



U.S. Cybersecurity Job Posting Data Report

Comprehensive Report from 2022 through 2024

Source: CyberSN, 2025



©2025 CyberSN

..... Data Collection Approach

Data Collection Period: The dataset encompasses all cybersecurity job postings across the United States from January 2022 to December 2024.

Data Sources: Data was sourced from over 30 major job boards as well as websites of Fortune 500 companies.

Changes in Data Accumulation: Initially, job postings were tracked with a 45-day job posting lifecycle. Starting in July 2023, this period was adjusted to a 30-day lifecycle to reflect more current hiring trends.

Inclusion Criteria: The dataset includes both Recruiting Agency job posts and Direct Employer job posts to provide a comprehensive overview of the market.

Data Cleaning: Duplicate job postings were identified and removed to ensure the accuracy of job vacancy counts.

Data Variability and Churn: Job posting dynamics such as posts that were added on Monday and removed by Saturday, followed by a new post on Sunday, were recorded as separate job entries. This churn effect is crucial for understanding job market fluidity and may affect the overall data interpretation.

NICE Cybersecurity Framework: On March 10th, NIST released a 2.0 update. Moving forward in our next publication, our data will be adjusted to recognize that.

Top Categories per Cybersecurity Job Postings 2024

Defense

157,399

Product Security

45,162

GRC

40,597

Management

32,372

Planning

26,263

Offense

16,820

Response

13,660

Education

5,522

Research

4,935

Top 25 Cybersecurity Functional Roles Posted in 2024

CATEGORY	FUNCTIONAL ROLE	2024 JOB POSTINGS	2023 JOB POSTINGS	2022 JOB POSTINGS
Defense	Security Engineer	64,300	67,456	85,697
Defense	Security Analyst	45,496	52,579	61,385
Product Security	DevSecOps	36,020	39,052	68,598
GRC	Cybersecurity / Privacy Attorney	22,465	15,962	18,746
Planning	Security Architect	22,246	23,186	30,810
Management	Cybersecurity Manager	17,975	17,985	21,434
Defense	Identity And Access Management Engineer	12,223	16,640	15,016
Defense	Cybersecurity Specialist	8,221	7,313	7,218
GRC	Cyber Risk Analyst	8,187	8,787	9,991
Response	Incident Responder	7,639	6,812	9,577
Offense	Application Security Engineer	7,621	8,403	10,121
GRC	Governance Risk and Compliance Analyst	7,602	6,799	10,095
Defense	Cloud Security Engineer	7,259	8,428	12,768
Defense	Cyber Threat Intelligence Analyst	5,928	5,189	8,048
Offense	Penetration Tester	5,808	5,865	5,985
Management	Cybersecurity Lead	5,611	6,743	8,696
Education	Cybersecurity Technical Writer	4,907	5,003	4,110
Management	Cybersecurity Director	4,719	4,498	5,720
Sales	Cybersecurity Sales Engineer	4,689	3,715	7,431
Product Security	Cybersecurity Software Engineer	4,680	7,593	6,719
Defense	Cybersecurity Administrator	4,525	4,862	4,610
Product Security	Product Security Engineer	4,462	3,981	9,373
Management	Chief Information Security Officer (CISO)	4,067	4,466	3,635
Offense	Red Teamer	3,391	2,625	3,751
Response	Reverse Engineer / Malware Analyst	3,349	3,140	2,675

January 2022 – December 2024

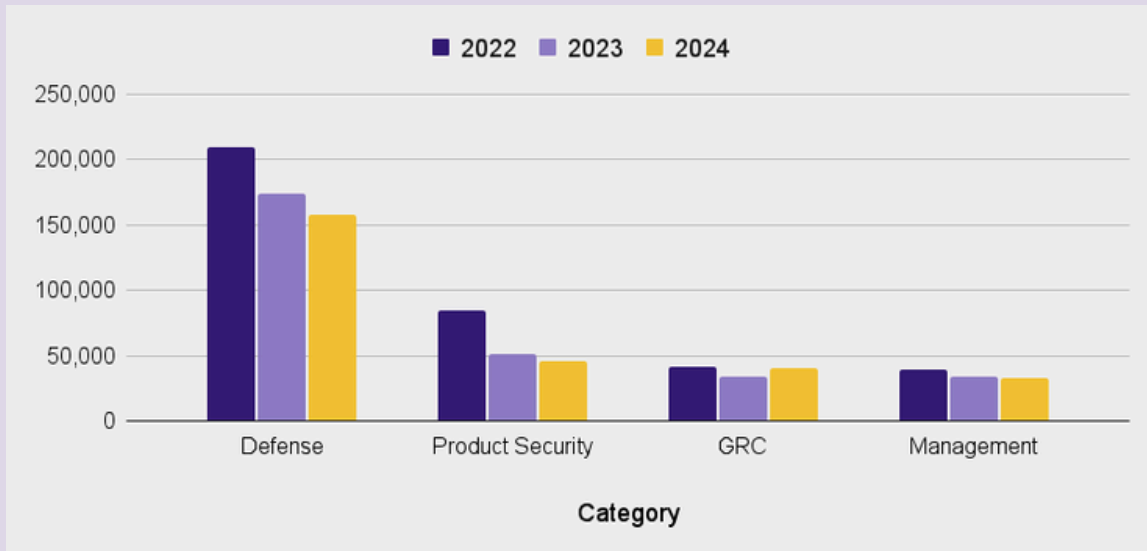
Source: CyberSN, 2025

Please Note: Starting July 2023 data accumulation changed from 45 days to 30 days job posting life cycle.



Key Takeaways

Top 4 Categories with the Most Job Postings for the Past 3 Years:



Note: For 3 years in a row, Defense, Product Security, GRC, and Management remain in the top 4 categories. **GRC** is the only top 4 category that has increased from 2023 to 2024.

Top 4 Functional Roles with the Most Job Postings

2022

- 1 Security Engineer
- 2 DevSecOps
- 3 Security Analyst
- 4 Security Architect

2023

- 1 Security Engineer
- 2 Security Analyst
- 3 DevSecOps
- 4 Security Architect

2024

- 1 Security Engineer
- 2 Security Analyst
- 3 DevSecOps
- 4 Cybersecurity / Privacy Attorney

The **Cybersecurity / Privacy Attorney** role is gaining significant traction, experiencing the largest increase among all functional roles, with a 40% rise from 2023 to 2024 and a 19% increase from 2022 to 2024.

Security Engineer, Security Analyst, and DevSecOps remain in the top 3 functional roles with the most job postings, despite a consistent decline in job postings over the past 3 years.



Increase in Functional Role Job Postings

2022 to 2024

1. Reverse Engineer / Malware Analyst ▲ 25.20%
2. Cybersecurity / Privacy Attorney ▲ 19.84%
3. Cybersecurity Technical Writer ▲ 19.39%
4. Cybersecurity Specialist ▲ 13.90%
5. Chief Information Security Officer (CISO) ▲ 11.88%

2023 to 2024

1. Cybersecurity / Privacy Attorney ▲ 40.74%
2. Red Teamer ▲ 29.18%
3. Cybersecurity Sales Engineer ▲ 26.22%
4. Cyber Threat Intelligence Analyst ▲ 14.24%
5. Cybersecurity Specialist ▲ 12.42%

Cybersecurity / Privacy Attorney and **Cyber Specialist** both had consistently high increases in job postings throughout the past 3 years.

Decrease in Functional Role Job Postings

2022 to 2024

1. Product Security Engineer ▼ -52.40%
2. DevSecOps ▼ -47.49%
3. Cloud Security Engineer ▼ -43.15%
4. Cybersecurity Sales Engineer ▼ -36.90%
5. Cybersecurity Lead ▼ -35.48%

2023 to 2024

1. Cybersecurity Software Engineer ▼ -38.36%
2. Identity And Access Management Engineer ▼ -26.54%
3. Cybersecurity Lead ▼ -16.79%
4. Cloud Security Engineer ▼ -13.87%
5. Security Analyst ▼ -13.47%

Cloud Security Engineer and **Cybersecurity Lead** have seen a steady decline in job postings over the past three years. While **Product Security Engineer** and **DevSecOps** also declined from 2022 to 2024, their growth from 2023 to 2024 indicates a positive shift.

Insights from Leadership

“ It's exciting to see job postings **increase for 10 of the top 25 functional cybersecurity roles over the past year**, though it is not surprising. Organizations can only pause forward motion for so long. Notably, Cybersecurity/Privacy Attorney job postings saw a 40% increase from 2023 to 2024, reflecting the growing complexity of the industry.

As this complexity continues to evolve, our Cyber Workforce Risk Management Practice is seeing organizations prioritize talent retention, development, and the need to address workforce gaps. Without this focus, the decline in cyber job postings and the increase in outsourcing over the past two years, both near and offshore, will inevitably lead to operational failures.

Our protectors need protection. Join us in this conversation.

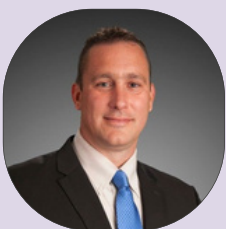


Deidre Diamond

Founder & CEO, CyberSN
Founder, Secure Diversity
Co-Founder, Day of Shecurity Conference
Board Member, Cyversity

“ Regulatory pressures on CEOs and Boards of Directors are reflected in our cybersecurity job posting data, highlighting how compliance-driven requirements such as the SEC breach reporting and expanded FTC enforcements are shaping workforce decisions.

Additionally, decreases in Security Engineer, Security Analyst, and DevSecOps job postings are **signaling an industry-wide shift toward AI-powered security automation** and internal security operations optimizations.



Dom Glavach

Chief Security & Technology Officer, CyberSN

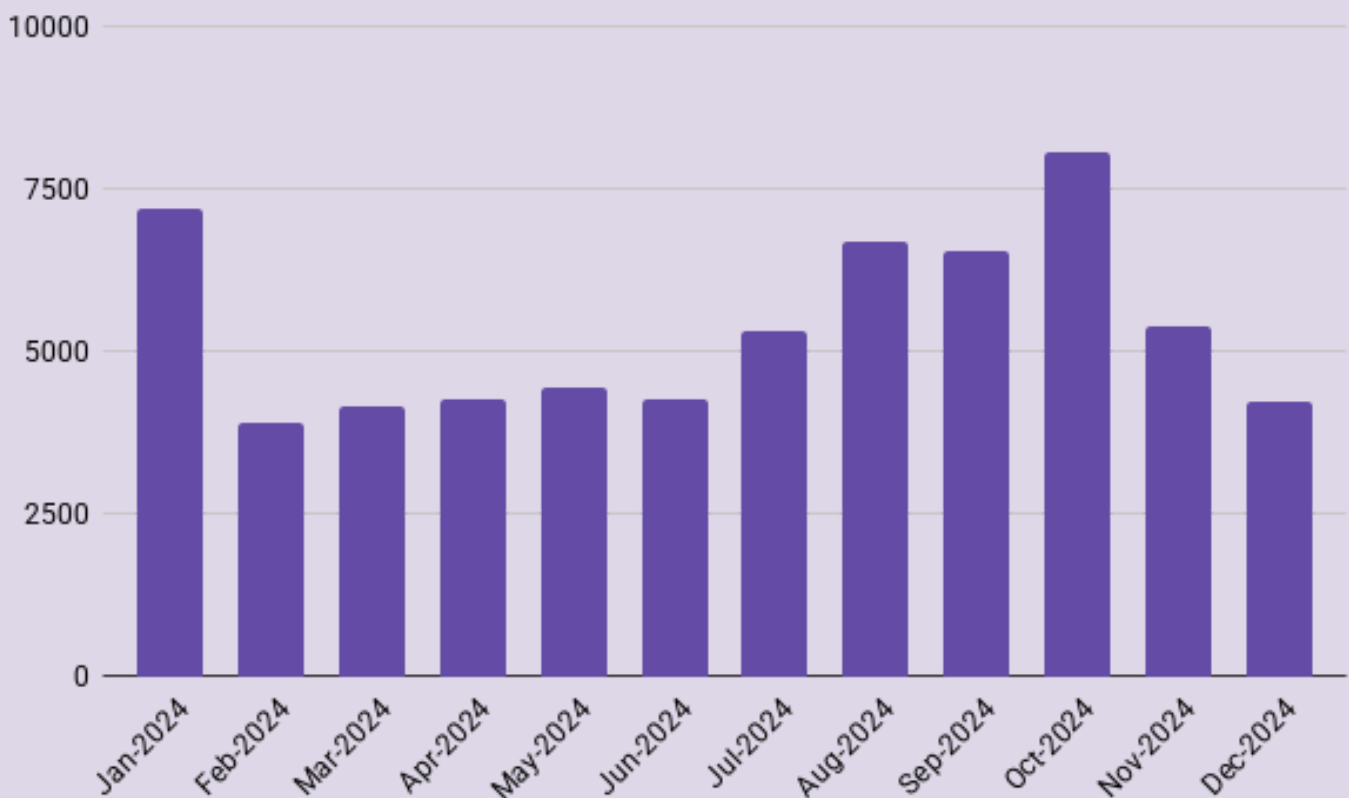


SECURITY ENGINEER

64,300 posted jobs

Security Engineers develop and maintain the systems that keep sensitive data safe from breaches and leaks. These professionals play a pivotal role in protecting an organization's data, reputation, and finances by working with penetration testers, security analysts, and technology managers to secure data, as well as installing firewalls and other breach detection systems.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy **Defense**

