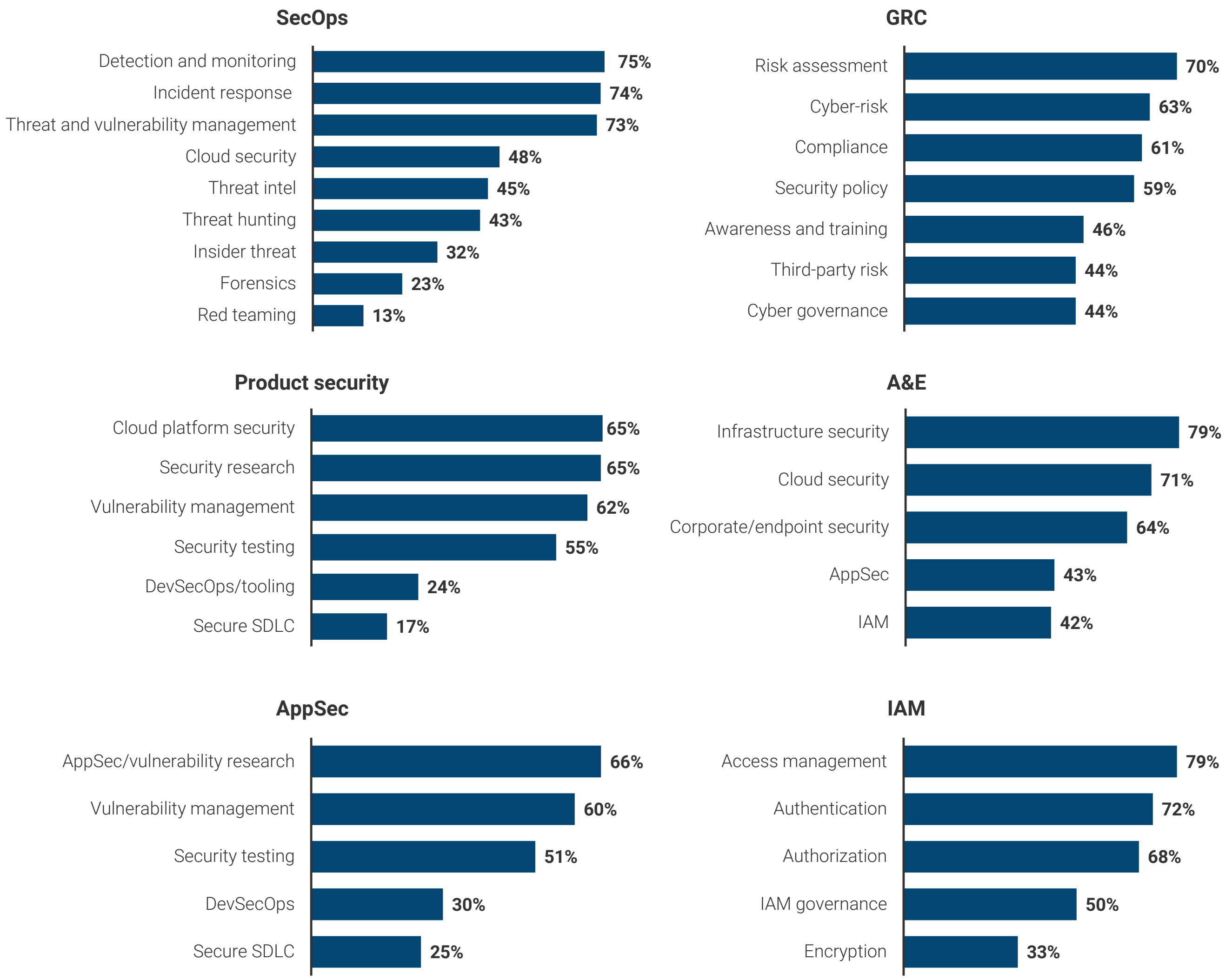
Main activities by function

Within each function, the staff is responsible for a core set of tasks. FIGURE 2 lists them by function. Notably, cloud responsibilities run across several functions, including SecOps, product security and A&E.

FIGURE 2

Day-to-Day Responsibilities by Function

Which best describes your day-to-day work activities? (Multiple answers accepted)



Cybersecurity Staff Compensation

The compensation ranges for U.S.-based staff, including cybersecurity directors, managers, architects, engineers and analysts follow in the section below.

