CIAT

ROADMAP FOR SUCCESS IN THE FIELD OF CYBERSECURITY

CIAT

ROADMAP FOR SUCCESS IN THE FIELD OF CYBERSECURITY

Table of Contents

What Are Employers Looking For In a Cybersecurity Candidate?

Congratulations if you're ready to start working as a cybersecurity professional. You're responsible for protecting the organization's data and networks by installing and maintaining security systems. The ability to react quickly to any security breaches in the network and keep an eye out for network and application problems is critical all everyone becoming a cybersecurity candidate.

Are you ready to learn about programming, networking, and security operations? These skills will help you secure your company's network. As a cybersecurity professional, you will continuously evaluate organizations' security needs and make recommendations.

Depending on the organization's needs, you could implement new security standards and best practices or ensure the company maintains updated security and assurance policies. Security breaches, inside data exfiltration, and external hacking are daily business problems. Students wanting to become "cyber warriors" should consider what it takes to become a valuable resource for their organization before starting this journey.

Flexibility, reliability, and understanding when working in cybersecurity are essential for all candidates.

58% Require a degree for entry-level cybersecurity positions.

27% say recent university graduates are well prepared for the cybersecurity challenges their organization is facing

31% say HR regularly understands their cybersecurity hiring needs.

Flexibility, continuous education, and being a scrum member are critical components to success in cybersecurity. Organizations will change their products, services, and locations based on cybersecurity breaches and ongoing threats. Candidates need to have that mindset before entering this field. Additional attributes include:

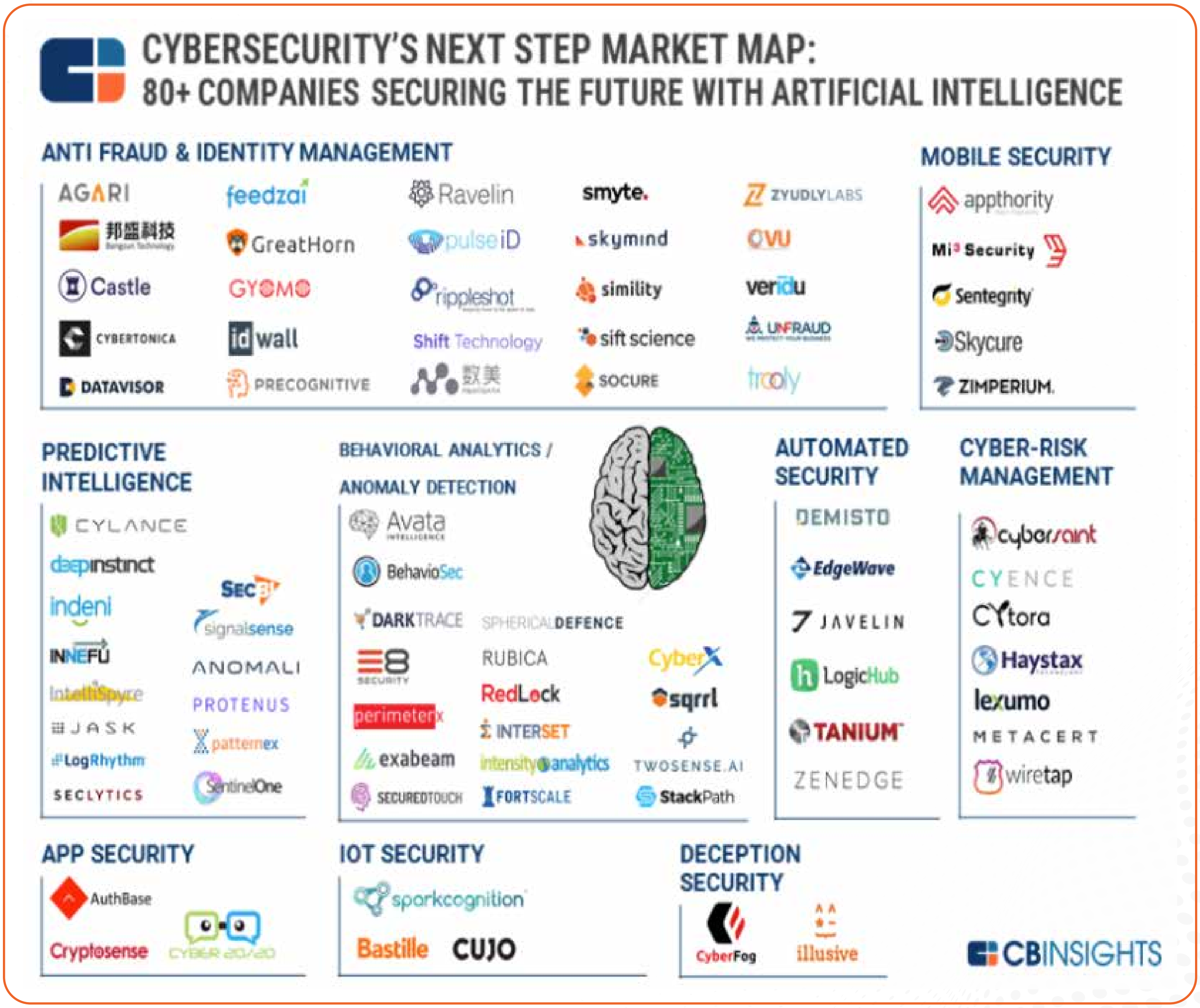
Read - Knowledge of security models, penetration testing, encryption, and research past cyber-attacks.