NICE **Securely Provision (SP)**

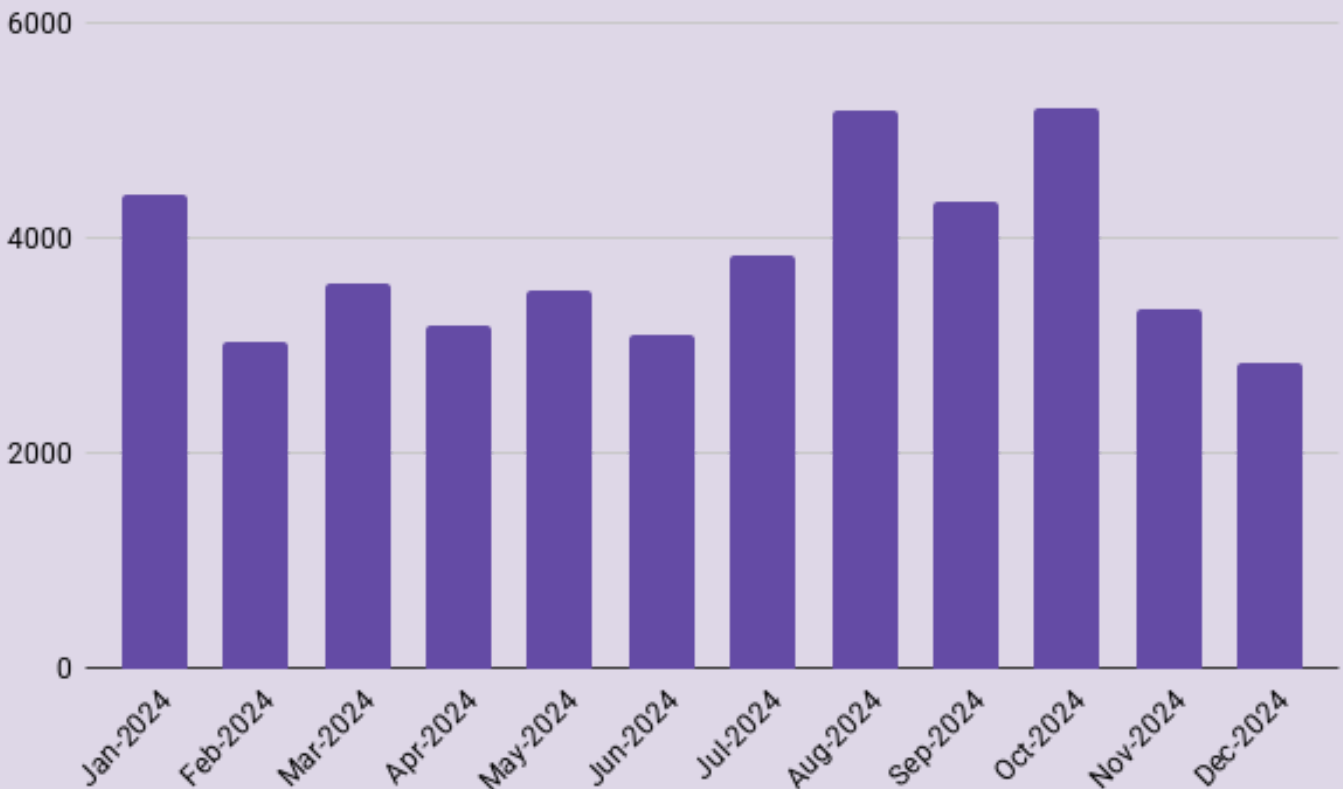
Operate and Maintain (OM)

SECURITY ANALYST

45,496 posted jobs

Security Analysts are responsible for enhancing their organization's cybersecurity posture by monitoring and responding to threats, implementing or enhancing security solutions such as firewalls, endpoint security, and security event monitoring.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy

Defense

NICE

Operate and Maintain (OM)

Protect and Defend (PR)

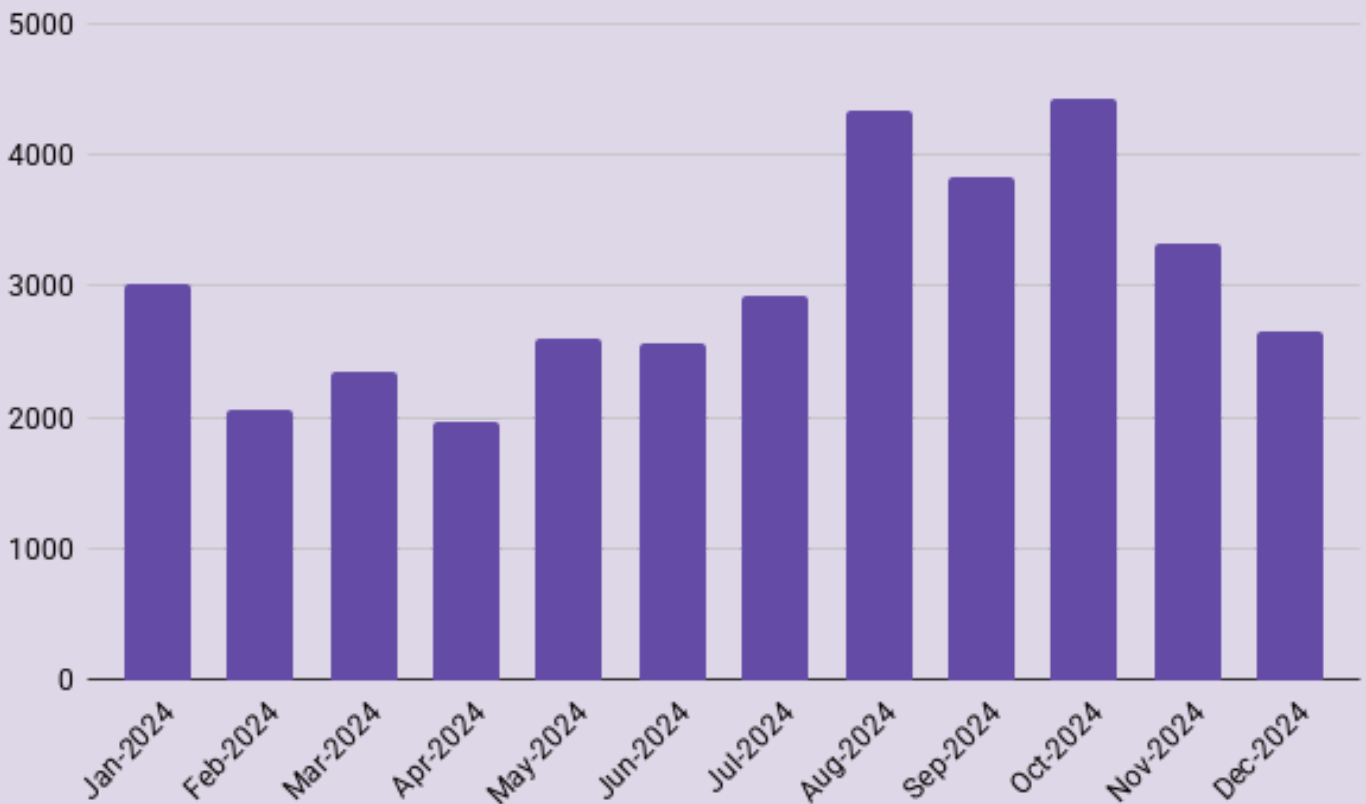


DEVSECOPS

36,020 posted jobs

DevSecOps (Development, Security, and Operations) professionals use a combination of programming knowledge, threat management, and communication skills to automate and integrate cybersecurity at every stage of the SDLC lifecycle.

January 2024 - December 2024 Source: CyberSN, 2025

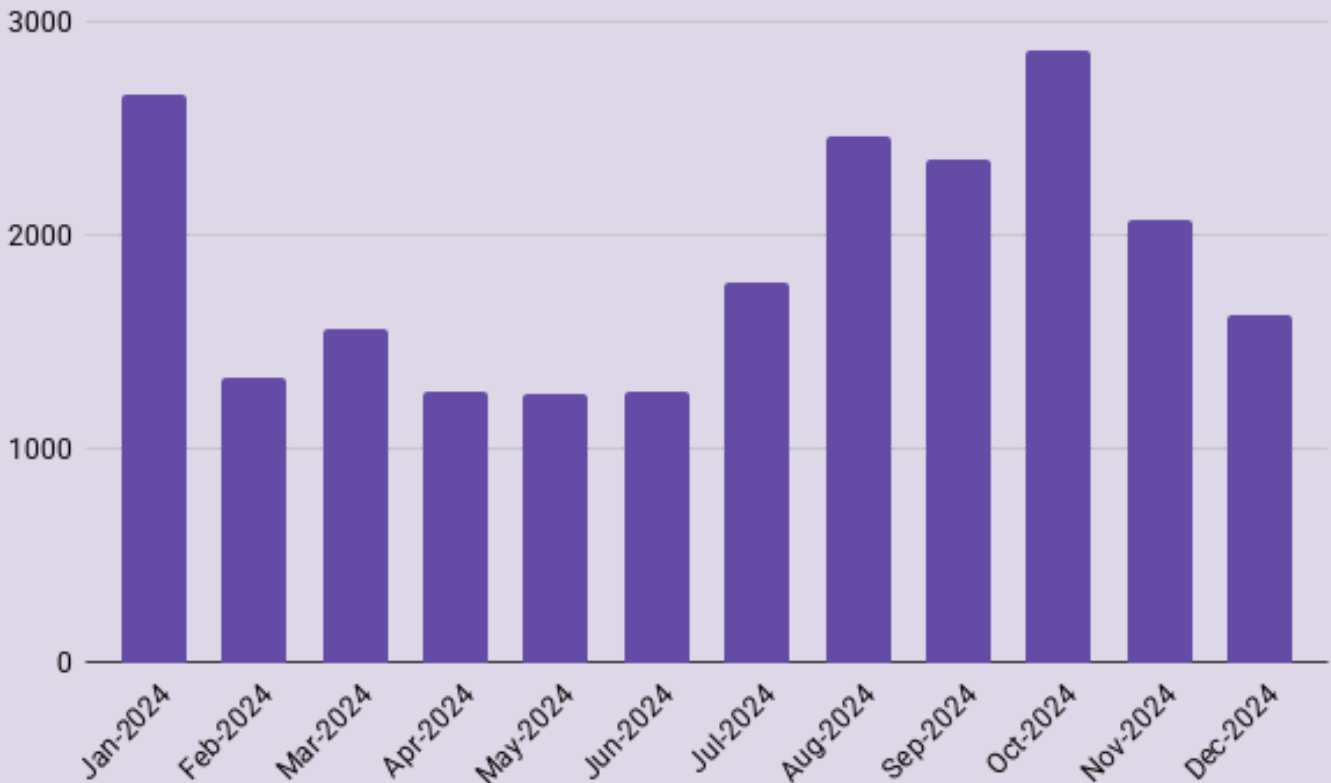


CYBERSECURITY/PRIVACY ATTORNEY

22,465 posted jobs

Cybersecurity/Privacy Attorneys advise on implementing the right processes to meet state, federal and international legal requirements relevant to personal data. They also represent clients before regulatory bodies and help prepare the right responses and reactions during incident response to mitigate loss and ensure legal compliance.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy

GRC

NICE

Oversee and Govern (OV)

