

Articles > IT > 10 Cybersecurity Jobs: Entry-Level and Beyond

10 Cybersecurity Jobs: Entry-Level and Beyond

Written by Coursera Staff • Updated on Nov 30, 2023

 Share

Find a cybersecurity role that fits your interests.

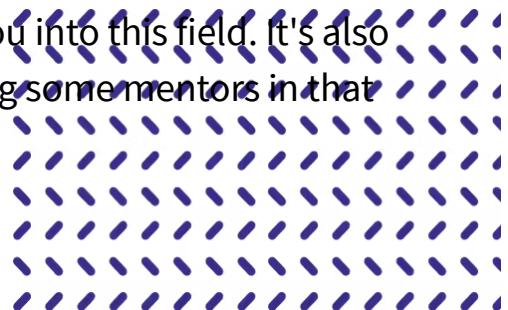


Cybersecurity professionals are in demand. Working in the cybersecurity field gives you the chance to work in a fast-paced environment where you continually learn and grow. Cybersecurity might be worth considering if you're already in the world of information technology (IT) or looking to make a career switch.

This article will look at some of the many roles available to cybersecurity professionals. We'll also discuss how to get started in cybersecurity and what your career path might look like.

When starting a new career path, it's helpful to network with industry professionals to learn more about the field and to create mutually beneficial relationships. Steve Graham, Senior Vice President Head of Product at EC-Council, had the following advice during Coursera's virtual panel, "How can online learning accelerate cybersecurity careers and talent?":

"There's a lot of different groups that you can join, whether it's meeting other students or joining special interest groups that get you into this field. It's also figuring out what you're passionate about and finding some mentors in that area that you can connect with to help guide you."



All salary data represents average annual total pay in the US, according to Glassdoor (September 2023). Total pay includes base salary and additional compensation such as commission, bonuses, and profit sharing.

4 entry-level cybersecurity jobs

In the context of cybersecurity, entry-level positions can be a bit of a misnomer. For some roles, the National Security Agency (NSA) defines entry-level as requiring a bachelor's degree plus up to three years of relevant experience—less with higher-level degrees. With a high school diploma or GED, you'll likely need between four and seven years of relevant experience on your resume.

Most cybersecurity professionals enter the field after gaining experience in an entry-level IT role. Here are a few of the most common entry-level jobs within the bigger world of cybersecurity.

1. Information security analyst

Average salary: \$107,343

Feeder role: network or systems administrator

As an information security analyst, you help protect an organization's computer networks and systems by:



- Monitoring networks for security breaches
- Investigating, documenting, and reporting security breaches
- Researching IT security trends
- Helping computer users with security products and procedures
- Developing strategies to help their organization remain secure

This is among the most common roles on a cybersecurity team and an excellent entry point into the world of information security.

Common certifications: CompTIA Security+, GIAC Certified Intrusion Analyst (GCIA), GIAC Certified Incident Handler (GCIH)

Related job titles: cybersecurity analyst, IT security analyst



**Microsoft Cybersecurity Analyst
Professional Certificate** >

Beginner level · 6 month(s)

Skills you'll build: Cloud Computing Security, Computer Security Incident Management, Network Security, Penetration Test, Threat mitigation, Computer Architecture, Cybersecurity, Cloud...
Operating Systems, Network Monitoring, Computer Network, Information Security (INFOSEC), Encryption techniques, threat intelligence, Compliance techniques, Authentication Methods, Access Management, Enterprise security, Identity governance, Event Management, Security Response, System Testing, Security Testing, Cybersecurity planning, Record management, Data Management, Cloud Architecture, Threat Model, Access Control, Asset Management, Cybersecurity strategies, Regulatory Compliance, Security Analysis

Average salary: \$140,108

2. Information security specialist

Feeder role: networking, IT support, systems engineering

In this role, you're the company's point person for security, ensuring that data remains secure against unauthorized access and cyberattacks. Responsibilities for security specialists vary from organization to organization but may include:

- Testing and maintaining firewalls and antivirus software
- Implementing security training

- Researching new security risks
- Suggesting improvements for security weaknesses