The average annual cash compensation for directors is $258,000 with a total compensation of $330,000. Senior directors—typically, more experienced and with a larger span of control than directors—average $325,000 in cash compensation and $402,000 in total comp. About 20% of the directors' total compensation is attributable to annual equity.

Cybersecurity manager cash compensation averages $175,000. Approximately $8,000 in annual equity value brings their total comp to $183,000. For senior managers, the total comp is higher at $268,000.

Among security architects, the average cash compensation varies from $184,000 to $229,000 for senior security architects, plus annual equity which value is approximately 40% of the base salary.

Security engineer cash compensation averages $158,000 and $175,000 for senior security engineers. The equity value brings their total comp to $174,000 and $193,000, respectively.

Analysts' comp ranges are lower than those of the other cybersecurity roles in this study, with an average of $118,000 in total comp for analysts and $145,000 for senior analysts.

Compensation ranges for the top 25%

The top quartile total compensation for security directors starts at $424,000 and the top 10% average total comp for this role is $783,000.

As Figure 3 illustrates, top quartile total earnings across the various roles in the sample are considerably higher than the median pay. In many cases, the top 10% average is as much as three times the median total compensation, indicating a significant pay band within each of the roles.

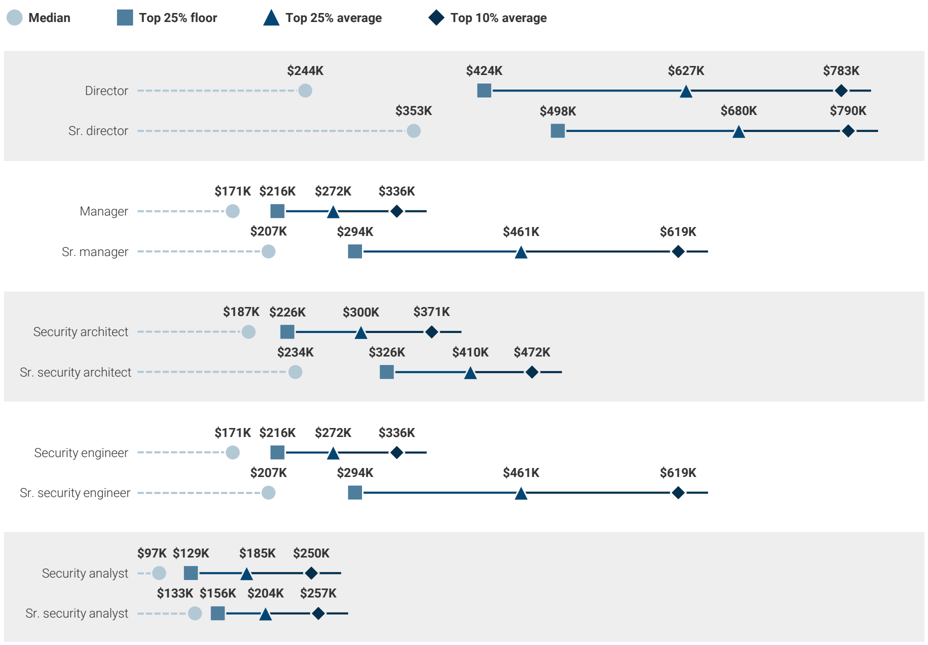
Steve Martano explains why CISOs, in general, should be mindful of the top 25% comp ranges:

> *CISOs who are concerned about attrition or are planning to begin a search for this talent should understand the market in order to target and source candidates who are in the compensation range and recruitable. If a CISO considers someone a top performer and in the top quartile for their peer group, they can then assess the compensation compared to that individual's peer group.*

FIGURE 3

Top 25% Total Compensation, by Staff Role

The median, top 25% and top 10% total compensation U.S.-based staff (USD)



Factors That Impact Staff Comp

We analyzed a range of criteria and their impact on pay. These include personal experience and education levels, gender, location and employer size.

To analyze these differences, we utilized aggregate comp data. First, we determined the overall average cash compensation and total compensation for all U.S.-based staff within the sample, setting them as the baseline at $185,000 and $210,000, respectively. Subsequently, we calculated the percentage variances of each industry from these baselines. Figure 4 shows the results.