Watch Youtube Videos - Classes of attacks, diagnostic tools, and networking concepts.

Attend Online Virtual Events - Career in cybersecurity, cybersecurity Programs, and vendor presentations.

Security vendors are constantly refreshing youtube and other online content. Blogs, whitepapers, and ebooks get released each week.

The candidate is encouraged to bookmark specific vendors, industry groups, and experienced cyber warriors. By following their blogs, candidates can pick up a first-hand account of a security breach or hear about the latest email security and encryption.



Top Employers Hiring Qualified Cybersecurity Candidates

CYBERSECURITY JOB MARKET IN 2022-2023

Cybersecurity expertise is a highly sought-after technical skill. With threats like phishing, ransomware, data breaches, and cyberattacks, businesses need cybersecurity engineers to help protect their networks.

According to the Bureau Of Labor Statistics, a career in cybersecurity is expected to increase by 33% from 2020 to 2030—much faster than the overall average for all occupations. Cyber-attacks increase in frequency, and cybersecurity analysts are expected to become increasingly important to help companies develop innovative solutions to prevent them from stealing critical information or causing problems for their computer networks.

There were 1 million unfilled cybersecurity jobs in 2013. By 2021, there would be 3.5 million unfilled cybersecurity jobs still seeking qualified applicants. Since the dot-com bust, the demand for cybersecurity professionals has been this high for the first time.

Employers are struggling to find qualified cybersecurity professionals. Employers in the United States currently employ less than half the number of cybersecurity candidates they need to meet their current demand. There are now 48 qualified candidates for every hundred cybersecurity jobs posted.

The U.S.'s job market reflects a global shortage of cybersecurity professionals.

1 in 5

say it takes **more than 6 months** to find qualified cybersecurity candidates for open positions

Women In Cybersecurity

Women represent 25% of the global cybersecurity workforce by 2021, up from 20% in 2019 and around 9% in 2011. As we expect a steady increase in women entering cybersecurity jobs over the next ten years, the skills gap between men and women will shrink.

Higher Education

An Associate's Degree in cybersecurity can lead to many entry-level job opportunities, such as cybersecurity analyst, information security specialist, and penetration tester. Annual median salaries range from $75,000-$100,000.

Associate Degree programs like the Associate of Applied Science in Computer Information Systems provide the foundational training for those new to tech or early-stage IT professionals with a prior degree but need industry certifications. Earning a CIS Associate Degree is a definitive way to show potential employers that you have specialized expertise in hardware and software support, networking, cybersecurity, and cloud administration. Cybersecurity professionals need to demonstrate a wide range of technical skills, from hardware and software management to network security, and this program prepares students for entry-level cybersecurity careers, starting with the CompTIA Security+ certification.