Common certifications: CompTIA Security+, Systems Security Certified Practitioner (SSCP), GIAC Security Essentials (GSEC)

Related job titles: cybersecurity specialist, information security specialist



(ISC)² Systems Security Certified Practitioner (SSCP) Specialization >

Beginner level · 6 month(s)

Skills you'll build: Asset, Risk Management, Access Control, Security Software, Cloud Computing Security, Wireless Security, Incident Detection and Response

★ 4.7 (706 ratings)

3. Digital forensic examiner

Average salary: \$102,375

Feeder role: IT support, risk analyst

If you enjoy seeking clues to solve a puzzle, this role might be for you. Digital forensic investigators retrieve information from computers and other digital devices to discover how an unauthorized person accessed a system or to gather evidence for legal purposes. Day-to-day tasks might include:

- Collecting, preserving, and analyzing digital evidence
- Recovering data from erased or damaged hard drives
- Documenting the data retrieval process and maintaining chain of custody
- Assisting law enforcement in criminal investigations
- Providing expert testimony in court proceedings

Common certifications: GIAC Certified Forensic Analyst, EnCase Certified Examiner (EnCE), AccessData Certified Examiner (ACE)

Related job titles: computer forensic specialist, cyber forensic specialist, digital forensics analyst



Cyber Incident Response Specialization

Beginner level · 4 month(s)

Skills you'll build: Network Forensics, Computer Security Incident Management, incident response handling, CSIH, analysis, Malware Analysis, Memory Forensics, Traffic Analysis,...

Continuous Function, Verification And Validation (V&V), Ordered Pair, Representational State Transfer (REST), Domain Name System (DNS), Image Resolution, Breach (Security Exploit), Packet

Analyzer



4. IT auditor

Average salary: \$90,252

Feeder role: network administrator, risk analyst, IT support

As an IT auditor, you'll assess your organization's technology for potential issues with security, efficiency, and compliance. Some of your regular tasks might include:

- Planning and performing audits
- Documenting and presenting audit findings
- Providing guidance on recommended and mandatory security measures
- Designing plans to fix any security risks
- Identifying opportunities for better efficiency

Common certifications: Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA)

Related job titles: internal IT auditor, security auditor



Information Systems Auditing, Controls and Assurance Course

Beginner level · 1 month(s)

Skills you'll build: Information Technology (IT) Management, Risk Management, Change Management, Information Security (INFOSEC), Audit



Moving up: 6 mid-level and advanced cybersecurity jobs

As you gain experience in cybersecurity, several paths can open up for advancement into more specialized roles. These are just a few options for mid-level and advanced cybersecurity professionals.

1. Security systems administrator

Average salary: \$68,264

Feeder role: systems administrator, information security analyst

In this role, you're typically put in charge of the day-to-day operations of an organization's cybersecurity systems. Your responsibilities might include:

- Monitoring systems and running regular backups
- Managing individual user accounts
- Developing and documenting security procedures for the organization
- Collaborating with security teams to respond to unwanted intrusions
- Participating in company-wide security audits

Common certifications: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM)

Related job titles: security administrator, cybersecurity administrator, information security officer



Cybersecurity Compliance Framework System Administration Course

Beginner level · 1 month(s)

★ 4.7 (3,097 ratings)



2. Penetration tester

Average salary: \$114,856

Feeder role: information security analyst, incident responder

As a penetration tester (pen tester for short), you'll help businesses identify their security weaknesses before malicious hackers can do the same. You do this by attempting to breach computer networks with the company's permission. Penetration testing tasks might include:

- Planning, designing, and carrying out penetration tests
- Creating reports on test results and offering recommendations to security decision-makers
- Developing scripts to automate parts of the testing process
- Conducting social engineering exercises (attempting to get company employees to disclose confidential information)
- Providing technical support during incident handling

Common certifications: Certified Ethical Hacker (CEH), CompTIA PenTest+, GIAC Certified Penetration Tester (GPEN)

Related job titles: white hat hacker, ethical hacker, vulnerability assessor



Exploiting and Securing Vulnerabilities in Java Applications Course

Intermediate level · 1 month(s)



