enspire
partners

Job Opportunities for Cybersecurity Professionals

Learn about the best job opportunities on the market for Cybersecurity professionals and discover the experience Enspire Partners'clients expect.

The job prospects for Cybersecurity professionals are strong. In fact, the number of Cybersecurity jobs is climbing fast, from 3.5 million worldwide in 2020 to 4.1 million in 2022.

But specific roles in Cybersecurity vary, and it can take time to figure out which niche you want to target.

This whitepaper identifies the top Cybersecurity jobs for 2022, 2023, and beyond, plus what you can do to land a great position.

NOTE: Some clients refer to Cybersecurity as Information Security (or InfoSec) or IT Security. We will use these terms interchangeably, but the roles described below apply to each of these areas.

Job Opportunities for Cybersecurity Professionals

Top Cybersecurity Jobs for 2022 and Beyond

The following pages identify the most in-demand Cybersecurity jobs, organized according to entry, mid-level and advanced positions. Each section explores what's involved with each job and projected compensation.

Entry-Level Cybersecurity Positions

Entry-level jobs typically may be obtained through certification and training, although you will need strong technical aptitude and job-specific skills.

Information Security Administrator - Salary: $80,000+

An Information Security Administrator has a relatively wide range of responsibilities. They're responsible for protecting the organization from threats and helping individual users and departments maintain high Cybersecurity standards.

In many companies, the Information Security Administrator becomes the escalation point where users, from management to new employees, interact with the InfoSec team. Most candidates for these roles have some experience supporting networking environments and have obtained certifications and some practical training in Cybersecurity fundamentals.

Job responsibilities for an InfoSec Analyst include:

- Maintain Cybersecurity tools and monitor the network
- Research the latest Cybersecurity trends
- Identify, document, and report successful breaches
- Help users properly implement Cybersecurity technologies and protocols

Job Opportunities for Cybersecurity Professionals

IT Auditor/Security Process Analyst - Salary: $75,000+

Auditing functions exist in many IT areas, and Cybersecurity has an increasing demand for IT Audit professionals. IT Auditors are responsible for analyzing and assessing a company's technological infrastructure, ensuring processes and systems run accurately, efficiently, securely, and in adherence to regulations.

IT Auditors with a Cybersecurity focus have many of the following job responsibilities:

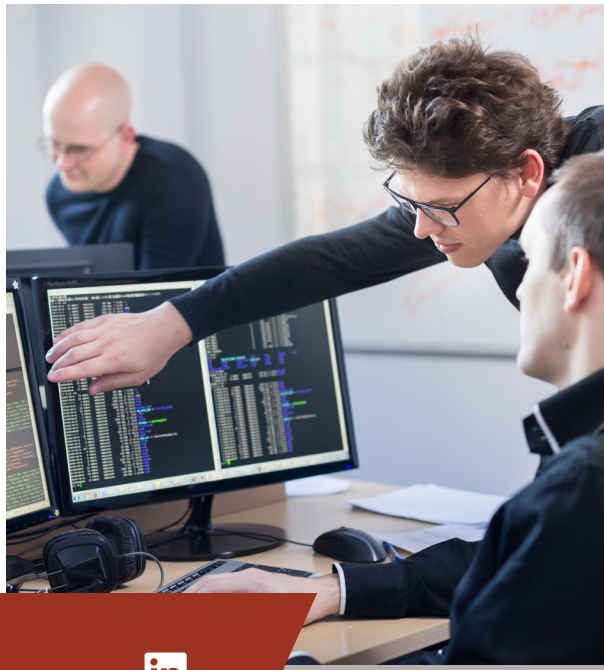
- Establish and ensure compliance with Information Security standards for all employees, contractors, vendors, and suppliers.
- Documentation and mapping of business processes and supporting IT functions.
- Applying established audit standards throughout the infrastructure.
- Auditing and assessing all aspects of the company's network applications, including software, programs, security, and communications.
- Creating and maintaining reporting and metrics of audit results.

Penetration Tester - Salary: $80,000+

A Penetration Tester, often referred to as a "Pen Tester," systematically identifies weaknesses in an organization's Cybersecurity system by designing and simulating attacks on the company's IT systems. Penetration Testers may have developed some of their skills in social settings outside of the workplace but usually have previous Programming or Quality Assurance experience.

For example, a Pen Tester may design an assault on:

- Company databases containing sensitive information
- Cloud resources, such as applications the organization uses to do business
- Web applications the company makes available to its employees or customers
- An organization's website, including testing how it reacts to a distributed denial-of-service (DDoS) attack, which involves overwhelming it with fraudulent requests



Mid-Level Cybersecurity Positions

In many companies, the most significant factor when determining who qualifies for advancement to higher-level positions is experience. The following positions typically require previous experience in these roles and specific certifications, such as the Certified Information Systems Security Professional (CISSP). Many of these roles also branch off into areas with a niche focus.