- Washington, D.C.
- New York, NY
- Chicago, IL
- Arlington, VA
- San Diego, CA
- Atlanta, GA
- Charlotte, NC
- Boston MA
- Detroit, MI
- Los Angeles, CA
- Santa Clara, CA
- Portland, OR
- Austin, TX

Top Employer - United States (Cybersecurity):

Every organization needs cybersecurity resources. If the company uses email, web content, and online platforms for clients to access products and services, they need a cybersecurity team. Security vulnerabilities, cyber threats, and digital attacks impact employers.

Employers from 5 people to 100,000 continue recruiting cyber security engineers to help support DevOps, SecOps, NetOps, and AppDev teams. Many organizations outsource critical IT and secondary roles because they lack candidates and experienced personnel. Relevant experience in data analytics, problem-solving skills, and hands-on experience are a plus.

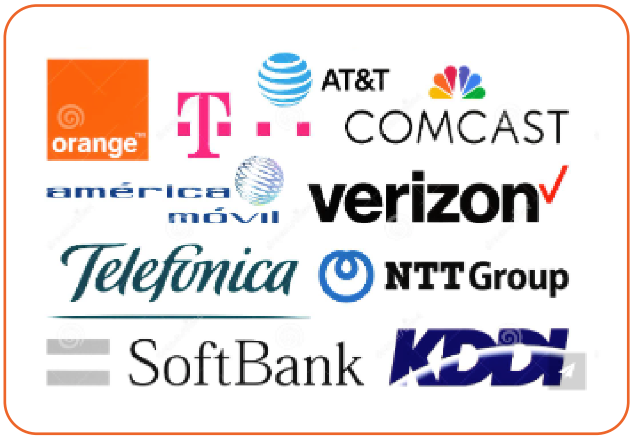
Job Roles: Cybersecurity engineer, network security engineer, software engineering, penetration testing engineers, application security engineers.

Adding Roles: Cloud Architects- Sales- Marketing – SecOps-DevOps-Netops -Incident Response – Product engineering – Customer Success – Partnership Manager – IT Helpdesk – Security Analyst

Employers Include:

FAAG

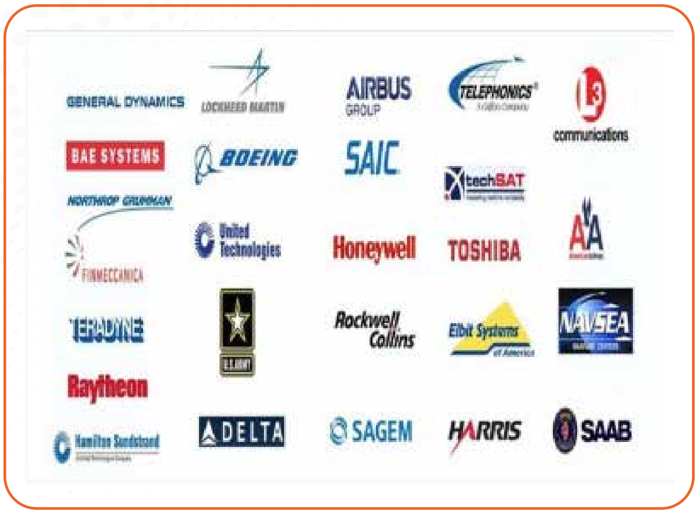
Global Telecom-Service Providers:



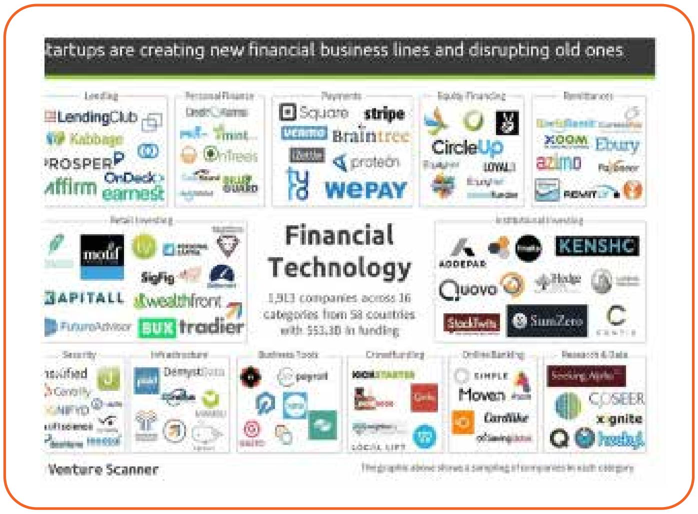
Public Sector(State Local Government, Higher Ed)