Experience and education: As expected, experience and level of education contribute favorably to compensation levels. Experienced staff with at least 12 years of relevant experience can have an annual cash comp as much as 22% above the baseline. For those with advanced degrees, the impact on cash comp is a positive 12%. An advanced degree, in combination with a technical role, commands a premium of 21% for cash comp.

On the flip side, staff with fewer than three years of relevant experience earn packages of up to 40% below the baseline. Likewise, cybersecurity professionals who do not hold college credentials beyond an associate degree also tend to receive below-average comp levels.

Company size and type: Fortune-size companies—those with annual revenues exceeding $10 billion—tend to pay above-market rates. Many of them are publicly listed companies, a criterion that is also associated with higher pay averages. Conversely, small and midsize companies with revenues below $1 billion typically pay below the baseline. The same is true for private firms that are majority-owned by their founder or family-owned companies.

These pay disparities between fortune-size firms and small and midsize organizations exist among both people managers and individual contributors.

Gender: Our data suggests a gender pay gap of about 7%. The gender gap is more pronounced among staff with 12-plus years of experience for whom we see double-digit pay gap between male and females. Among respondents with up to three years of infosec experience, there is a 3% gap in favor of gender-diverse professionals.

The analysis did not look at potential cumulative effects of the aforementioned factors that influence pay.

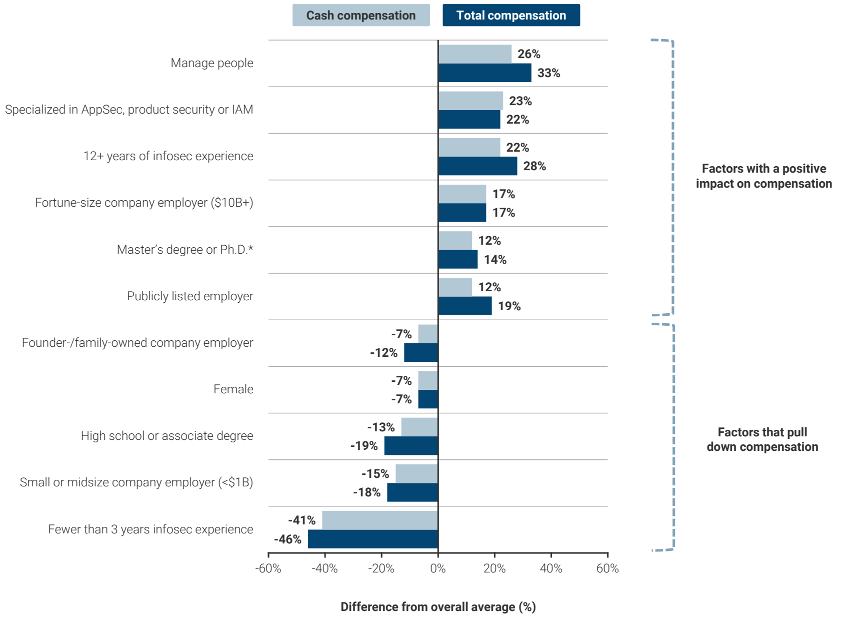
Matt Comyns comments on the pay premiums for technically specialized roles:

> *One of the reasons we see earlier-career cyber analysis-shattering pay bands is due to the lack of supply in security engineering, architecture and cloud security. These technical roles are competitive and are among the highest-paid entry-level roles available to recent graduates. Consequently, these positions are often misaligned with corporate pay bands.*

FIGURE 4

Factors That Impact Compensation

The percent difference in overall average staff compensation per factor



* For technical roles, the premium for a master's degree or Ph.D. is 21% for cash comp and 25% for total compensation

Gender Diversity Among Cybersecurity Staff

The survey data, based on gender self-identification, revealed that 20% of respondents self-identify as female or "other gender."

Gender diversity differs considerably across the six functional domains included in the study. As illustrated in Figure 5, GRC stands out with the highest percentage of non-male staff at 40%, followed by IAM at 25% (see Figure 5).