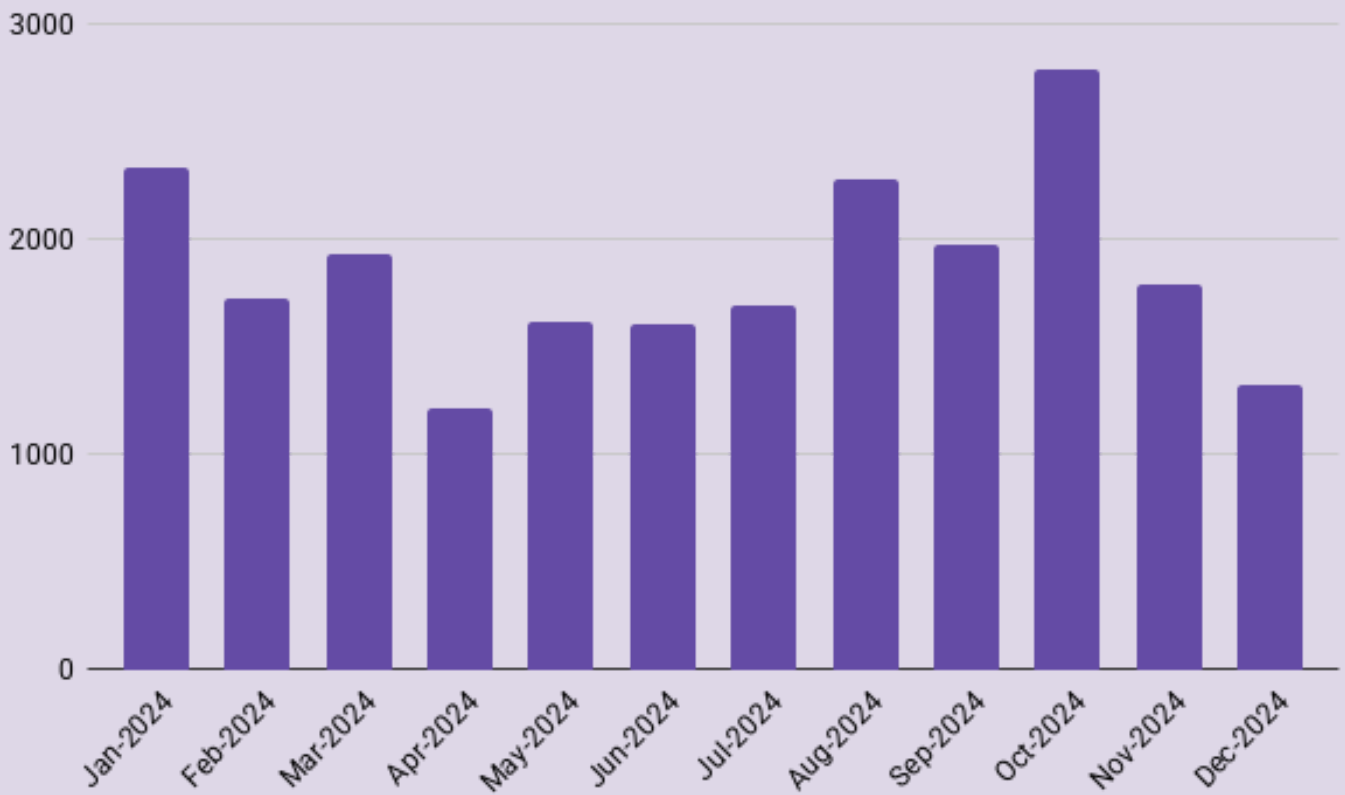


SECURITY ARCHITECT

22,246 posted jobs

Security Architects combine extensive hardware and software knowledge with policy development to anticipate cyber threats and design the systems that detect and prevent them. When new networks are developed, a security architect is needed to oversee the network build and ensure that the best defensive measures are implemented from day one.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy **Planning**

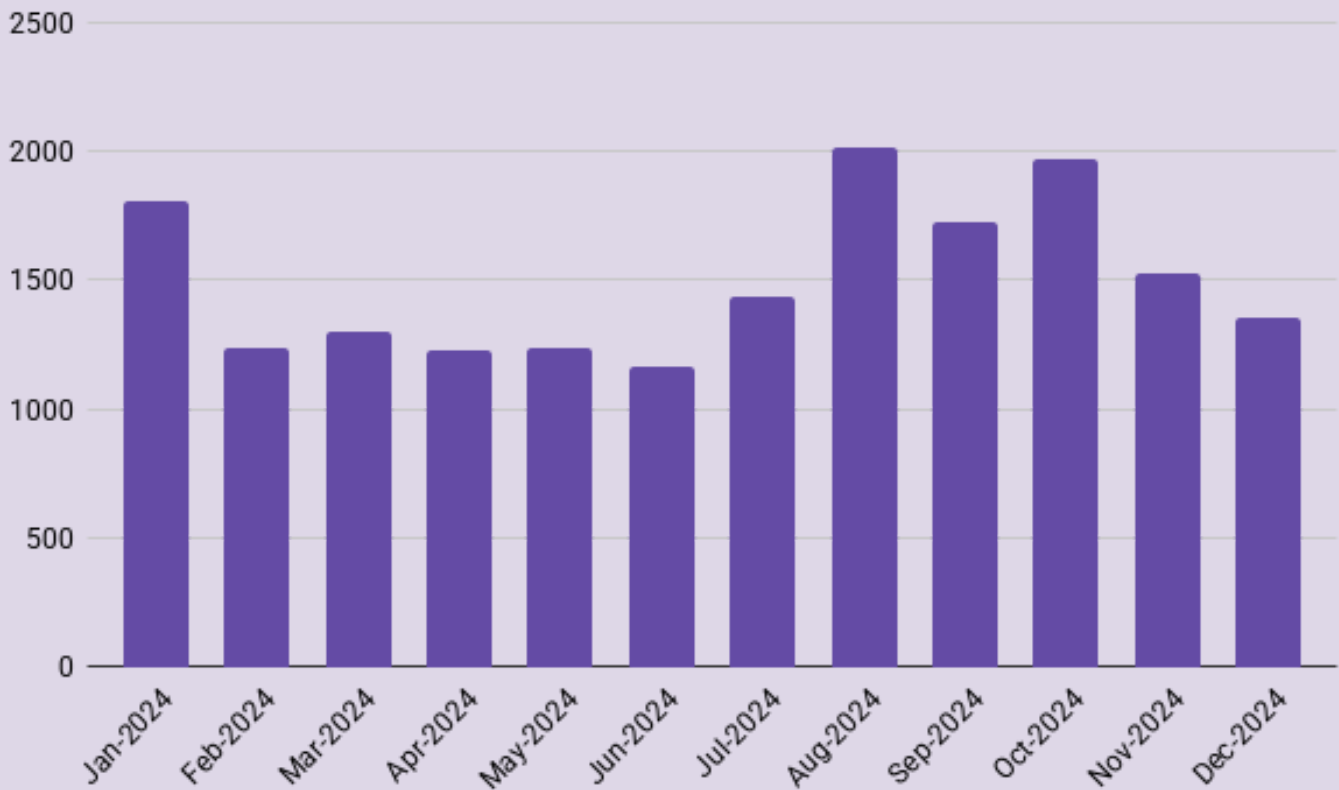
NICE **Securely Provision (SP)**

CYBERSECURITY MANAGER

17,975 posted jobs

Cybersecurity Managers manage a variety of projects within their organization, facilitating the planning and prioritization of complex cybersecurity services. These projects may be complex and span many offices, departments, and entities. The projects they manage may be short-term or long-term and could include significant business and technology changes.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy

Planning

NICE

Oversee and Govern (OV)

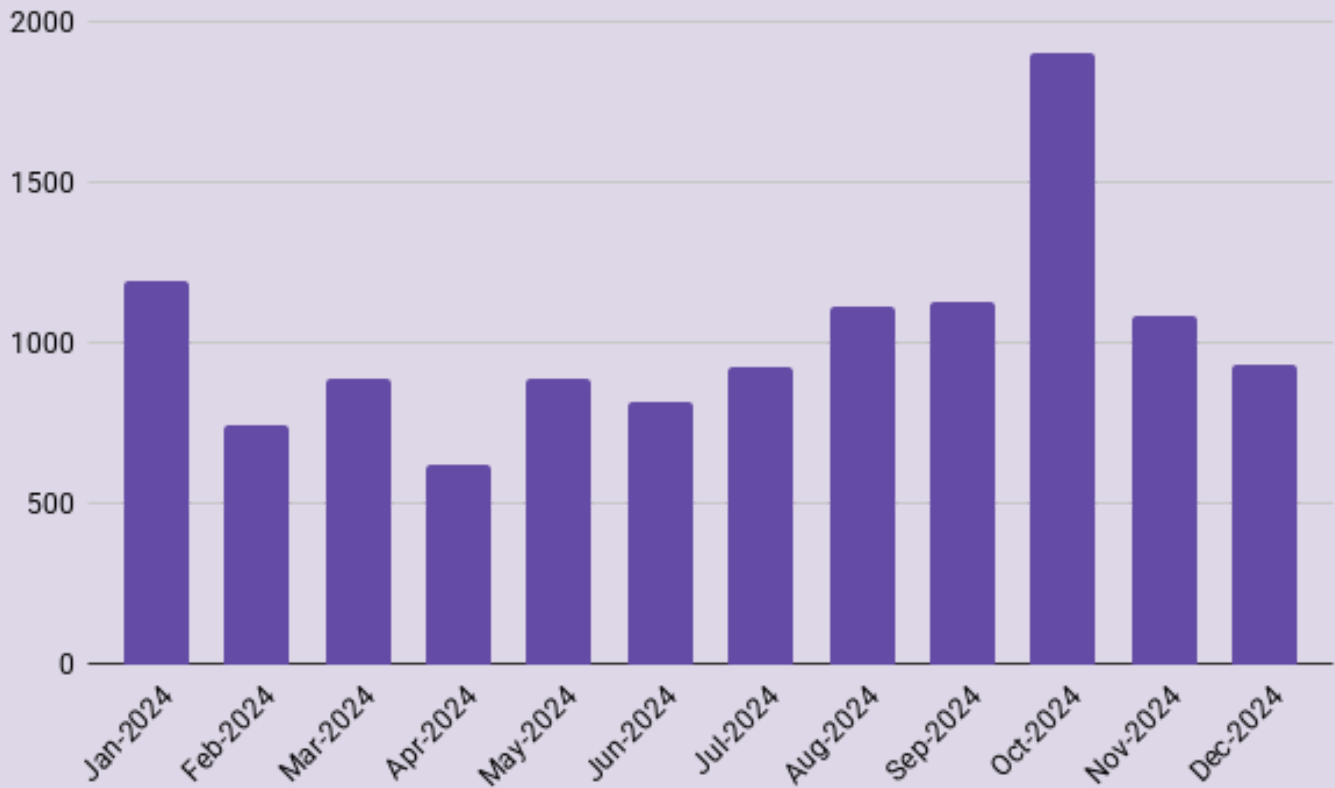


IDENTITY AND ACCESS MANAGEMENT (IAM) ENGINEER

12,223 posted jobs

IAM Engineers implement and continuously optimize Identity and Access Management services in line with evolving technologies and security regulations. They are responsible for designing, implementing, and maintaining IAM technologies to ensure audit and privacy compliance, driving automation wherever possible. IAM Engineers also assist with resolving any security issues related to IAM operations.

January 2024 - December 2024 Source: CyberSN, 2025

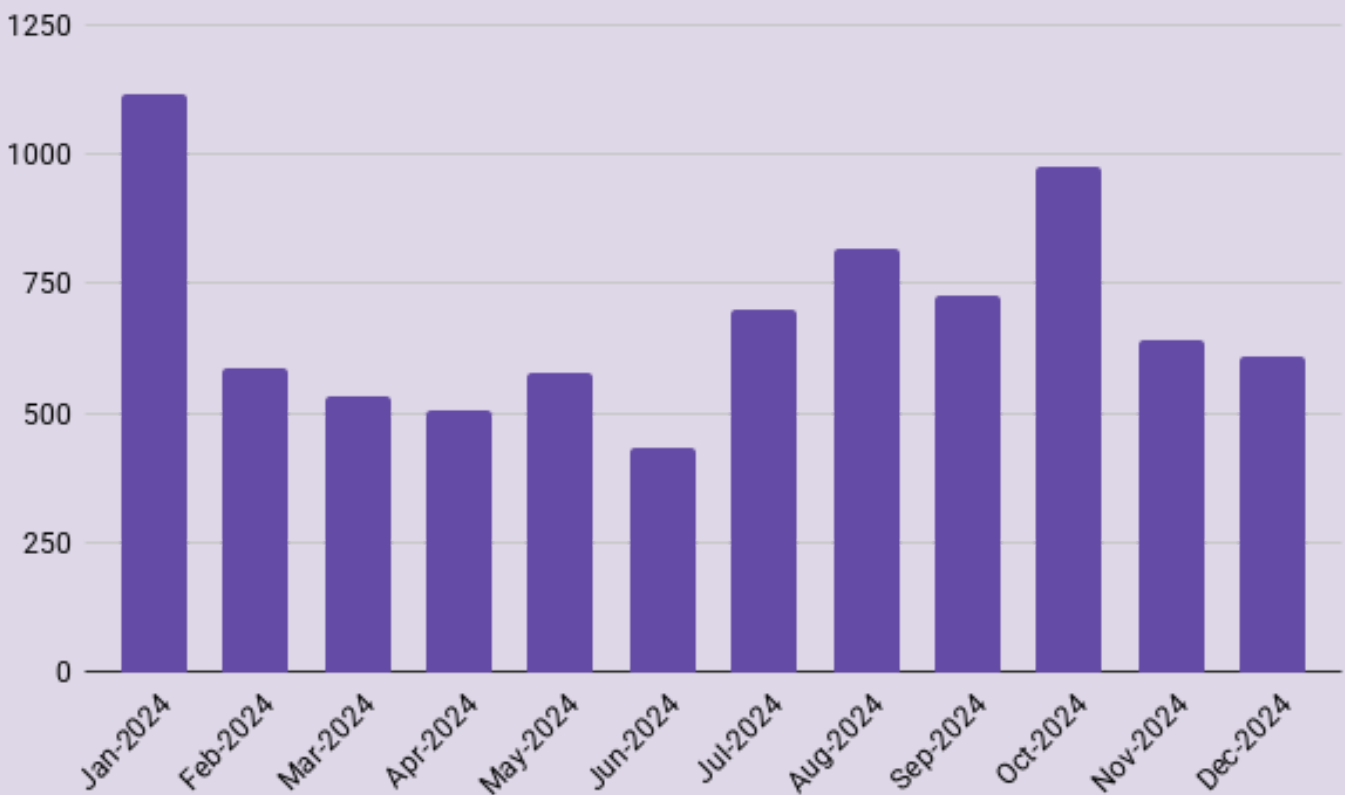


CYBERSECURITY SPECIALIST

8,221 posted jobs

Cybersecurity Specialists take charge of their organization's cybersecurity, or an aspect of cybersecurity, improving existing infrastructure, suggesting improvements, and staying current on new threats and solutions. By taking responsibility for their organization's cybersecurity, Security Specialists secure company data and protect against cyberattacks and the subsequent reputational damage.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy

Defense

NICE

Operate and Maintain (OM)

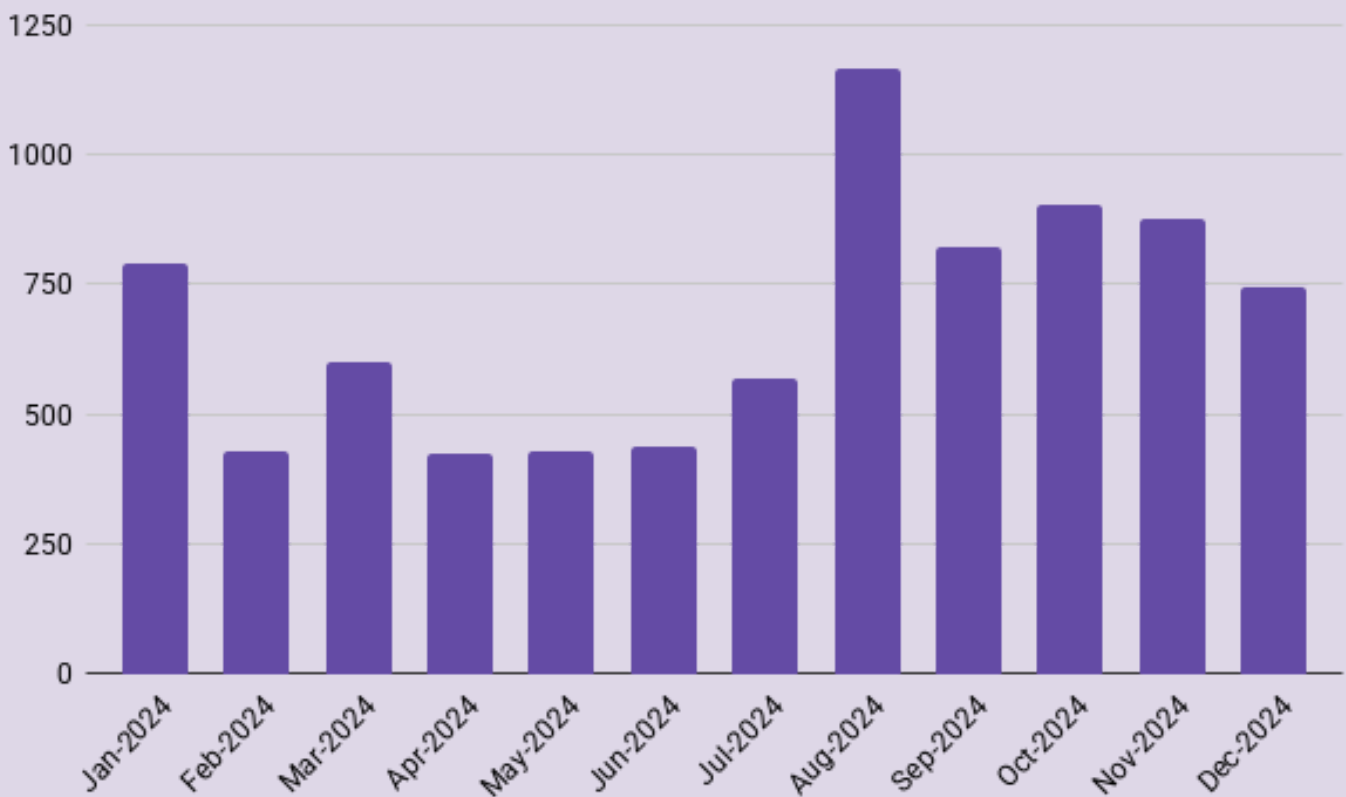


CYBER RISK ANALYST

8,187 posted jobs

Cyber Risk Analysts support the analysis, classification, and response to cybersecurity risks within an organization. This professional addresses cybersecurity risk and analyses the potential business and customer risk, aligning processes and controls to the relevant frameworks and internal systems. The Cyber Risk Analyst is able to identify areas of concern for their specific organization, supporting resolution and mitigation by providing advice and recommendations.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy

GRC

NICE

Securely Provision (SP)

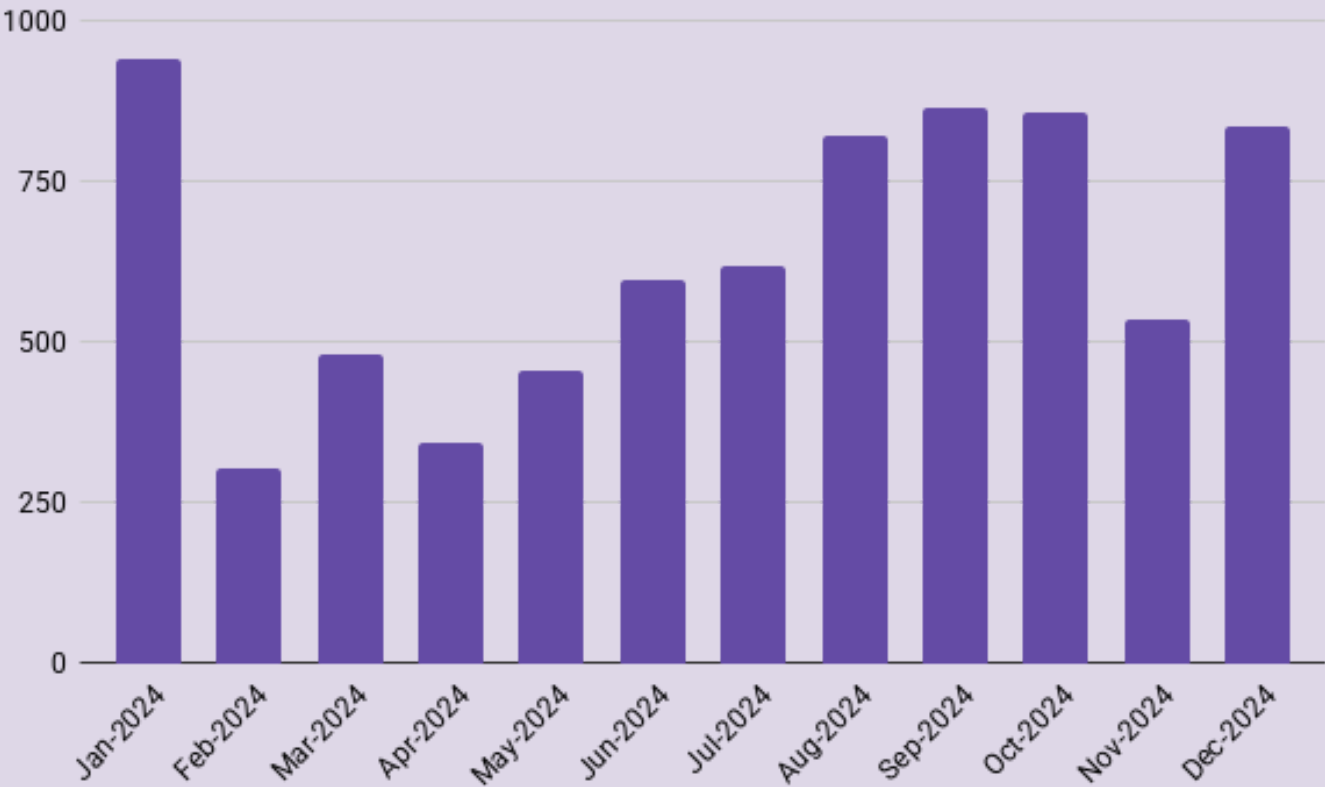


INCIDENT RESPONDER

7,639 posted jobs

Incident Responders protect and improve an organization’s security by addressing and managing the activities to recover from a cybersecurity event. The Incident Responder makes an assessment on threat severity, conducts investigations, and works to contain, eradicate, and recover from threats.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy **Response**

NICE **Protect and Defend (PR)**

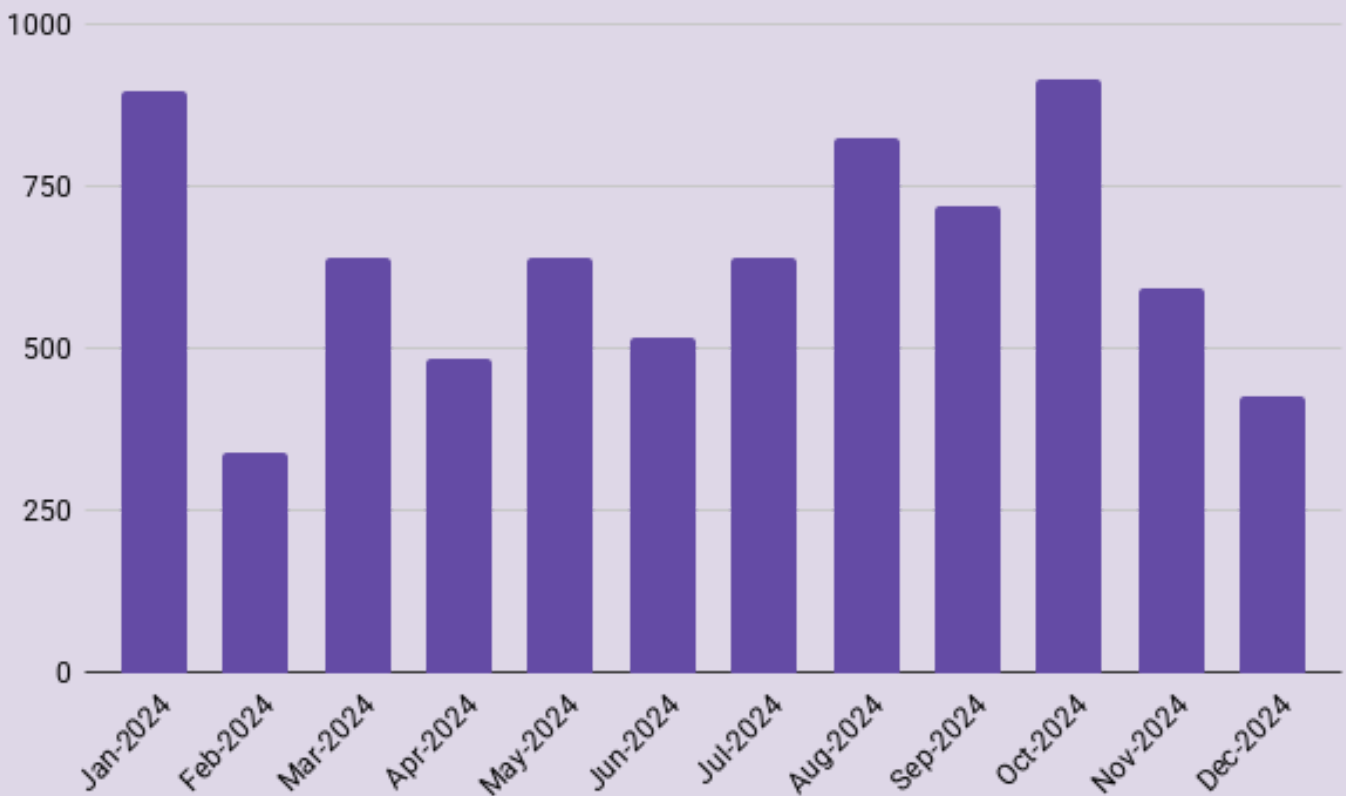
INVESTIGATE (IN)

APPLICATION SECURITY ENGINEER

7,621 posted jobs

Application Security Engineer develops and tests security components that make an application more secure. They proactively test their security posture from an attacker’s perspective, help shape engineering best practices, improve and drive application security monitoring, and work with the security team to educate engineers on emerging threats.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy **Defense**