Skills you'll build: Java, secure programming, security, Java Programming



★ 4.4 (58 ratings)

3. Security engineer

Average salary: \$142,763

Feeder role: information security analyst, penetration tester

In this role, you design the systems to keep a company's computers, networks, and data safe from cyberattacks to natural disasters. These security systems might include elements like firewalls and intrusion detection systems. Day-to-day tasks might include:

- Developing security standards and best practices
- Recommending security enhancements to management
- Ensuring new security systems are installed and configured correctly
- Testing security solutions
- Leading incident response teams
- Develop programs to automate vulnerability detection

Common certifications: Certified Information Systems Security Professional (CISSP), Certified Cloud Security Professional (CCSP)

Related job titles: cybersecurity engineer, network security engineer, information security engineer



Preparing for Google Cloud Certification: Cloud Security Engineer Professional Certificate >

Intermediate level · 10 month(s)

Skills you'll build: Google Compute Engine, Google App Engine (GAE), Google Cloud Platform, Cloud Computing, Create and understand custom IAM roles, Create and configure network...

Peering, Secure a Kubernetes environment

★ 4.8 (1,382 ratings)

4. Security architect



Average salary: \$245,303

Feeder role: security engineer, information security analyst

As a security architect, you set the vision for a company's security systems. This role combines programming, threat research, and policy development to keep an organization a step ahead of threats. Your responsibilities might include:

- Building and maintaining security networks and systems
- Preparing budgets and overseeing security expenses
- Coordinating security operations across IT and engineering departments
- Improving systems in response to security incidents or vulnerabilities
- Conducting breach of security drills

Common certifications: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), CSA Certificate of Cloud Security Knowledge (CCSK)

Related job titles: cybersecurity architect, information security architect



Managing Cybersecurity Specialization

Beginner level · 9 month(s)

Skills you'll build: Computer Security Incident Management, Risk Management, Network Security, Security Governance, Security Management, Cybersecurity terminology, cybersecurity...
program elements, Security vulnerabilities and treatments, Threats to cybersecurity, Cybersecurity planning, Risk identification, Risk treatment, Cybersecurity performance measurement, Wireless Security, Intrusion Detection System, Firewall (Computing), Computer Network, Business Continuity, Disaster Recovery, Incident response planning, Contingency Plan,

5. Cryptography engineer

Cybersecurity staffing, Cybersecurity Governance, Cyber-Security Regulation

Average salary: \$128,284

Feeder role: computer programmer, information security analyst, systems administrator

Working in cryptography involves securing data for communication and information exchange. [Cryptologists](#) create encryption algorithms, ciphers, and other security protocols to encrypt data. [Cryptanalysts](#) decrypt information that has been coded. Common tasks in this role include:

- Developing new cryptographic algorithms
- Analyzing existing algorithms for vulnerabilities
- Implementing encryption solutions
- Testing new encryption techniques and tools

Common certifications: EC-Council Certified Encryption Specialist (ECES)

Related job titles: cryptologist, cryptanalyst, cryptography engineer



Cryptography I
Course
1 month(s)
Skills you'll build: Cryptography, Cryptographic Attacks, Symmetric-Key Algorithm, Public-Key Cryptography
★ 4.8 (4,189 ratings)

6. Cybersecurity manager

Average salary: \$96,986

Feeder role: information security analyst, security administrator

In this cybersecurity leadership position, you're responsible for overseeing the security infrastructure at your organization. This might include:

- Managing human and technological resources
- Tracking changes to internal and external security policy
- Ensuring compliance with security rules and regulations
- Sourcing cybersecurity tools for the organization
- Leading risk mitigation efforts

Related job titles: information security ([InfoSec](#)) manager



**IBM Cybersecurity Analyst
Professional Certificate**

Beginner level · 4 month(s)

Skills you'll build: information security analyst, Junior cybersecurity analyst, IT security analyst, security analyst, Malware, Cybersecurity, Information Security (INFOSEC), IBM New Collar, Cyb...