County of Los Angeles – Los Angeles California
County of Orange – Orange California
University of California – Sacramento California
The University of Chicago
University of Southern California
Arizona State University
University of Oregon
George Mason University (VA)
University of Texas
Northwestern University
University of California San Diego
State of Virginia
State of California
State of Florida

Global Defense (Clearance):



Global Financial – Fintech:



Emerging Markets – Growth Sectors:

According to the Bureau of Labor Statistics, based on the number of openings in the U.S. economy today and over the next few years, the idea of lifelong employment may arguably be a statistical truth. However, the amount of knowledge required for cybersecurity varies from person to person, but there are endless career opportunities in our field.

Cybercrime, which costs the world $10.4 trillion annually by 2025, is expected to generate new jobs roughly equal to the ones being filled over the next five years.

"If you know cybersecurity, you have a job for life," said Robert Herjavec, a Shark on ABC's Emmy Award-winning TV show "Shark Tank," in a 2018 Cybercrime Magazine podcast interview. At that time, he claimed a zero-percent unemployment rate in cybersecurity.

What Are SecOps,
United States (Cybersecurity):

DevOps environments play a crucial role for software developers and systems administrators, while NetOps is a DevOps-influenced approach to networking. Both create greater business agility, improve the digital experience for clients, and faster adoption of public clouds.

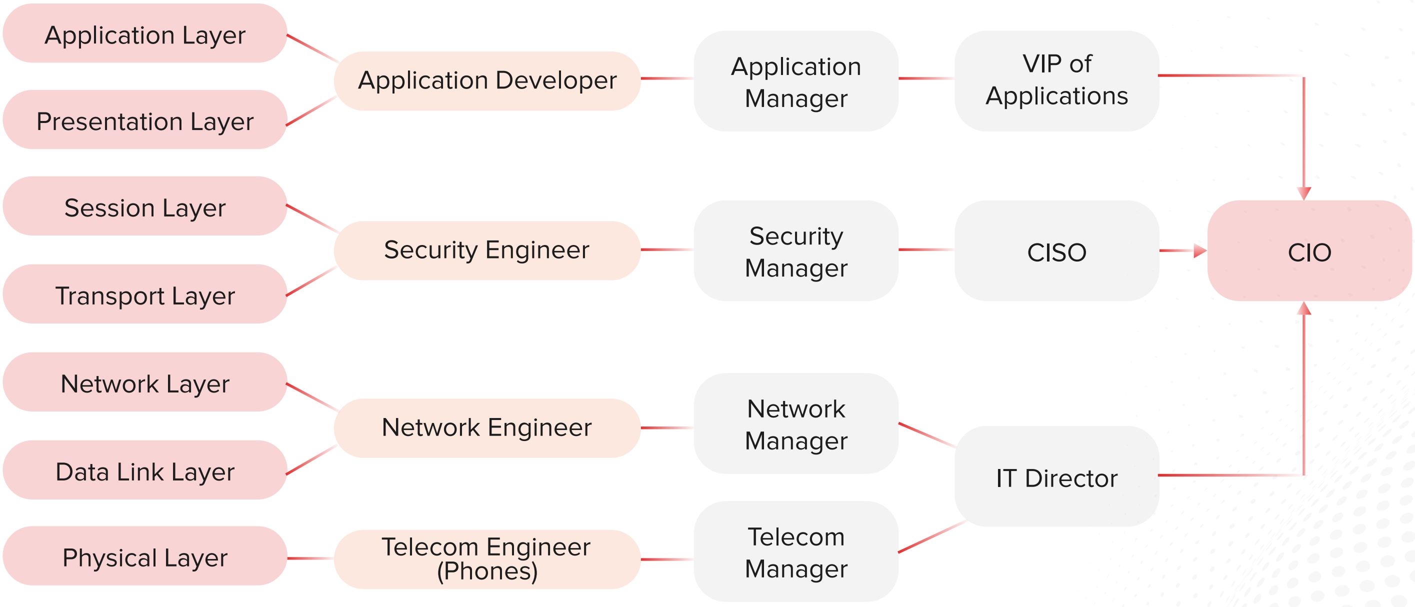
DevOps creates a fast and efficient application development cycle, while NetOps supports those apps' speedy and effective deployment. Organizations combine both groups to partner and leverage similar automation tools to streamline product development in less time.