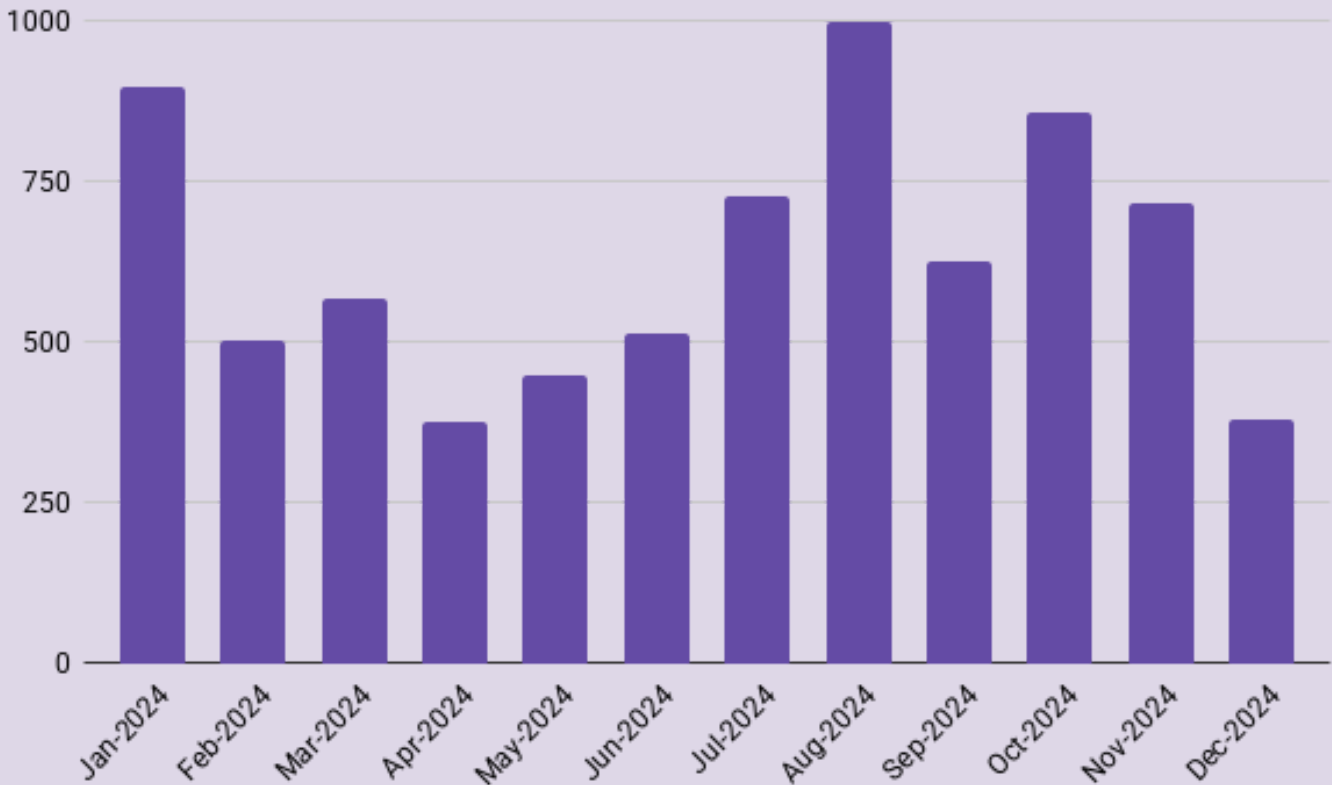
NICE **Securely Provision (SP)**

GOVERNANCE RISK AND COMPLIANCE ANALYST

7,602 posted jobs

Governance Risk and Compliance Analysts ensure that an organization's operations and procedures meet government and industry compliance standards. They research regulations and policies on behalf of the enterprise, communicate the necessary requirements, apply for certifications, and serve as a subject matter expert on all compliance-related matters.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy

GRC

NICE

Oversee and Govern (OV)

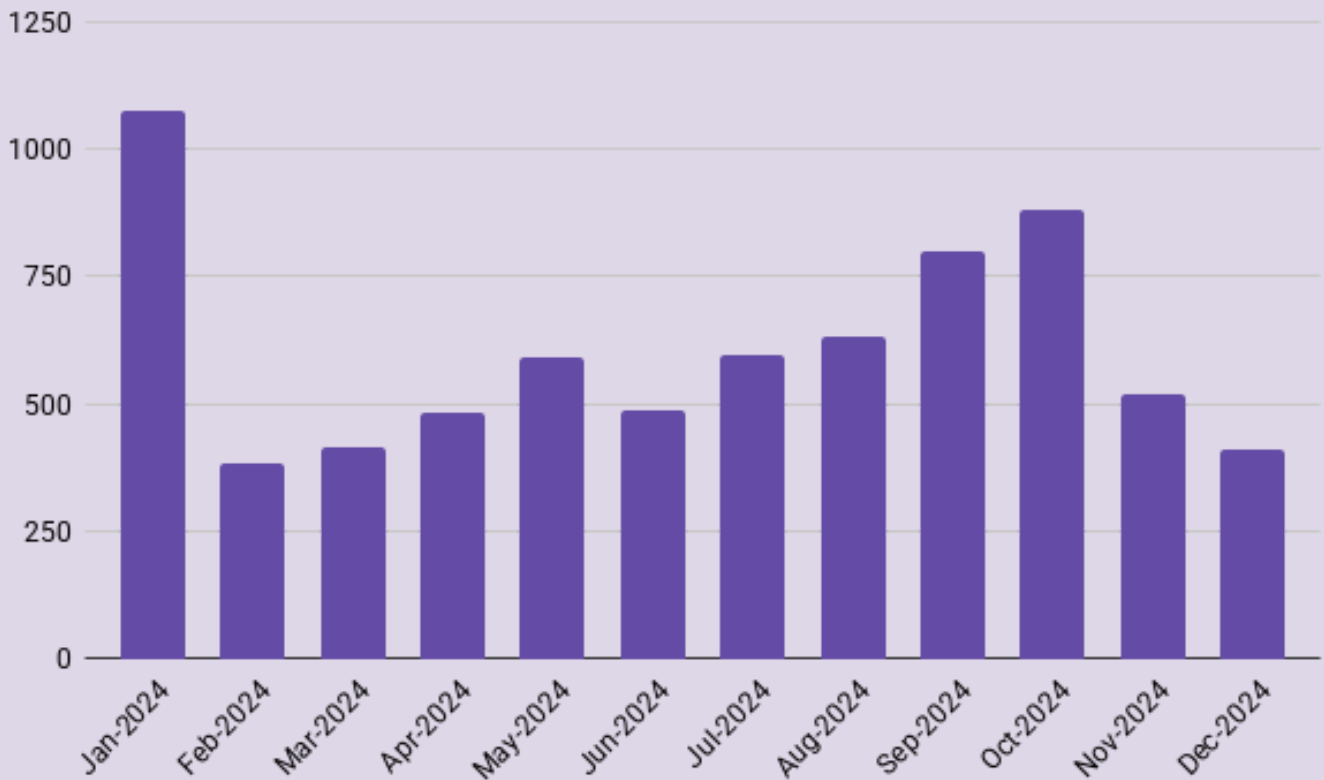


CLOUD SECURITY ENGINEER

7,259 posted jobs

Cloud Security Engineers are responsible for the secure operations of cloud infrastructure, platforms, and software, including the installation, maintenance, and improvement of cloud computing environments. They also help develop new designs and security strategies across cloud-based applications, including infrastructure, platform, and SaaS.

January 2024 - December 2024 Source: CyberSN, 2025

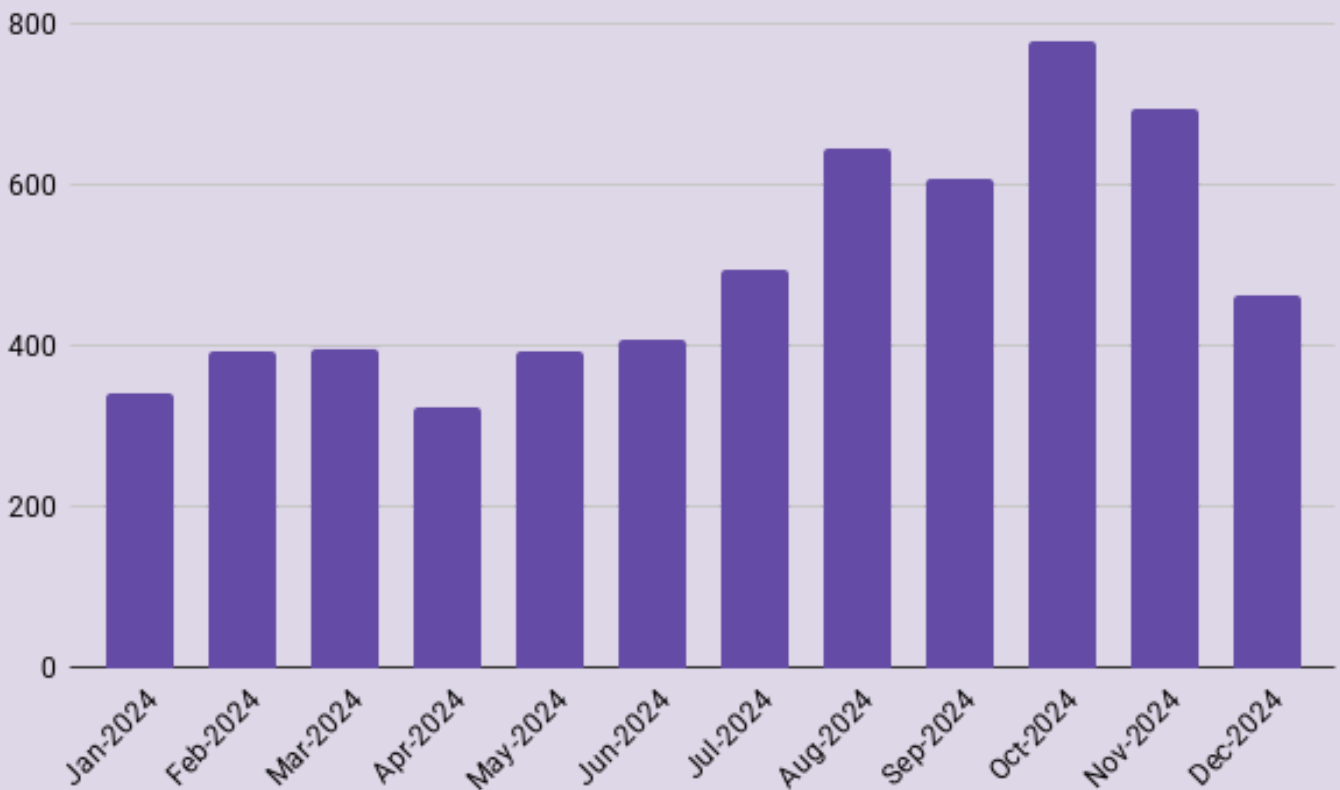


CYBER THREAT INTELLIGENCE ANALYST

5,928 posted jobs

Cyber Threat Intelligence Analysts use their expert knowledge of malicious software to research and analyze cyber threats, reporting their findings to business leaders, using this intelligence to predict similar attacks, and ultimately helping to counter the activities of cybercriminals for their organization.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy

Defense

NICE

Analyze (AN)

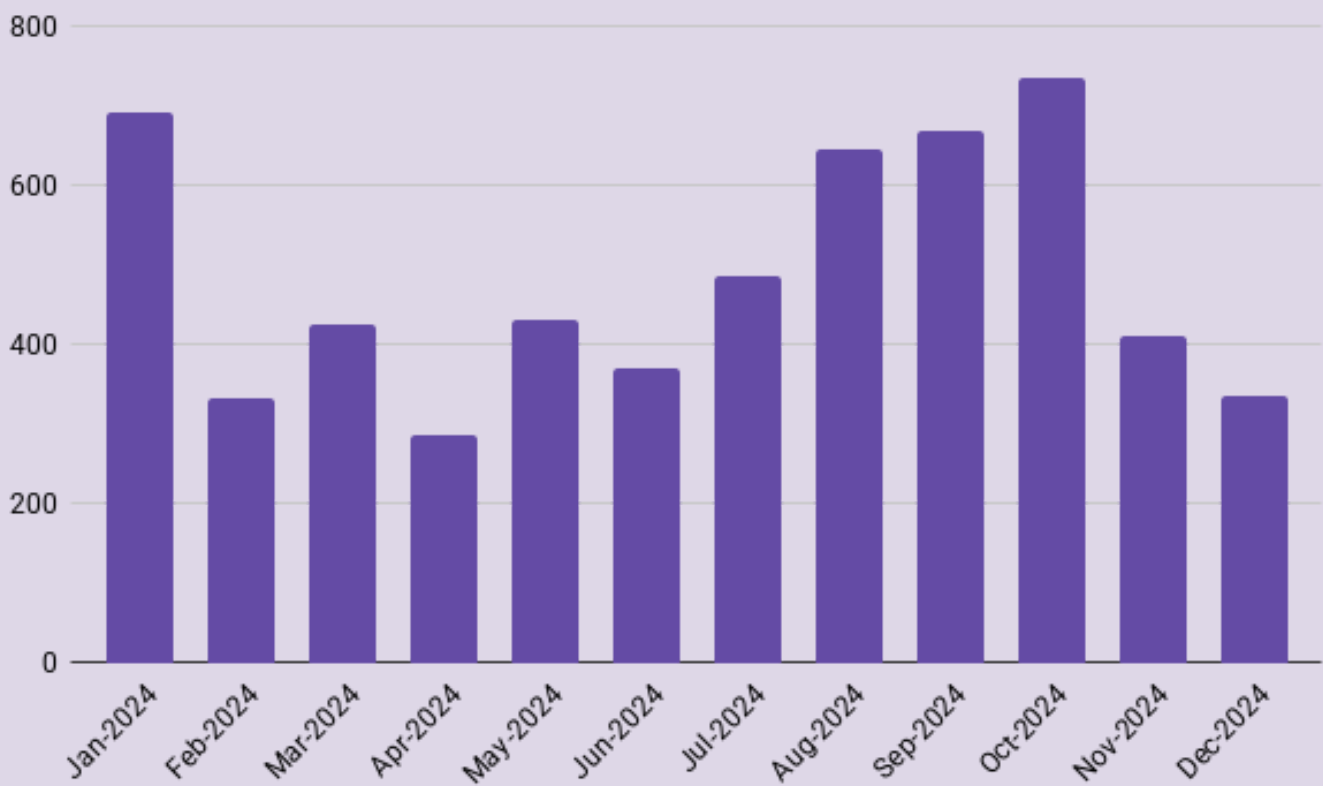


PENETRATION TESTER

5,808 posted jobs

Penetration Testers identify and attempt to breach weaknesses in an existing system to help organizations resolve security vulnerabilities and weaknesses. These systems include websites, data storage systems, and other IT assets. This testing simulates cyberattacks and other breaches designed to access valuable sensitive data. Pen Testers can then document their actions to generate detailed findings and remediation reports.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy **Offense**