★ 4.6 (10,964 ratings)

Attacks, networking basics, Network Security, database vulnerabilities, Sql Injection, Computer Security Incident Management, scripting, forensics, Penetration Test, network defensive tactics, threat intelligence, Application Security, Breach (Security Exploit), cyber attack, professional certificate, cybersecurity analyst



How to get a job in cybersecurity

While requirements for cybersecurity jobs vary widely from company to company, you might notice some common trends. Let's take a closer look at some of the requirements and how you can go about meeting them to get your first cybersecurity job.

Educational requirements

Many jobs in security list a bachelor's degree in [computer science](#), information technology, or a related field as a requirement. According to Zippia, 56 percent of cybersecurity specialists have a bachelor's and 23 percent have an associate degree [1]. While degrees are common among professionals in the cybersecurity industry, they're not always required.

That said, having a bachelor's or master's degree can often create more job opportunities, make you a more competitive candidate in the cybersecurity job market, or help you advance in your career. Some degree programs, like the [Online Master of Computer Science from Arizona State University](#) (available on Coursera), let you concentrate your studies in cybersecurity.

Cybersecurity certifications



Typically cybersecurity job postings may request at least one certification. You'll find more than 300 different certifications, and the quality isn't always the same.

If you're new to cybersecurity, consider starting with a more foundational certification, like the CompTIA Security+. From there, you can begin gaining the necessary work experience to earn more advanced certifications.

Read more: [10 Popular Cybersecurity Certifications](#)

In-demand cybersecurity skills

With so many cybersecurity positions to fill, having the right skills can go a long way toward securing you a job. To prepare for a cybersecurity career, start building your workplace and technical skills through online courses, boot camps, or self-study. These skills are a good place to start:

- Cloud security
- Programming (especially scripting) languages
- Encryption
- Knowledge of [cyber threats](#)
- Risk assessment and threat analysis
- Intrusion detection
- Problem solving
- Analytical thinking

Read more: [Is Cybersecurity Hard to Learn? 9 Tips for Success](#)

Finding entry-level opportunities

Getting started as an IT support technician or network administrator allows you to establish yourself within an organization and build up your technical skills before taking on the added responsibilities of a security role.

The National Security Agency (NSA) also offers [Development Programs](#) in Cybersecurity Operations and Cybersecurity Engineering. These three-year, full-time, paid roles help participants build their skills or switch to a new career.

When you're ready to start looking for jobs in cybersecurity, expand your search beyond the usual job sites (LinkedIn, Indeed, ZipRecruiter, etc.). You'll find a couple of sites that specialize in cybersecurity and tech job postings, including:

- [Dice](#)
- [ClearedJobs.Net](#)
- [NinjaJobs](#)

Get started in cybersecurity

Ready to develop both technical and workplace skills for a career in cybersecurity? The [Microsoft Cybersecurity Analyst Professional Certificate](#) and [Google Cybersecurity Professional Certificate](#) on Coursera are your gateways to exploring job titles like security analyst, SOC (security operations center) analyst, and more. Upon completion, you'll have exclusive access to career resources like resume review and interview prep that will support you in your job search.



Microsoft Cybersecurity Analyst Professional Certificate

Beginner level · 6 month(s)

Skills you'll build: Cloud Computing Security, Computer Security Incident Management, Network Security, Penetration Test, Threat mitigation, Computer Architecture, Cybersecurity, Cloud...

★ 4.8 (604 ratings)

(INFOSEC), Encryption techniques, threat intelligence, Compliance techniques, Authentication Methods, Access Management, Enterprise security, Identity governance, Event Management,



Google Cybersecurity Professional Certificate

Beginner level · 6 month(s)

Skills you'll build: Python Programming, Security Information and Event Management (SIEM) tools, SQL, Linux, Intrusion Detection Systems (IDS), Cybersecurity, Information Security...