DevOps rapidly has become the next business model for organizations process for better app delivery, software solutions revenue growth, and operational transformation.

In the novel "The Phoenix Project," (Gene Kim) wrote extensively about how dysfunctional IT departments have become. Duplication of systems, over-redundant networks, and poorly created legacy applications and system operations plagued the organization. Departments fighting over the budget, blaming other groups for system-wide failures, and IT leaders could not address business and financial impact issues to the board of directors in a language they could understand.

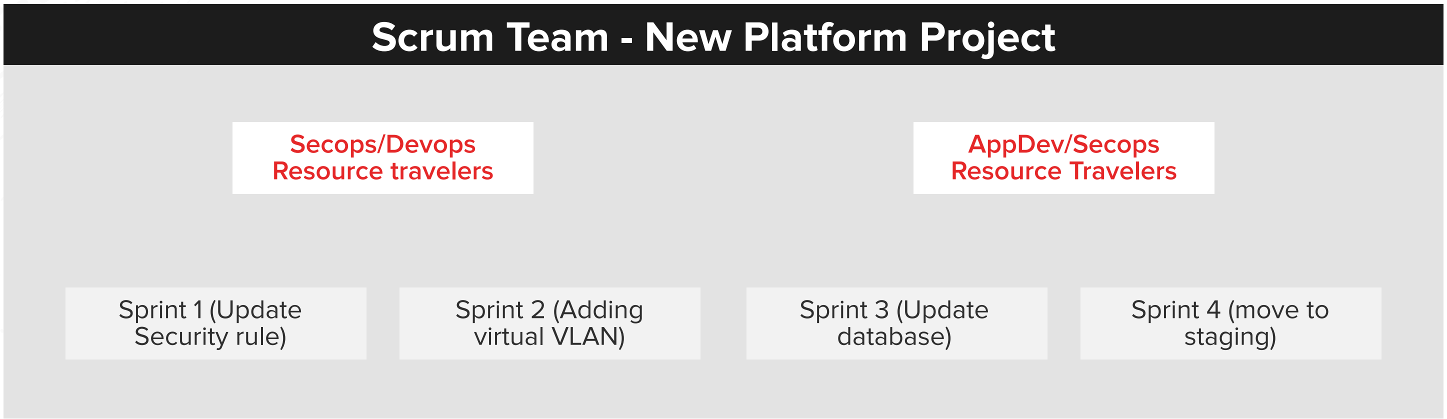
The book introduced the concept of development operations or DevOps in great detail.

DevOps changed how organizations develop the next generation of modern applications by moving toward an Agile workstream instead of the traditional Waterfall method. Agile development focused more on measuring "sprints" to accomplish tasks.



Traditional IT workflows categorize resources as network infrastructure and architecture design team personnel, including the “network engineer” or “security manager.” Roles like automation architects, scrum leads, and service delivery managers did not exist. Legacy IT structured its resources more around the OSI model. DevOps shifted the thinking toward a collaboration workplace or “scrum” team.

DevOps, SecOps, and NetOps agility became a horizontal model built on common workflows running in parallel compared to waterfall methods that relied on business functions before the next task could be completed.



Scrum Team - New Platform Project

Secops/Devops Resource travelers

AppDev/Secops Resource Travelers

Sprint 1 (Update Security rule)

Sprint 2 (Adding virtual VLAN)

Sprint 3 (Update database)

Sprint 4 (move to staging)

The Alignment between Netops And DevOps Roles

Infrastructure as code (IaC) enables DevOps teams to manage an application’s operational environment throughout the development and testing phases via automation and self-service. DevOps best practices were constructed from IaC projects. Adaptive applications leveraging next-generation application-centric view enablement follows the DevOps blueprint with IaC.

IaC helps organizations with their digital transformation journey through developing modern applications based on agile development, not a waterfall framework. Greater performance of applications and application protection is recognized early in the development cycle under DevOps agility. Security functions become enabled at each stage of development instead of at the end of the creation cycle.

Networking Teams Were Slow To Join The DevOps Movement.