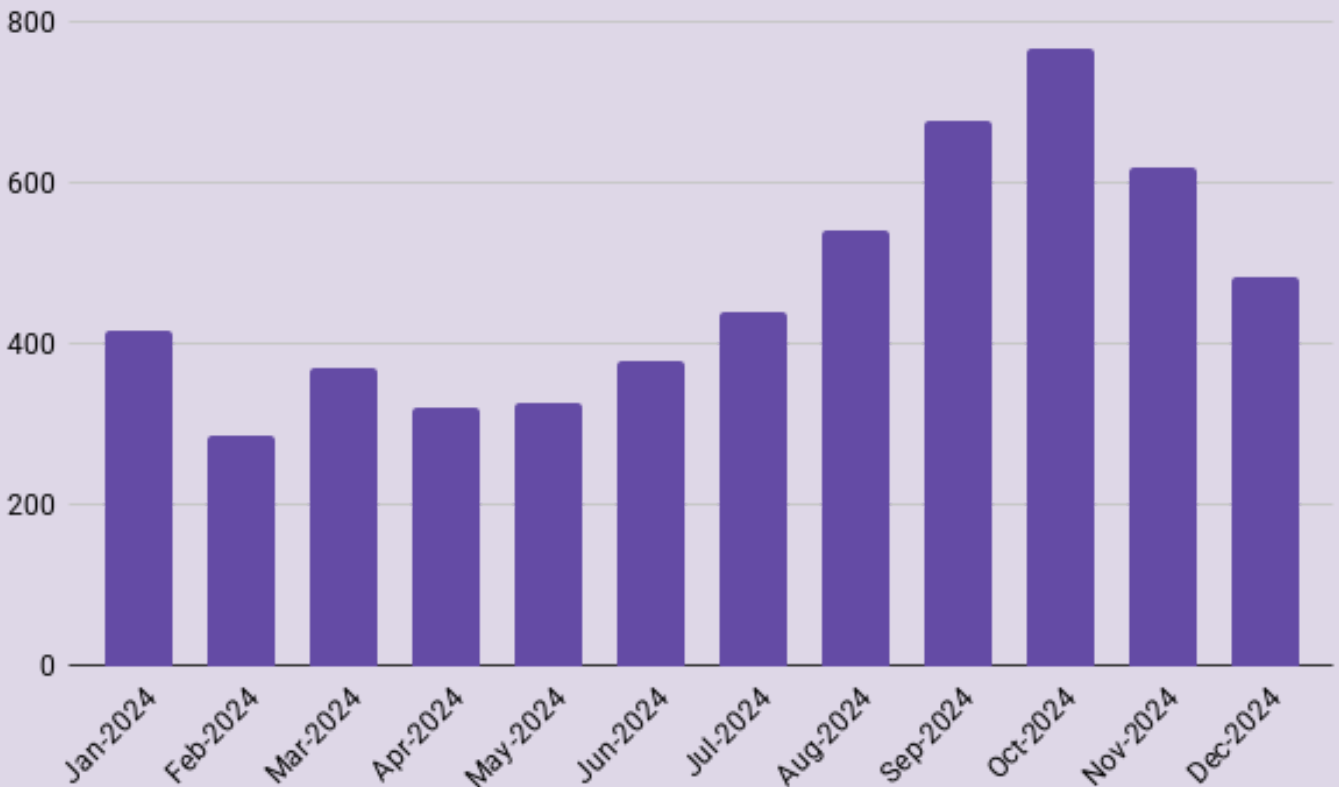
NICE **Securely Provision (SP)**

CYBERSECURITY LEAD

5,611 posted jobs

Cybersecurity Leads head up the cybersecurity team, or a specific department within the cybersecurity team, responsible for ensuring that teams are working towards the right goals efficiently. Cybersecurity Leads oversee the delivery of services, manage relationships, and take control of any issues in their department or specialism.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy **Management**

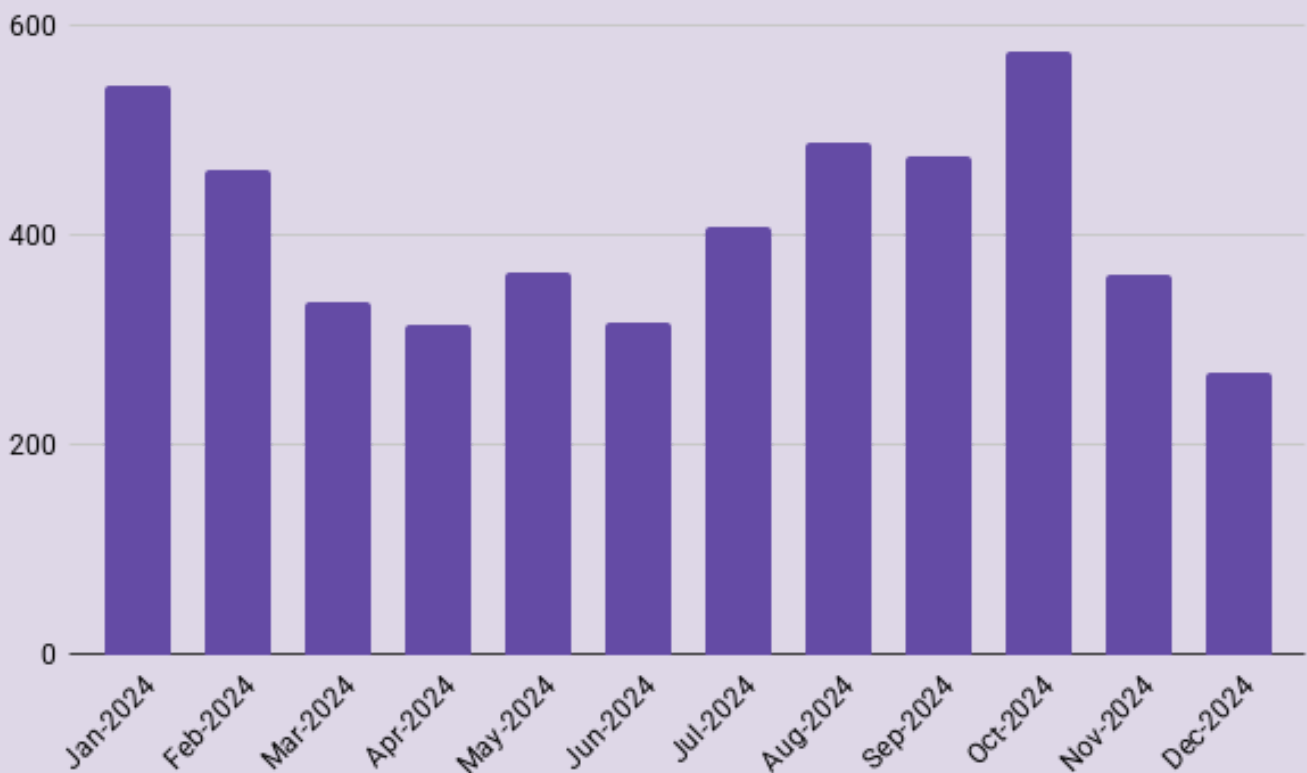
NICE **Oversee and Govern (OV)**

CYBERSECURITY TECHNICAL WRITER

4,907 posted jobs

Cybersecurity Technical Writers create and oversee cybersecurity content, whether it's composing reports, synthesizing data, creating manuals, or editing cybersecurity policies to resonate with the target audience. These professionals convert strategy into actionable steps or digestible copy, working with the organization's needs and cybersecurity goals in mind to plan and proofread technical documentation. Technical writers can successfully expound on a variety of topics so that other professionals can easily understand and further use the company documentation they write.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy

Education

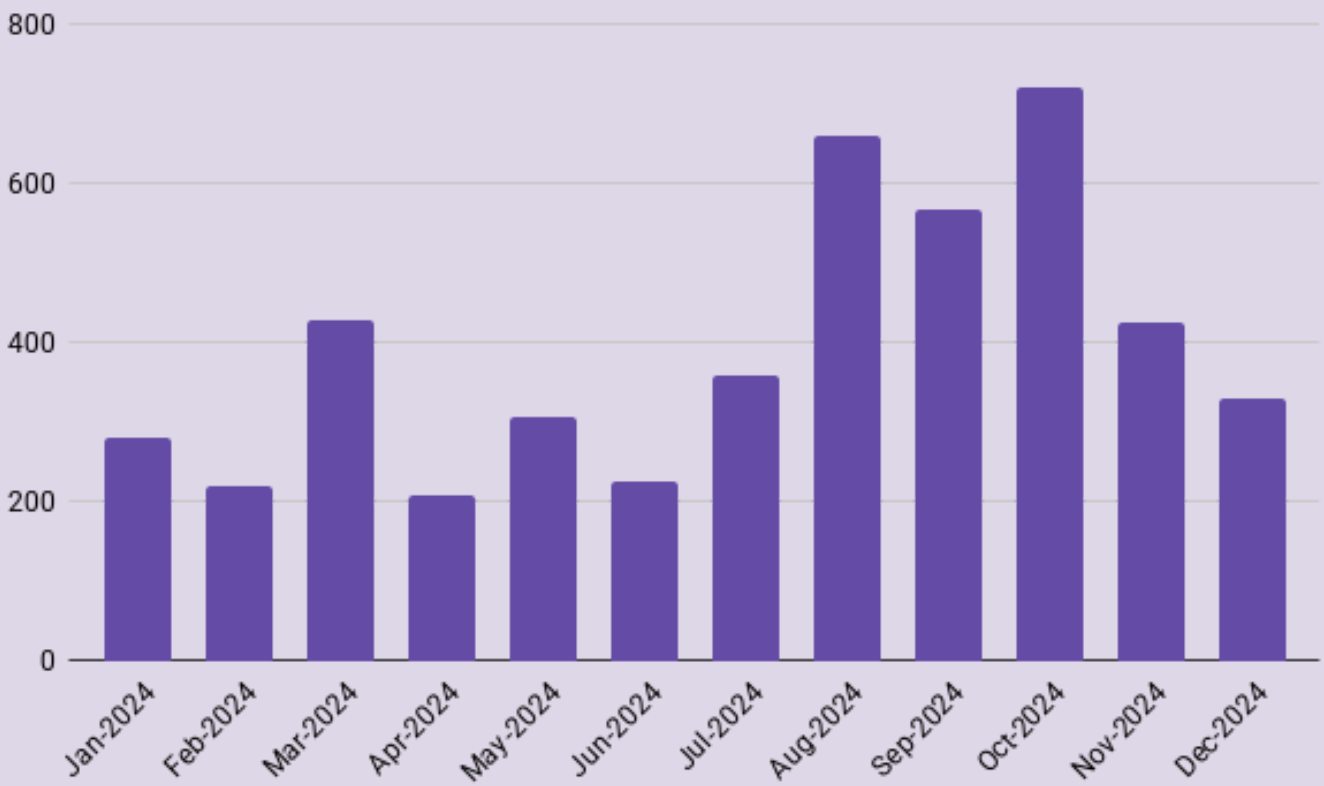


CYBERSECURITY DIRECTOR

4,719 posted jobs

Cybersecurity Directors are responsible for overseeing an organization’s overall cybersecurity. The role supervises aspects of IT security including design, development, implementation, incident response, budgets, and adherence to various regulations. The Cybersecurity Director contributes to overall cybersecurity strategy by identifying growth opportunities based on the latest threats, as well as managing security personnel and reporting on the company’s cybersecurity posture.