Cybersecurity Engineer - Salary: $110,000+

Most Cybersecurity Engineers have previous experience in the Cybersecurity Administrator role outlined previously. The Cybersecurity Engineer leverages this experience to research and implement leading-edge tools to mitigate the risk of a devastating cyber attack. Deciding which technologies a company needs to use to protect its digital assets is central to the Cybersecurity Engineer's job.

Typically, they will be hands-on with most or all of the following security tools:

- Firewalls—both hardware and software
- Intrusion detection systems
- Identification and authentication systems
- Antivirus software
- Web application firewalls, which specifically safeguard web apps from attacks

In addition to choosing the best tools, the Cybersecurity Engineer ensures these technologies are installed, maintained, and updated correctly.

Job Opportunities for Cybersecurity Professionals

Vulnerability Management Specialist - Salary: $120,000+

The Vulnerability Management Specialist leads the InfoSec Team in developing proactive measures to understand and prevent unauthorized penetration of the company's information systems. Vulnerability Management attempts to anticipate and interdict attacks that may have never occurred previously.

Vulnerability Management Specialists job responsibilities may include:

- Devising and leading White Hat vs. Black Hat scenarios to anticipate hacking attempts proactively. Because of these responsibilities, the Vulnerability Management Specialist may also manage the Penetration Testing Team.
- Reviewing databases, servers, and devices to analyze how an attacker might penetrate the system and develop strategies to stop such attacks.

Incident Response Specialist- Salary: $120,000+

The Incident Response Specialist develops contingency plans in the event of a successful systems breach and is responsible for managing the Incident Response process in the event such a breach occurs.

Incident Response job responsibilities may include:

- Developing the Incident Response strategy and communicating it to stakeholders across the country.
- Representing the InfoSec team in the event of a breach and effectively implementing IR plans and procedures.
- Helping law enforcement officials as they investigate a cyber attack
- Recovering data that's been stolen or lost due to damaged hard drives
- Manages post-attack analysis and remediation procedures.

Job Opportunities for Cybersecurity Professionals

Advanced/Senior Cybersecurity Positions

In addition to hands-on skills with the previous roles outlined, more senior roles typically require management and strategic leadership responsibilities.

Security Operations Manager - Salary: $150,000+

The Security Operations Manager oversees the Security Operations Center ("SOC"), a centralized unit dealing with security issues on an organizational and technical level, integrating people, processes, and technology to provide an optimal security posture.

Position responsibilities may include:

- Defining, recruiting, selecting, and managing various roles identified previously within the financial and business restraints available.
- Being a Thought Leader in innovative concepts of continuous improvement for all corporate security apparatus and processes.

Chief Information Security Officer - Salary: $200,000+

In response to an awareness of the need for Cybersecurity and the growing headcount employed by clients, a new C-level Executive role called the Chief Information Security Officer (CISO) has been created. This is a strategic position at progressive companies with a segregation of duties distinct from the traditional CIO/IT management team and "a seat at the table" in C-level decision-making.

In addition to other responsibilities, the CISO is responsible for:

- Developing the overarching Cybersecurity strategy from the company and blending various teammates in the InfoSec organization and matrixed areas of IT to ensure a safe and protected IS environment.
- Communicating and prioritizing these initiatives to other Executives and Business Leaders

Other Cybersecurity Positions

With the dynamic growth we are experiencing in Information Security, no list of titles and responsibilities could be exhaustive as companies recognize the increased need for Cybersecurity personnel across all levels of the enterprise. Some interesting areas we are seeing companies explore include Data Scientist Security Specialist (using Data Engineering techniques to classify high-volume attacks and vulnerabilities to enable the InfoSec Team to parse between high-priority threats and things not as critical) and even implementing Cybersecurity Standards in the manufacturing setting with PLC and firmware devices. No doubt, this escalation of the war in Cyberspace will continue as companies endeavor to protect their information assets while nefarious actors around the globe are constantly developing new methods of skirting defensive measures.

Job Opportunities for Cybersecurity Professionals

How to Get a Cybersecurity Job

The best way to land a Cybersecurity job is to leverage your current IT experience to move into a new role with a Cybersecurity focus. Training and certification are prerequisites for many openings, but there is no substitute for real-world knowledge when it comes to Infosec positions.

One practical way you can gain this experience is to join an ethical hacking group so you can learn how systems are attacked and defended in the corporate world. You should volunteer for any Infosec-related projects at your current job or seek out non-profits in need of IT resources and offer to help staff tasked with technology responsibilities.

Enspire Partners' Cybersecurity Center of Excellence

In response to client demand, Enspire Partners has developed a Center of Excellence associated with Cybersecurity. Our goal is to connect companies interested in growing their Cybersecurity capabilities with the best people and training resources available. Please join us for upcoming webinars on this topic and reach out to us directly if we can assist you with talent in this highly competitive space.

enspirepartners.com 770-312-8180 info@enspirepartners.com