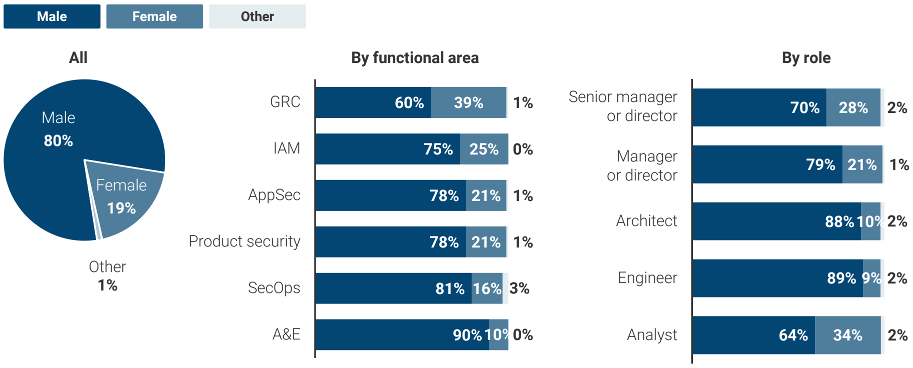
A&E and SecOps are the most male-dominated with gender diversity figures of just 10% and 19%, respectively.

Within specific roles, we see above-average representation of females among senior managers and senior directors. Also, analyst roles show a higher likelihood of being filled with gender-diverse candidates, while roles in A&E are predominately occupied by male professionals.

FIGURE 5

Gender Diversity Varies Greatly Between Functional Areas and Roles

Respondents' self-identified gender (%)



Cyber Staff Prefer Flexibility in Their Work Location

More than half of respondents indicated they work remotely and about a third are hybrid workers with between one and four days per week on site. Representing just 3%, only a slim minority work fully on site at a company office location.

If left to the staff, work location flexibility would further expand. When asked about their preferred situation, an even larger share of respondents indicate they prefer to work fully remote than is currently the case (see Figure 6).

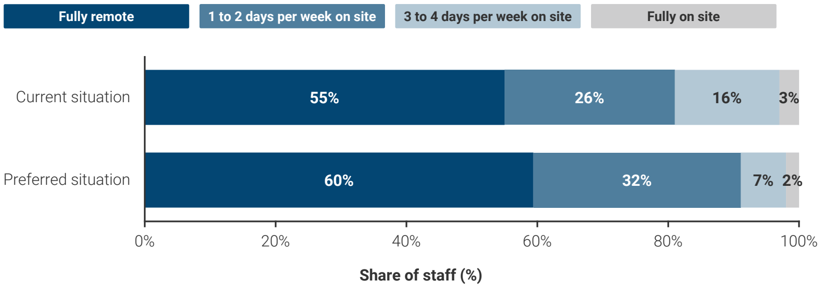
Steve Martano discusses what this means for organizations looking to introduce stricter in-office requirements:

> *Organizations pushing a return to the office should be aware that security professionals often have options for remote work. Companies with flexible work arrangements can gain an advantage recruiting top talent by prioritizing work locations and logistics overcompensation, as well as presenting a case for flexibility and a healthy work/life balance.*

FIGURE 6

Most Staff Prefer a Flexible Work Arrangement

The current vs. the preferred work situation among staff (%)



Detailed Staff Compensation and Role Insights by Function

The following pages contain a set of charts with role-specific insights and compensation ranges pertaining to the main security functions, including security operations (SecOps), GRC, and A&E.

CISOs can use the data in the charts to benchmark the responsibilities and compensation of current and future security staff on their teams.