DevOps became successful without significant networking involvement. Traditionally, when development teams finish building applications, they move the project to the networking team, who then begins to configure each server for deployment manually. The security department operated independently from the rest of the company and rarely had an input in the application development lifecycle.

By shifting networking left in the continuous integration continuous delivery (CI/CD) pipeline, NetOps helps increase efficiency in the software development lifecycle (SDLC) and minimizes late-stage deployment problems.

Moving Ahead Of Traditional IT To The DevOps Culture

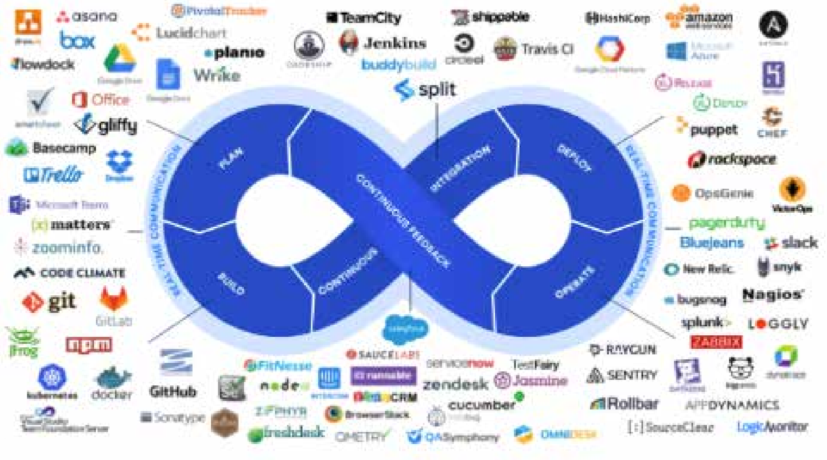
IT departments in the late 1990s and early 2000s were structured similar to the Open Systems Interconnection (OSI) model.

Well structured for its time, this model proved to lack the flexibility to adjust to the changing business climate. Each department would only focus on their part of the "stack" and quickly pass responsibility to other groups.

Change control became a struggle for organizations within the traditional IT stack. Simple changes require downstream and upstream communication, testing, and production validation. Often, a small application change could require a significant firewall change or a network topology costing the company money and time. In many cases, simple delays could take months to execute.

After 2008, when cybersecurity events became daily business impacts, companies needed to become flexible, nimble, and quick to react to stay up with the competitive market and hackers.

Everything about DevOps changed the company's culture around information technology operations.

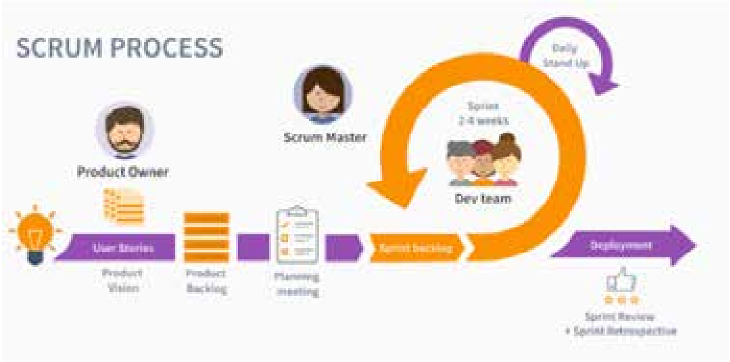


DevOps Tools

The rapid adoption of the DevOps culture to support digital transformation initiatives
Sub-groups or scrums are created from the traditional IT model. Previous IT security team members become the SecOps team. The application teams became part of the application owners group. NetOps teams are formed from the legacy telecom and network teams.

Be A Member Of A Scrum

Being a member of the team is critical to success in cybersecurity. Being a member of the scrum is all about teaming, collaboration, and contributing to the organization's effort to develop products and solve complex business objectives while protecting the company from cyber breaches.



Learn To Be A Scrum-Traveler

Travelers are subject matter experts with experience in specific domains. These experts move between various scrum teams and support multiple projects.

