



CORMARKGROUP

Recruitment Leaders in Cybersecurity & Technology Talent

UNITED STATES • REGULATED INDUSTRIES • 2026

2026 Cybersecurity & Technology Hiring Report

Talent, Integrity, Results - navigating the convergence of security, cloud, AI and compliance hiring across financial services and regulated industries

PREPARED BY:

Cormark Group, Inc.

AUDIENCE:

CISOs, CIOs, CTOs, Cybersecurity Hiring Managers & HR Leaders

PUBLISHED

2026

COVERAGE:

United States - Financial Services, FinTech, Insurance & Healthcare

INSIDE THIS REPORT

- Why cybersecurity roles in regulated industries have become convergence roles, and what that means for hiring
- The roles under greatest demand pressure: cloud security, AI-adjacent governance, assurance and architecture
- Directional compensation ranges for senior cybersecurity and technology roles in 2026
- What top candidates are evaluating beyond salary, and how to compete for them
- A practical playbook for defining, searching and closing high-impact cyber hires

THE MARKET AT A GLANCE

A Shortage That Is Uneven, Not Generic.

Cybersecurity hiring in financial services, FinTech, insurance and healthcare is being driven by a combination of regulatory scrutiny, cloud dependence, and AI related risk. These sectors are under pressure to make controls not only effective, but explainable, evidenced and defensible to auditors, executives and regulators.

That changes the shape of the talent market. Employers need people who can reason about technical controls, understand frameworks such as NIST, ISO 27001 and SOC 2, and work cross functionally with engineering, audit, risk and business leadership. The hardest roles to fill are not the generic analyst jobs. They are the positions requiring technical depth, framework fluency and operational judgment all at once.

514K+

Cybersecurity job openings in the U.S. with only 74 workers per 100 openings

65%

Of roles now span multiple security domains, not a single specialty

40 days

Average time to fill for focused, **exclusive searches** using the TRUST Hiring Model

The **TRUST™** Hiring Model

T Targeted Talent Mapping

R Rigorous Vetting (Technical + Behavioral)

T Transparent Partnership

TRUST™
Hiring Model

U Understanding Business Context

S Strategic Presentation
Quality > Quantity

EXECUTIVE SNAPSHOT

The Shape of Cyber Hiring Has Changed

Cybersecurity hiring in 2026 is no longer about filling one neat box on an org chart. Many of the highest value roles now sit at the intersection of security, cloud, identity, DevOps, data, AI and compliance rather than inside a single domain. This report blends Cormark Group's placements and live searches with external market data to give you a practical view of what's really happening.



KEY TAKEAWAYS

- 65% of cybersecurity roles now span multiple domains - cloud, DevOps, data, identity, AI and compliance, rather than sitting inside a single specialty.
- The market remains structurally short of experienced practitioners, with more than 514,000 cybersecurity job openings in the U.S. and 55% of organizations report understaffed teams.

- The sharpest shortage is not generic analysts, it's professionals who combine technical depth, framework fluency (NIST, ISO 27001, SOC 2) and operational judgment.
- Strong candidates in cloud security, architecture and assurance are commonly managing multiple offers simultaneously.
- Compensation is tracking complexity, not just title and density of expertise commands a material premium over narrowly scoped roles.
- Candidates weigh mission, executive support, scope quality and growth path alongside base salary and bonus.



INSIGHTS

How Cybersecurity Hiring Is Actually Playing Out

WHAT WE'RE SEEING IN SEARCHES

- Many job descriptions still treat cyber roles as single-category - AppSec, IAM, cloud security, GRC or DevSecOps. In practice, the work spills across those boundaries consistently.
- When titles and job descriptions don't reflect this convergence, searches stall because no candidate looks perfect on paper, or hires are made into roles that are broader than originally framed.
- Focused, exclusive searches with clear success definitions consistently outperform high-volume approached. Speed comes from precision, not volume.
- Cormark Group's TRUST Hiring Model defines success beyond the job description, consistently reduces time to fill and improves long term placement outcomes.

WHAT CANDIDATES ARE EVALUATING

- Multiple competing offers are common for experienced professionals in cloud security, architecture, assurance and senior engineering roles.
- Remote or hybrid flexibility is a strong preference. Candidates are actively comparing this alongside compensation.
- Career path and growth trajectory: candidates want to know what the role becomes in 12-24 months, not just what it is today.
- Mission quality and executive support: top cyber professionals are pricing the risk of the role, whether the organization is serious about security and whether they'll have real authority.
- Sign-on bonus and equity are increasingly part of the conversation, particularly for roles requiring candidates to leave competing offers.



TOP THREE CHALLENGES WE SEE

- 1 Cybersecurity roles have become convergence roles**
Security engineers are now expected to understand cloud, DevOps, data, identity, AI and compliance, not just one domain. 65% of roles span multiple areas. When job descriptions don't reflect this reality, searches stall and expectations create friction at offer stage.
- 2 Strong candidates have options, and they know it**
Experienced professionals in cloud security, architecture and assurance are frequently managing multiple interview processes in parallel. They're not just comparing salaries, they're comparing mission quality, executive support, scope and long-term trajectory. Slow or unclear processes lose them.
- 3 Generic Cyber talent without technical depth is often not enough**
Organizations relying on generic cybersecurity talent without technical depth face measurably higher breach risk, leaving teams able to monitor threats but unable to effectively contain, investigate, or remediate them in today's AI-driven, cloud-native threat landscape.