FIGURE 7

SecOps Manager, Engineer and Analyst Roles

Functional overlap and routine responsibilities of SecOps roles

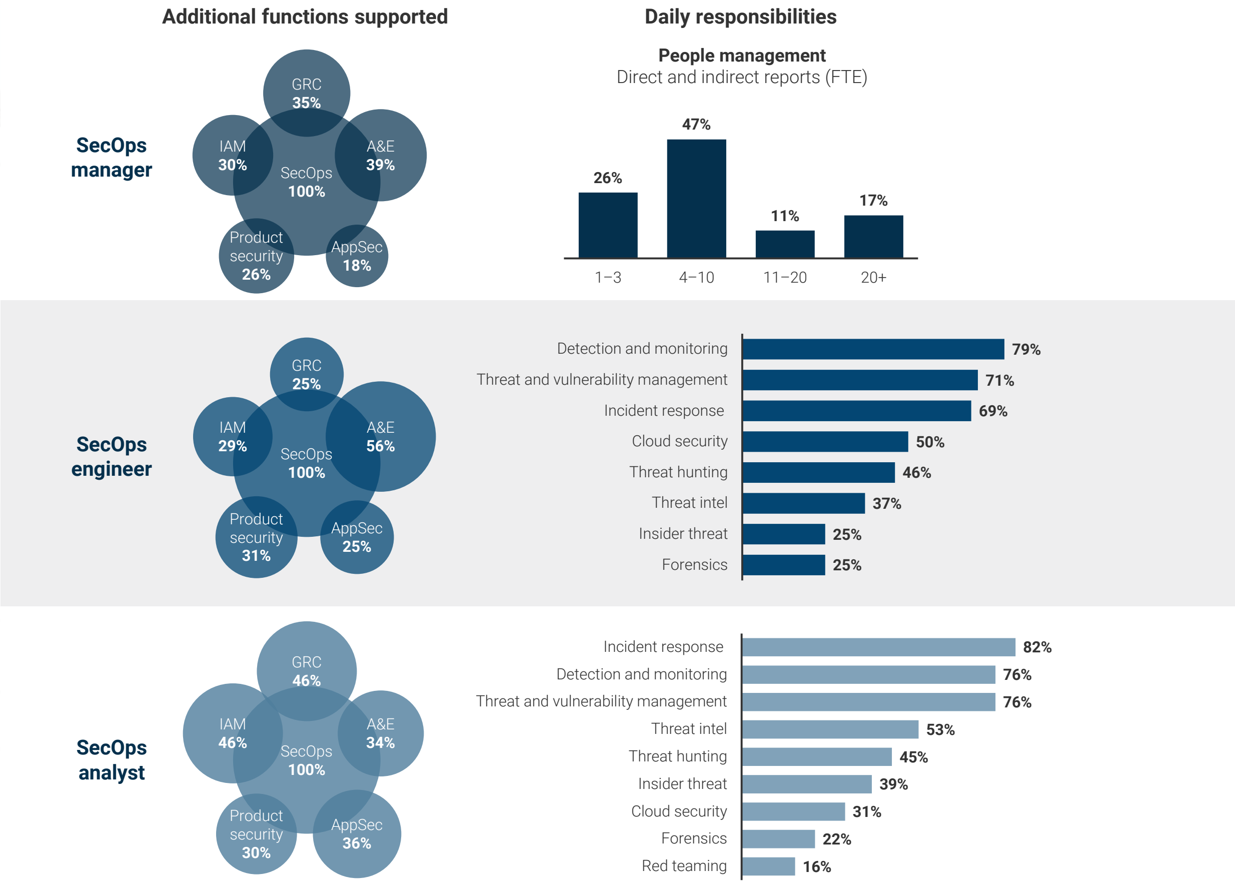


FIGURE 8

SecOps Roles' Compensation Levels

Average base salary, annual cash compensation and total compensation for U.S.-based staff (USD)