Candidates become valuable to any organization through continuous learning, experience, and collaboration. Being a scrum-traveler helps organizations leverage their talents between various components within the Agile development model. In one week, the scrum-traveler could be at the front-end of a new project sprint cycle providing expertise in security within a Microsoft platform. The following week, the traveler could be involved in several sprints around the quality assurance of a new solution. Every investment in learning cybersecurity will pay off for each candidate. The more the candidate invests in knowledge, the more significant opportunity to serve the organization.

Both reported to a scrum leader. Scrum leaders would be accountable for the project's success and be responsible for sprint execution.

Conclusion

In the spirit of the DevOps movement is a need for digital transformation change. Risk management, pen-testing, and vulnerability scanning should be considered a "sprint" within the agile security model supporting threat modeling engagements. Small to mid-size enterprise organizations could save money while gaining greater insight into their environment by executing these audits into a unified project instead of silo (waterfall) work cycles. The true benefactor of this new model would be the risk management team. By pulling together outputs from these "sprints" into a centralized contextual risk scoring methodology, organizations will better assess the environment by cross-correlation data sources from pen-testing, scanning, and IT audit control reviews.

All cybersecurity current and future professionals should be well-versed on each OPS term and their relationship to each other. Gone are the days of silo IT and waterfall methodologies. The future of IT is DevOps, SecOps, NetOps, NetSecOps, and DevsecOps.

Cybersecurity jobs - top career, salaries, and education options

The role of a cybersecurity warrior is comprehensive and exciting. Industry trends show a considerable demand for several cybersecurity roles. Cybersecurity analysts, cloud architects, and network security professionals are some of the most sought-after candidates.

A degree in cybersecurity provides many options for candidates to move laterally within the industry. Many cybersecurity candidates start as network engineers, eventually moving to a security architect role or an information security manager. Finding cybersecurity talent is a challenge for every industry to help fill many cybersecurity job openings that go unfilled over time due to the lack of available candidates.

Why the demand for cybersecurity professionals?

IBM's annual Cost of a Data Breach study revealed a single data breach could cost a company up to $3.29 million, a 12 percent increase from the cost of violations from the previous year. Add to this the devastating impact cyberattacks have had on corporations like Equifax, Facebook, and T-Mobile. No wonder businesses are paying more than ever to net in-demand cybersecurity professionals to protect their sensitive data and valuable assets.

Cybersecurity experts are pivotal in every organization's success. A secured network, applications, and cloud systems are financially and economically critical. Many companies seek out corporations that are secure, audited, and proven to be compliant with privacy and data security mandates.

The career outlook for cybersecurity positions

Depending on the position and employer, the education requirements for this profession usually include a bachelor's degree like an IT degree, computer science degree, or information assurance degree. Many security administrators gain professional experience through entry-level IT support jobs. Earning a certification can significantly improve career prospects.

All Cyber security professionals are critical to the success of the organization.

Cybersecurity careers are like other professions: people most likely to succeed are the ones that possess specific job skills. Specific skills in the field of cybersecurity are undoubtedly valuable for anyone aiming to thrive in a cybersecurity career.

However, that doesn't mean individuals should give up on cybersecurity career paths if they don't have all the capabilities yet. Before applying for jobs in cybersecurity, the candidate should consider their education, certifications, and experience. Each candidate should possess relevant knowledge and skill sets:

- **Analytical skills**
  Security incident analysis - attack tool analysis - critical thinking
- **Technical Skills**
  Determining Security Weaknesses - Understanding security protocols
- **Communication Skills**
  Communicating events throughout the organization
- **Presentation Skills**
  Document and present all security issues, events, and breaches to internal stakeholders.
- **Patience**
  Cybersecurity is dynamic. You must be patient with your career. Opportunities spawn every day. Companies continue to struggle to retain top talent, and demand for cybersecurity warriors continues to increase. Security training is constant in the cybersecurity job market.

Critical technical skills needed for a career In cybersecurity

- **Basic Information Knowledge**
  Networking, applications, and internet security.
- **Troubleshoot several problems at one time (horizontal thinking)**
  Candidates should focus on being a member of a scrum and not on being the top security person. Having the experience to cross troubleshooting multiple problems at one time and correlating the events is a critical skill set all candidates should work to achieve.

- **Understand the difference between Agile and Waterfall Application Development**

  The main difference is that Waterfall is a linear working system requiring the team to complete each project phase before moving on to the next one. At the same time, Agile encourages the team to work simultaneously on different project stages.