★ 4.8 (12,418 ratings)

(INFOSEC), Ethics in cybersecurity, NIST Cybersecurity Framework (CSF), Historical Attacks, NIST Risk Management Framework (RMF), Security Audits, Incident Response Playbooks, Security

Frequently asked questions (FAQ)

Hardening, Network Security, Transmission Control Protocol / Internet Protocol (TCP/IP),

Network Architecture, Cloud Networks, Command line interface (CLI), Bash, Authentication,

vulnerability assessment, Cryptography, asset classification, threat analysis, Packet Analyzer,

Computer Programming, Coding, PEP 8 style guide, escalation, resume and portfolio

- Is it hard to get a cybersecurity job?
preparation, stakeholder communication, Job preparedness, integrity and discretion

- What types of companies are hiring cybersecurity jobs?

- What kind of cybersecurity jobs can you do remotely?

▽ Show all 4 frequently asked questions

Article sources

▽ View all sources

Keep reading

Cybersecurity Job Description: What to Expect

⌚ 7 min read · November 29, 2023

What Is Security Clearance? Types and Requirements for US Jobs

⌚ 6 min read · November 29, 2023

What Does a Cybersecurity Analyst Do? 2023 Job Guide

⌚ 6 min read · November 29, 2023

What Is a Compliance Analyst? Job Role, Skills, and Salaries

⌚ 7 min read · November 29, 2023

Updated on Nov 30, 2023

 Share

Written by:



Coursera Staff

Editorial Team

Coursera's editorial team is comprised of highly experienced professional editor...

This content has been made available for informational purposes only. Learners are advised to conduct additional research to ensure that courses and other credentials pursued meet their personal, professional, and financial goals.

Take \$100 off your annual subscription

Save now →

- ✓ For a limited time, you can get a new Coursera Plus annual subscription for \$100 off for your first year!
- ✓ Get unlimited access to 7,000+ learning programs from world-class universities and companies like Google, Microsoft, and Yale.
- ✓ Build the skills you need to succeed, anytime you need them—whether you're starting your first job, switching to a new career, or advancing in your current role.

Popular AI Content

AI For Business Specialization (Penn)
AI For Everyone Course (DLAI)
AI Product Management Specialization (Duke)

Popular Programs

Google Cybersecurity Professional Certificate
Google Data Analytics Professional Certificate

Popular Skills

Cybersecurity Courses
Data Analysis Courses
Data Science Courses
Digital Marketing Courses
Excel Courses

Popular Career Resources

Become a Data Analyst
CAPM Certification Requirements
Cybersecurity Career Paths
Data Analyst Career Guide



Deep Learning Specialization (DLAI)	Google Digital Marketing & E-commerce	Google Courses Power BI Courses	Essential IT Certifications
Generative AI for Everyone Course (DLAI)	Professional Certificate	Product Management Courses	High-Income Skills Worth Learning
Generative AI Fundamentals Specialization (IBM)	Google IT Automation with Python Professional Certificate	Project Management Courses	How to Get a PMP Certification
Generative AI with LLMs Course (DLAI & AWS)	Google IT Support Professional Certificate	Python Courses	Popular Cybersecurity Certifications
IBM Applied AI Professional Certificate	Google Project Management Professional Certificate	SQL Courses	Popular Data Analytics Certifications
Machine Learning Specialization (Stanford)	Google SEO Fundamentals	See All Courses	Popular PMI Certifications
NLP Specialization (DLAI)	Google UX Design Professional Certificate		Popular SQL Certifications
Prompt Engineering for ChatGPT Course (Vanderbilt)	Intuit Academy Bookkeeping Professional Certificate		See All Career Resources
Supervised Machine Learning Course (DLAI)	Python for Everybody		
See All AI Courses	Specialization		
	UI / UX Design Specialization		

Coursera

- About
- What We Offer
- Leadership
- Careers
- Catalog
- Coursera Plus
- Professional Certificates

Community

- Learners
- Partners
- Beta Testers
- Translators
- Blog
- Tech Blog
- Teaching Center

More

- Press
- Investors
- Terms
- Privacy
- Help
- Accessibility
- Contact
- Articles

Learn Anywhere



MasterTrack®

Certificates

Degrees

For Enterprise

For Government

For Campus

Become a Partner

Coronavirus
Response

Social Impact

Directory
coursera
Affiliates

Modern Slavery
Statement

Manage Cookie
Preferences



© 2023 Coursera Inc. All rights reserved.