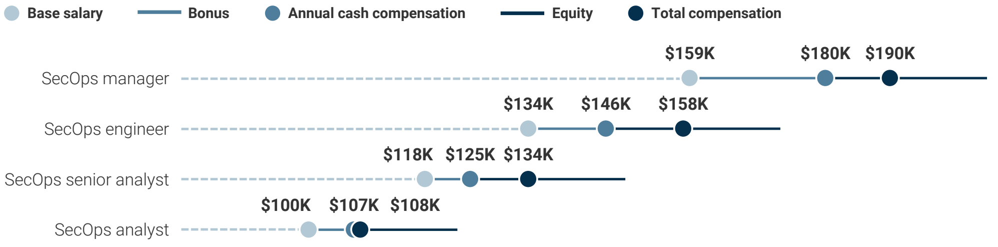


FIGURE 9

GRC Manager, Analyst and Risk Analyst Roles

Functional overlap and routine responsibilities of GRC roles

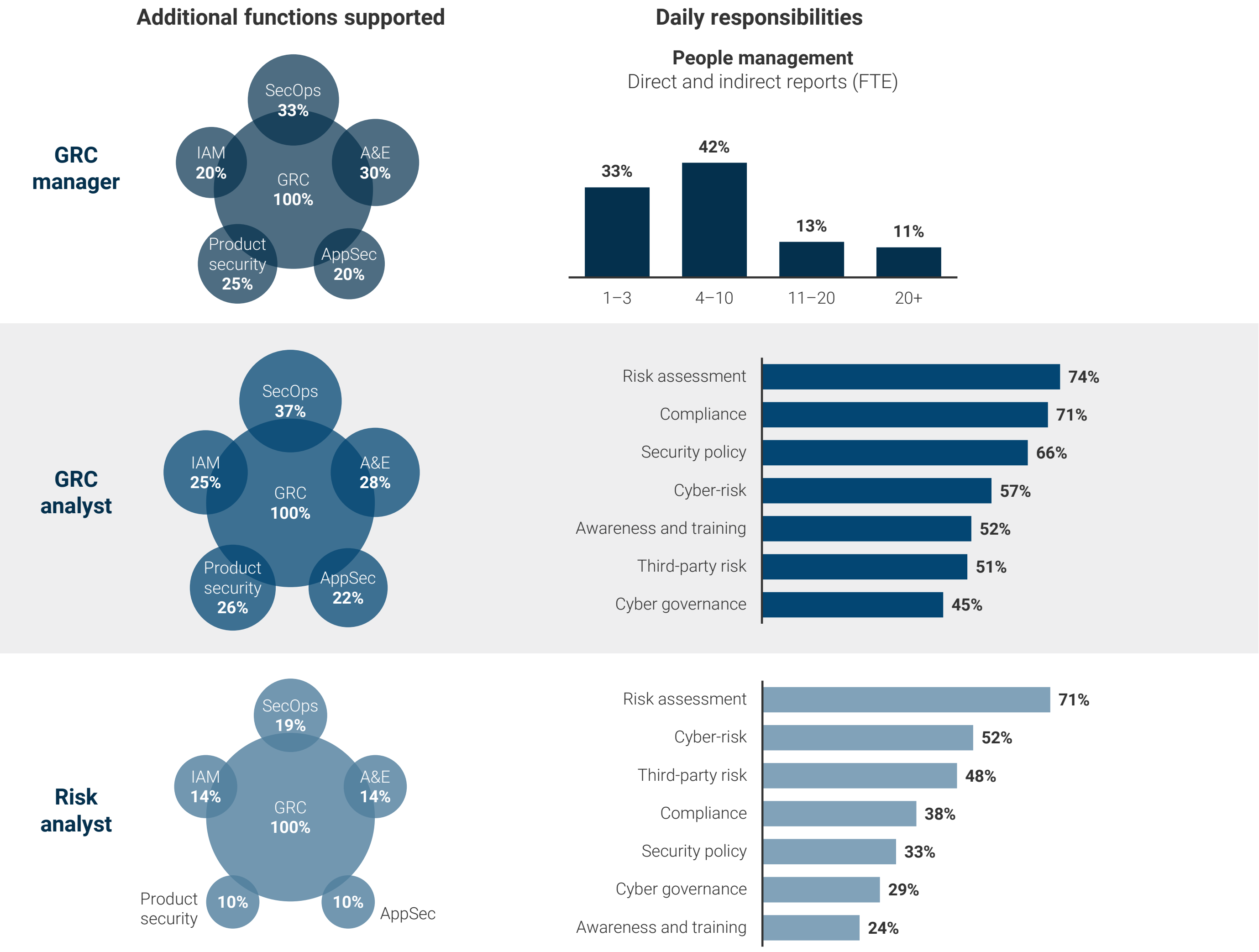


FIGURE 10

GRC Manager, Risk Analyst and Analyst Compensation

Average base salary, annual cash compensation and total compensation for U.S.-based staff (USD)