A RECENT PLACEMENT THE TRUST HIRING MODEL IN ACTION

A financial services company supporting critical U.S. market infrastructure needed a Security Assurance leader with rare expertise spanning cybersecurity, cloud systems and regulatory frameworks including NIST, ISO 27001 and SOC 2.

Using the TRUST Hiring Model, Cormark Group partnered with the hiring manager to define success beyond the job description. Within one week, 7 qualified candidates were identified and 3 finalists presented. The role was filled in under 40 days, despite the candidate receiving three competing offers.

Outcome: the placed candidate immediately brought structure to a previously reactive function, streamlined evidence collection and uncovered critical vulnerabilities. Within 13 months, she was promoted to Director of Cybersecurity.

COMPENSATION SNAPSHOT

Compensation in 2026 is tracking complexity, not just title. Employers are paying materially more for density of expertise. Candidates who can connect engineering, cloud, architecture, controls and regulated-sector expectations command a significant premium over narrowly scoped specialists.

Role	Compensation Range	Key Requirements
AI Product & Strategy Executive	\$270,000–\$300,000 + bonus	AI strategy, product leadership, regulated-sector experience
Senior AI Architect	\$250,000–\$300,000 + bonus	Design, build, and scale AI/ML systems and frameworks
Artificial Intelligence Engineer	\$190,000–\$210,000 + bonus	ML model development, AI systems, data engineering
Senior Security Engineering	\$190,000–\$220,000 + bonus	Multi-domain engineering, cloud, identity, DevSecOps
Principal Security Architect	\$180,000–\$210,000 + bonus	Architecture, framework fluency, cross-functional leadership
Cloud Security Engineer / Architect	\$150,000–\$250,000 + bonus	Broad range reflecting depth of cloud + security expertise
Quantitative Risk Model Development	\$160,000–\$200,000 + bonus	Quant modelling, risk frameworks, regulated finance
Security Cloud Engineer	\$160,000–\$190,000 + bonus	Cloud platforms, security controls, infrastructure as code
Senior Cyber Defense	\$140,000–\$170,000 + bonus	Detection, response, threat intelligence

ROLES DRIVING THE STRONGEST DEMAND

HIGH DEMAND (GROWING)

- Multi-domain security engineers and principal architects, technical depth plus business-context judgment, spanning cloud, identity, resilience and regulatory expectations.
- AI-adjacent cybersecurity roles - professionals who understand model risk, third-party AI exposure, access controls for AI tooling and governance. Moving from future issue to current hiring priority.
- Assurance, governance and evidence-heavy roles, connecting technical controls to frameworks, audit expectations and regulator-facing evidence. Increasingly strategic, not administrative.
- Cloud security engineers and architects.

WHAT MAKES THESE HARD TO FILL

- Titles still reflect single-domain thinking; job description increasingly require multi-domain capability. The gap creates friction in sourcing and assessment.
- The expectation that one person can span cloud platforms, identity and access patterns, resilience, observability and regulatory requirements simultaneously.
- Generic talent without technical depth is increasingly insufficient and regulated clients need people who understand what's actually at stake when controls fail in a regulated, high-consequence environment.
- Strong candidates have options and are weighing the quality of the role, the mission and the organization's seriousness about security before accepting.

"The highest value cyber hires are not simply busy technical contributors but strategic operators who reduce risk, enable the business, and scale security across the organization."

**CORMARK GROUP, 2026
MARKET INSIGHT**



ACTION PLAN

How to Hire Strong Cybersecurity Talent in Regulated Industries

To build a high-performing security function in a regulated environment, you need clarity on what the role genuinely requires, discipline in the search process and an offer that speaks to how senior cyber professionals actually make decisions.

Before you go to market

- Define the real intersection of which domains the role genuinely needs to cover and what outcomes are expected in the first 12–24 months.
- Clarify which requirements are truly non-negotiable versus which gaps can be trained or developed.
- Consider convergence: does your job description reflect the actual multi-domain scope of the work?
- Align compensation to complexity density of expertise commands a premium over years of experience alone.

During the process

- Use the TRUST Hiring Model: define success beyond the job description before sourcing begins.
- Pre-sell the mission - top candidates are assessing whether the organization is serious about security and whether they'll have real authority.
- Be explicit about remote or hybrid flexibility, career trajectory and sign-on structures early.
- Move efficiently because strong candidates in high-demand niches are managing multiple processes simultaneously.

After the hire

- Hire for control maturity, not just technical activity - the most valuable hires move a team from reactive to structured.
- Invest in the onboarding: clear scope, authority, tools, team structure and 90-day success definition.
- Support the build: the best cyber hires need executive backing and cross-functional access to deliver impact.
- Recognize long-term trajectory, leaders who build structure tend to grow fast. Build that into the role from day one.

IF YOU ONLY DO THREE THINGS AFTER READING THIS, DO THESE:

- 1 Treat senior cybersecurity roles as convergence roles and design job descriptions, assessments and reporting lines accordingly.
- 2 Prioritize operators who can build structure and evidencable control - not just run tools or respond to incidents.
- 3 Define success beyond the title before you go to market so the search is anchored to outcomes, not keywords.

**NEXT STEP****Let's Discuss Your Hiring Needs**

For more than 20 years, Cormark Group has been connecting exceptional cybersecurity and technology talent with organizations in financial services, FinTech, insurance and healthcare that demand excellence. We don't post and wait, we proactively identify, vet and present only the top two or three candidates for each search, saving you time and improving the quality of every hire.

If you have a cybersecurity or technology role to fill, or you're thinking about how to scale your function for the next 12-24 months, we'd welcome the conversation.

Reach out to book a call and talk through your hiring needs.

Email us at Info@Cormarkgroup.com