January 2024 - December 2024 Source: CyberSN, 2025



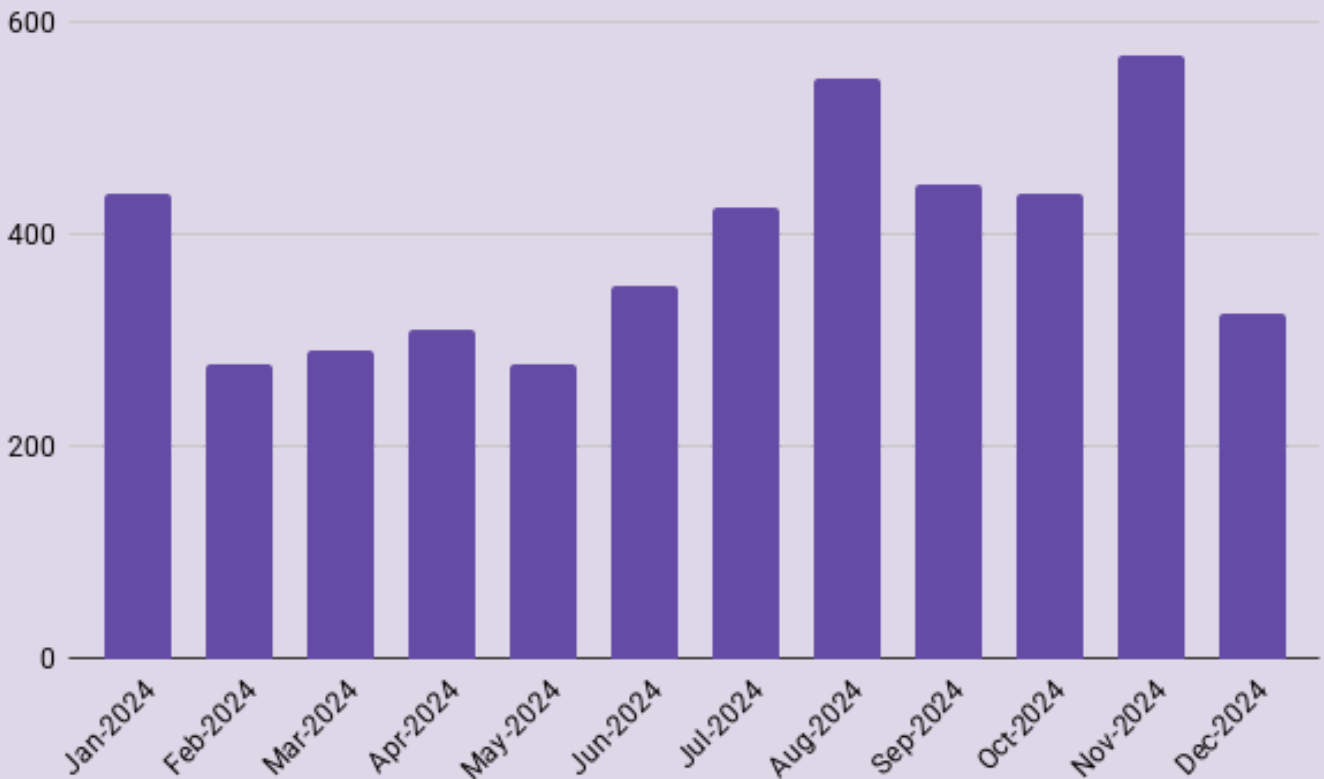
CyberSN Taxonomy **Management**

CYBERSECURITY SALES ENGINEER

4,689 posted jobs

Cybersecurity Sales Engineers actively drives and manages the technology evaluation stage of the sales process, working with the entire sales team to advise on all product sales. Sales Engineers unite technical knowledge and sales skills and are able to explain, in detail, the technical and functional aspects of a product or service, prepared for any technical questions or issues that may arise.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy

Sales

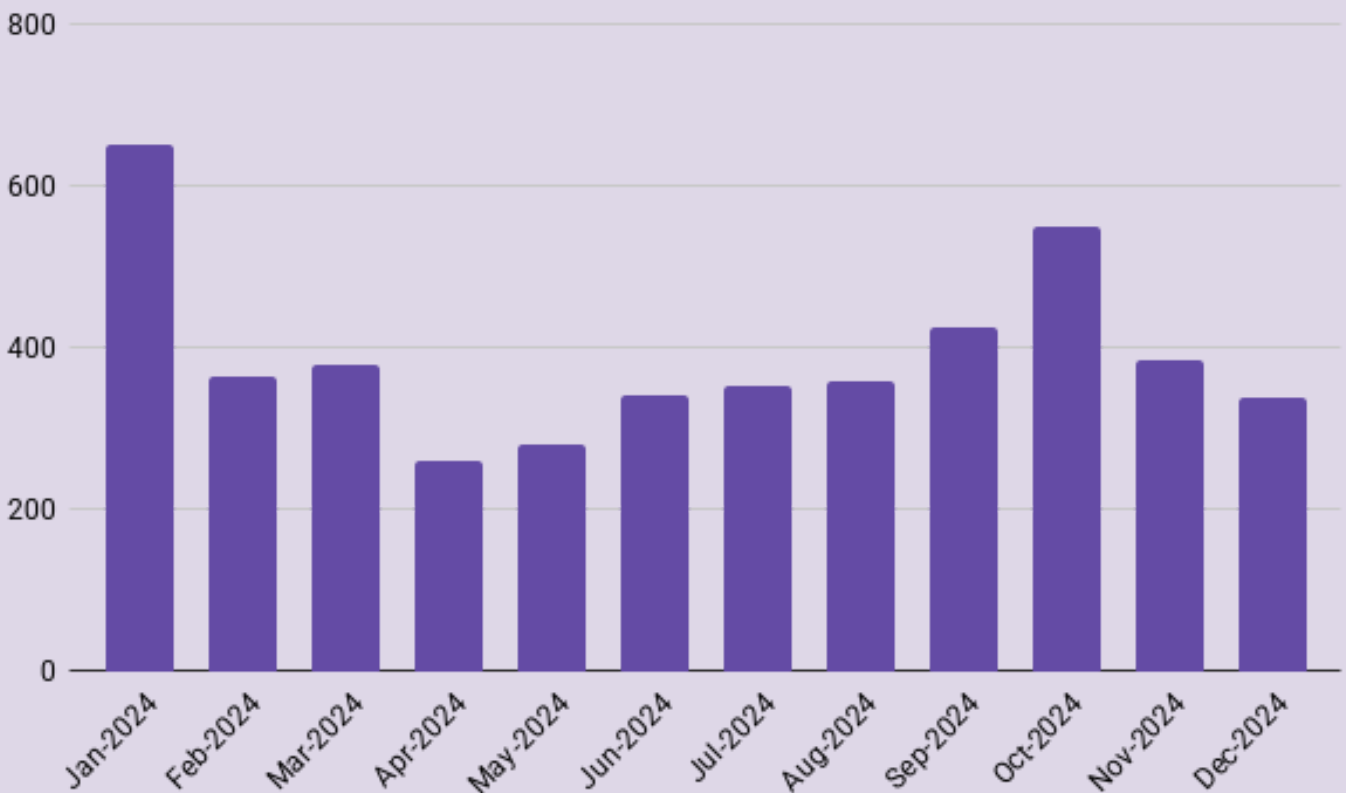


CYBERSECURITY SOFTWARE ENGINEER

4,680 posted jobs

Cybersecurity Software Engineers are a key part of the entire software program lifecycle. They participate in the design, development, testing, and implementation of technologies to best meet the organization’s cybersecurity needs and business goals. Software Engineers are primarily responsible for the safety and efficacy of software, continually carrying out upgrades and testing. They may work as part of a software development team with other cybersecurity professionals or build each part of an application or program independently.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy

Product Security

NICE

Securely Provision (SP)

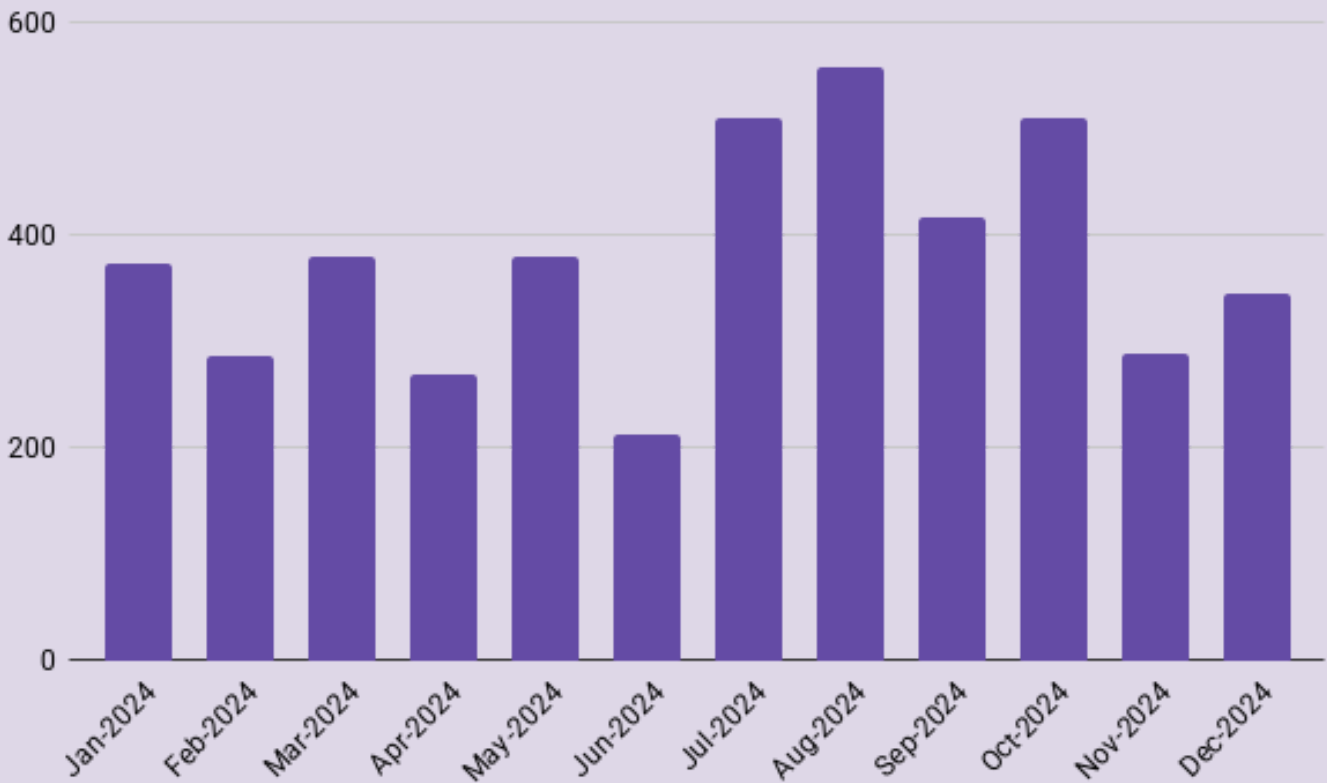


CYBERSECURITY ADMINISTRATOR

4,525 posted jobs

Cybersecurity Administrators typically work as part of a team to cover all the digital security needs of an organization. The role varies with the size and nature of the organization, but in general, Security Administrators ensure the safety of the organization's data. They are tasked with managing the safety of the business' systems, networks, applications, devices, hardware, and software.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy

Defense

NICE

Protect and Defend (PR)

Operate and Maintain (OM)

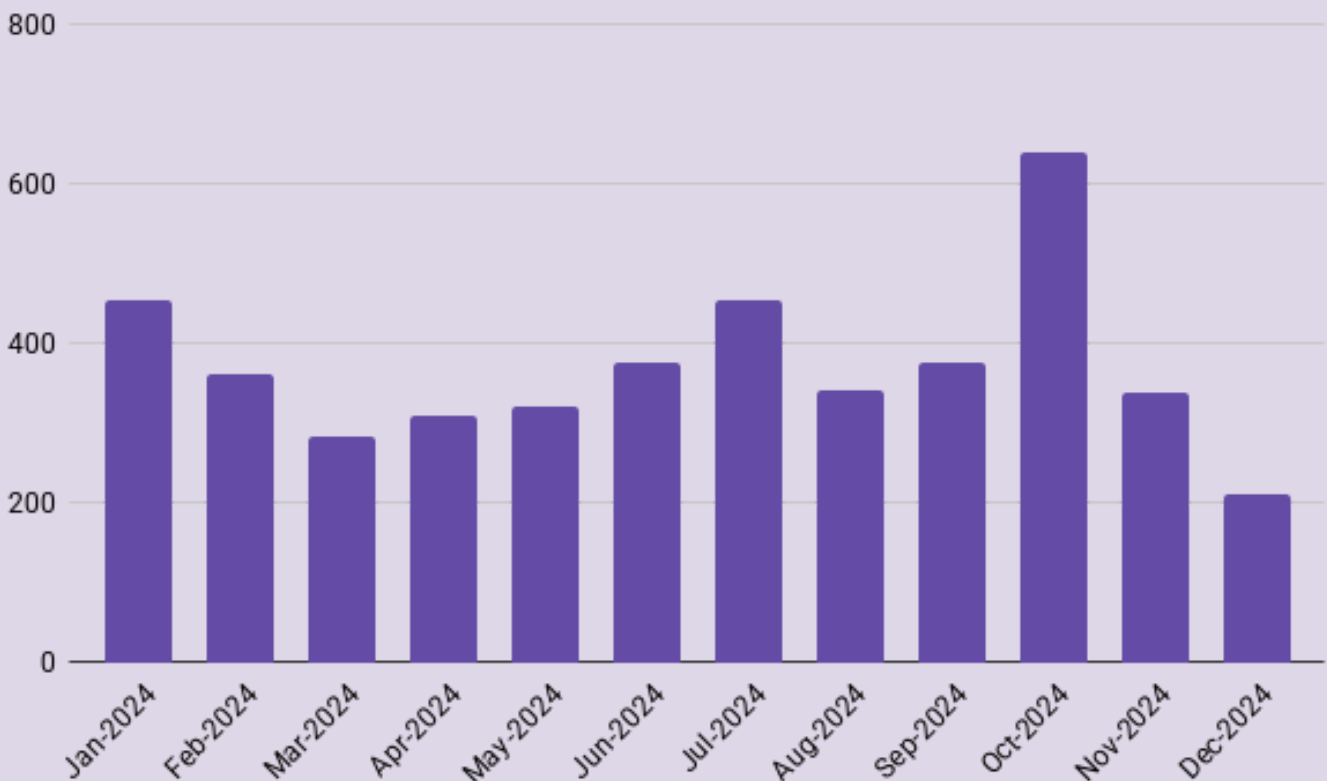


PRODUCT SECURITY ENGINEER

4,462 posted jobs

Product Security Engineers work closely with software engineering and product teams to achieve product and security business objectives. They support the implementation of secure development practices, threat modelling, architecture, design, vulnerability assessments and security verification, as well as defining the security standards for a variety of products and tools.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy