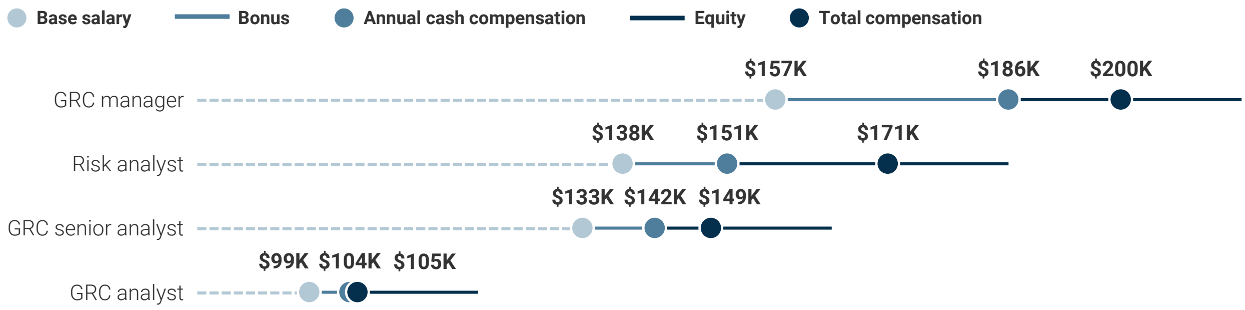


FIGURE 11

A&E Manager, Architect and Engineer Roles

Functional overlap and routine responsibilities of A&E roles

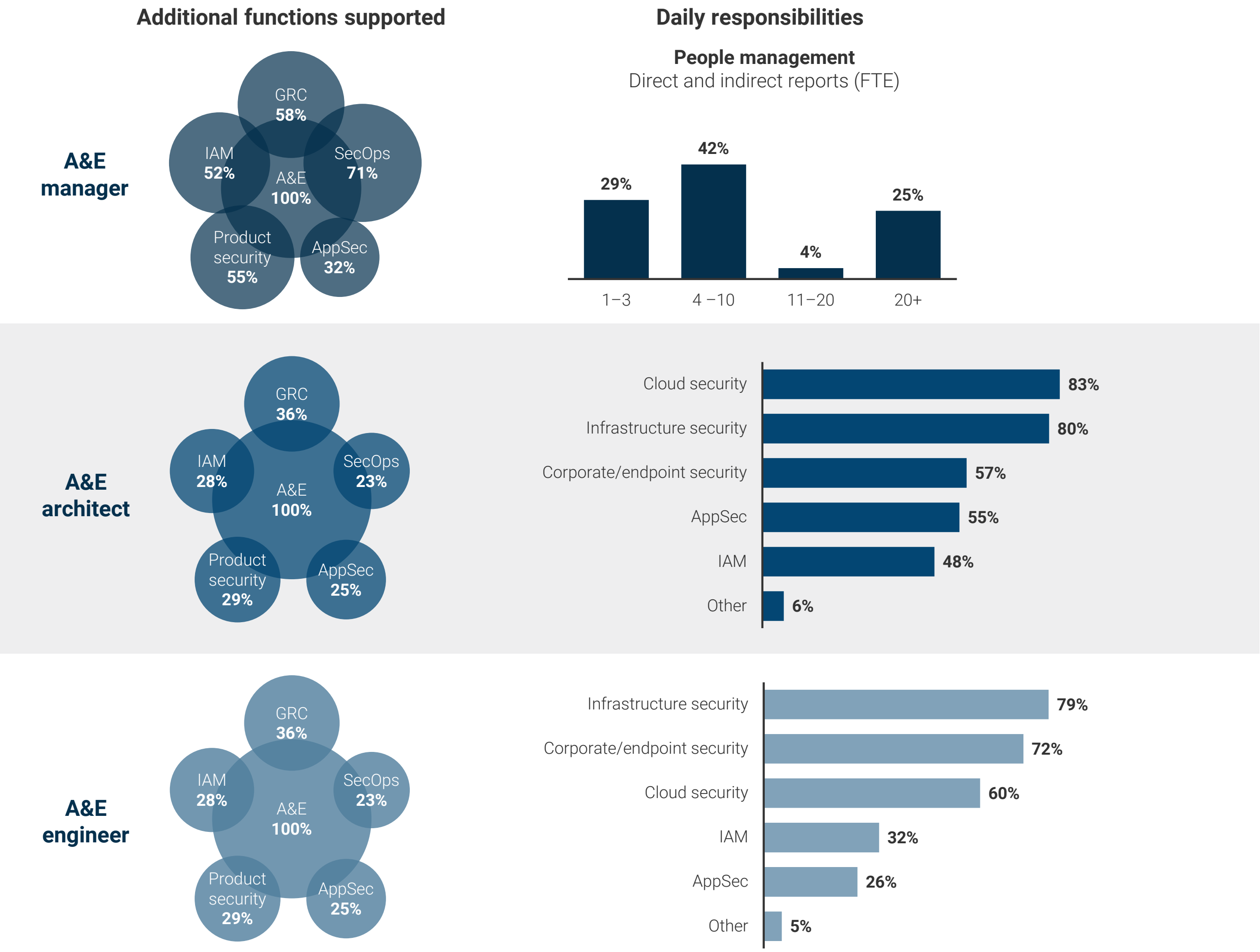
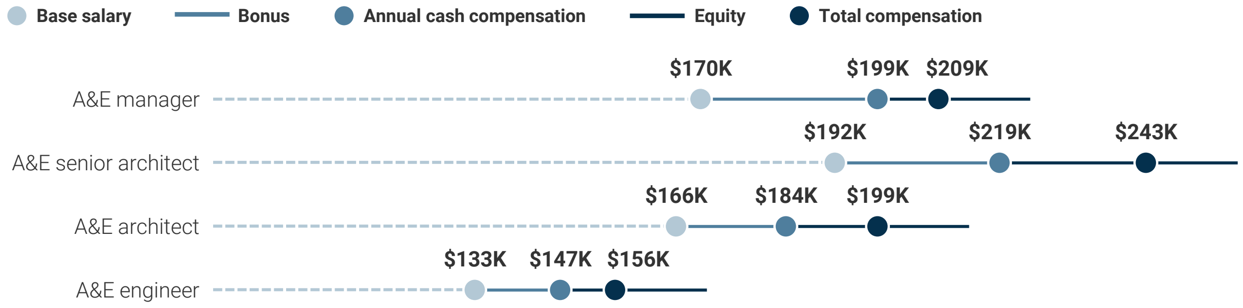


FIGURE 12

A&E Manager, Architect and Engineer Compensation

Average base salary, annual cash compensation and total compensation for U.S.-based staff (USD)



Methodology

IANS and Artico Search fielded a new Staff Compensation and Career survey in April 2023. From early April until the end of November, we received survey responses from 563 security professionals from companies that varied by size, location and industry.

Key steps in the research process are:

Survey design

We design our surveys by incorporating feedback from CISOs and respondents and by focusing on topics that clients express a strong interest in.

Data hygiene

The survey design and data collection process include precautions to prevent fake responses and survey response errors. For example, respondents can skip questions if they don't have access to the requested information.

Analysis

A five-member team runs the analysis, builds the storyline and writes the report. This is a multidisciplinary team with combined expertise in data science, cybersecurity, CISOs' key imperatives, and cyber executive talent and recruitment.

Objectivity

This research is neither influenced by nor paid for by third parties. We report on the data objectively and free from personal bias and opinions. Clarifying insights are drawn from Artico Search's cyber practice and clearly marked as quotes.

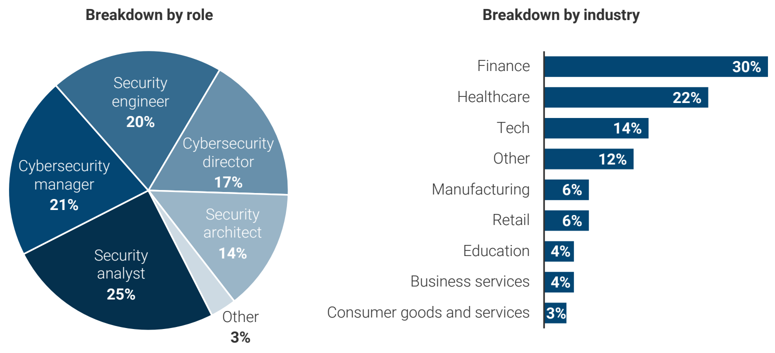
Sample breakdown

The three largest industries in terms of representation among cybersecurity staff in the sample are finance (30%), healthcare (22%) and tech (14%).

In terms of role, the sample breaks down as follows: security analyst (25%)—including GRC analyst, risk analyst or security analyst—security managers (21%), security engineers (20%), security directors (17%) and security architects (14%). Three percent indicate "other" as their role, which includes mainly security consultants and program managers (see FIGURE 26).

FIGURE 13

Sample Breakdown



"Other" includes mainly security consultants

"Other" includes mainly education, transportation, government and utilities

Respondents provided their compensation metrics, including base compensation, target bonus percentage and equity percentage. These three metrics allowed us to compute the annual cash compensation (base salary plus bonus) and total annual compensation (cash compensation plus equity) for each respondent. We then calculated the averages across the relevant sample. These are provided in several places in the report.

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.