Product Security

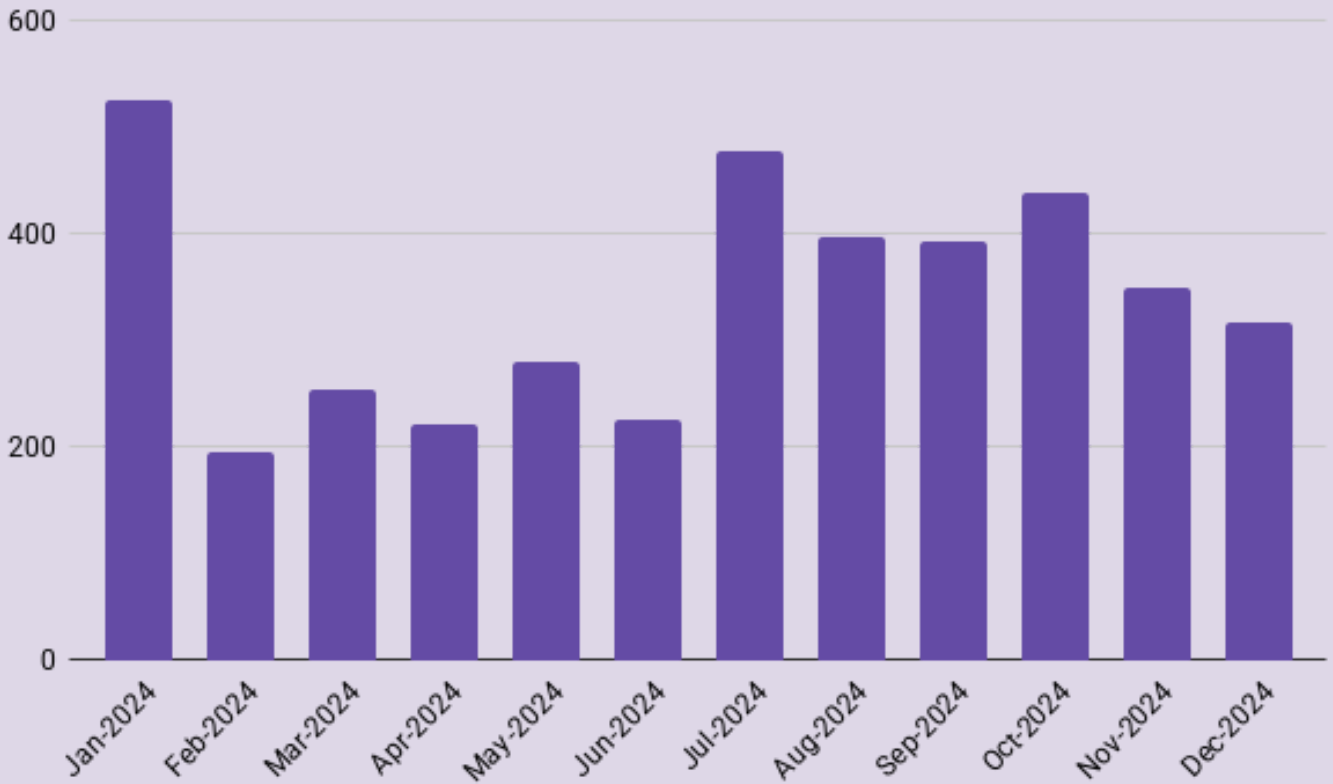


CHIEF INFORMATION SECURITY OFFICER (CISO)

4,067 posted jobs

CISOs develop information security policies and procedures for a business or organization. They manage teams of security analysts, information security specialists, and fellow executives to identify and manage security threats for the business. CISOs work in organizations across all sectors, carefully monitoring for security vulnerabilities and allocating resources to increase efficacy and efficiency.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy **Management**

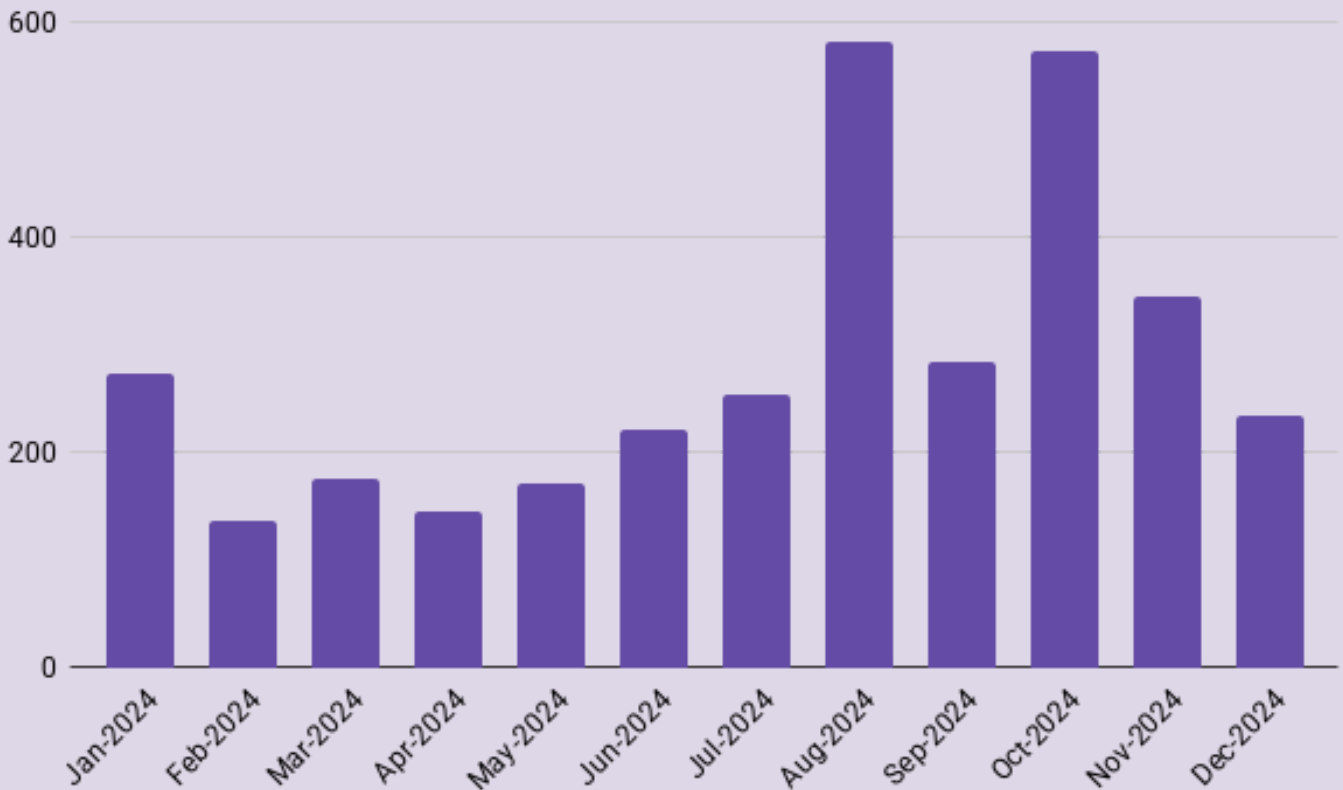
NICE **Oversee and Govern (OV)**

RED TEAMER

3,391 posted jobs

Red Teamers access sensitive information that achieves their unique goal. They do this by acting as swiftly and quietly as possible, emulating a malicious actor. Red Team assessments are employed to rigorously test an organization's detection and response capabilities. A Red Team assessment is far more targeted than penetration testing.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy **Offense**

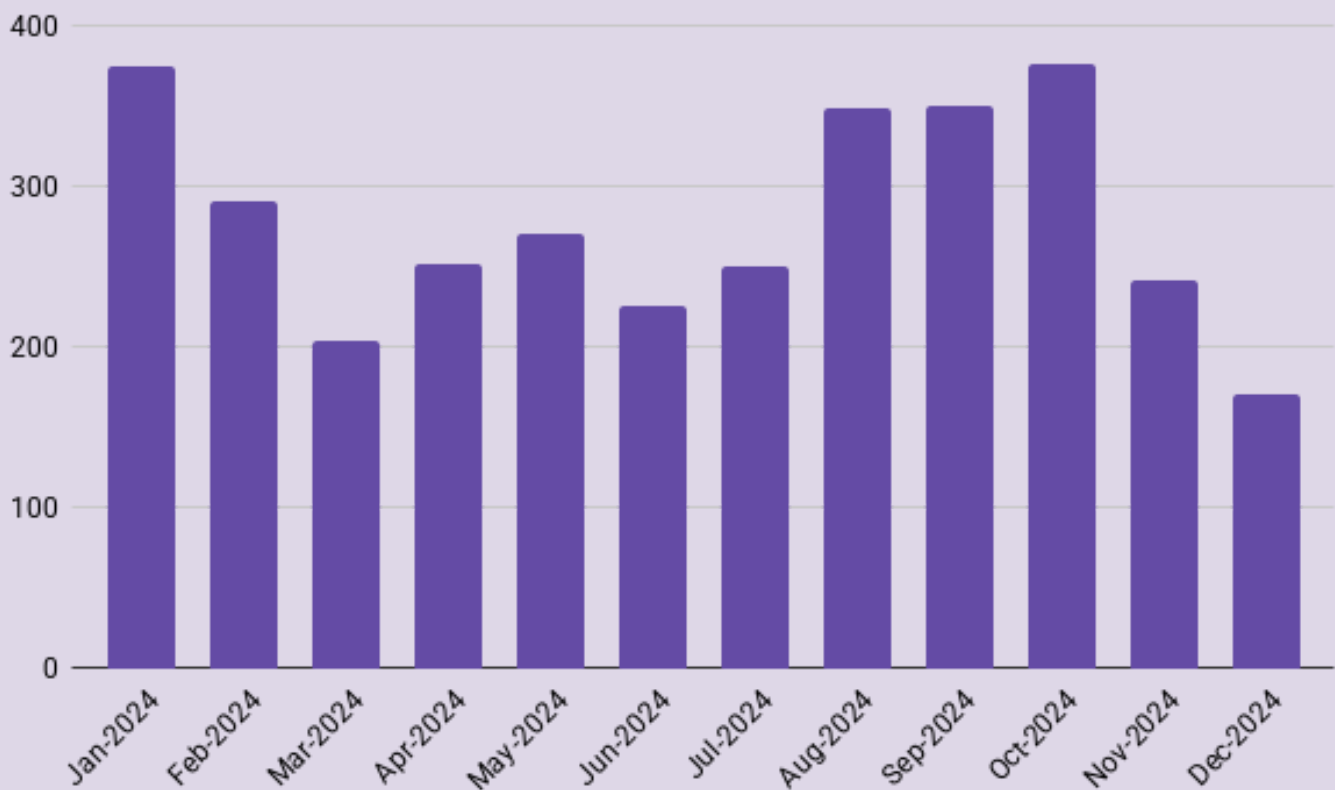
NICE **Analyze (AN)**

REVERSE ENGINEER / MALWARE ANALYST

3,349 posted jobs

Reverse Engineers, also known as Malware Analysts, use decompiling, disassembling, and de-obfuscating to gain a deeper understanding of how and what a malicious software operates. They identify, examine, and understand various forms of malicious software, such as adware, bots, rootkits, spyware, ransomware, Trojan horses, viruses, and worms.

January 2024 - December 2024 Source: CyberSN, 2025



CyberSN Taxonomy

Response





Get in Touch

For more information on our cybersecurity talent acquisition solutions, [contact CyberSN.](#)

To read more insights on the cybersecurity job market in 2023, check out our [2023 U.S. Cyber Job Posting Data Report.](#)