- **Have a working knowledge of the Python language**

  The cornerstone of security automation for DevOps and SecOps continues to evolve around scripting. Security operations automated response (SOAR) is a critical skill set for all candidates to understand. Python is the preferred language for SOAR.

- **Know the basics of programming in Powershell**

  Along with mastering python, having a working knowledge of Powershell for scripting also is critical for all candidates to understand.

What are the most common entry-level jobs in the cybersecurity field?

A cybersecurity candidate has several entry-level positions to apply for. Each role is in very high demand by companies, governments, and education institutions.

- **Desktop Security Analyst/Network administrator**

  Highly recommend the first position(excellent growth in learning and experience gathering)

- **Desktop Support Engineer**

  Recommend for candidates with basic knowledge of networking and troubleshooting skills

- **Cyber Security Engineer**

  It is highly recommended for candidates that start as desktop security analysts wanting to move up to a more significant challenge and more responsibility.

- **Cloud Architect - Amazon - Azure - Google**

  Ideal for candidates that have finished their cloud architect and cloud security certifications

What are the most advanced cybersecurity positions?

- **Security Architect- Senior level position:**

  The candidate should have at least three years of experience in cloud and networking engineering and hold a CISSP, AWS Cloud Architect certificate, and completed courses in SANS GIAC.

- **Cloud Security Architect**

  The candidate should have at least two years of experience in cloud engineering, operations, and automation. The candidate should complete the AWS cloud architect certification and Microsoft Azure credential.

- **Incident Response Engineer**

  The candidate should be familiar with Syslog, SNMP, security operations procedures, event correlation, and SIEM solutions. Many cybersecurity candidates start their careers working in the security operations department.

- **Cybersecurity Manager**

  An analyst or manager is in charge of protecting the confidentiality and integrity of data, whether in storage or transit.

- **Penetration Tester**

  Often referred to as Penetration Testing experts or Vulnerability Testers, these ethical hackers conduct frequent security tests across systems, networks, apps, databases, and your virtual infrastructure to identify potential vulnerabilities that cybercriminals can exploit.

- **Chief Information Security Officer**

  The Chief Information Security Officer remains in the highest position within a company related to cyber security. Any person in a CISO role establishes and maintains the vision and strategy to ensure that data assets (and relevant technology) are successfully protected.

- **Security Consultant - IT Auditors**

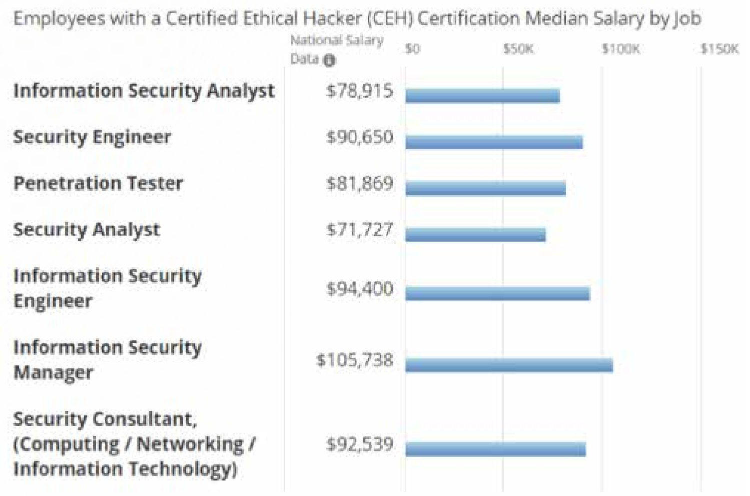
  Security consultants and auditors need excellent analytical, communication, computer, and other technical skills. Many security consultants earn professional certifications to stay relevant and expand their career opportunities. Popular certifications include certified information systems security professional, certified information systems auditor, and certified ethical hacker. Security consultants and IT auditors often manage all risk assessments completed within the organization to support various compliance mandates.

Cybersecurity average salary range by position

Many cybersecurity role compensations will vary depending on the organization’s size, where the role fits into the overall company structure and the geolocation of the position. Some parts of the country pay more or less depending on the region’s cost of living.

Many compensation packages will include a salary, bonus program, stock options, 401K, medical/dentist, education reimbursement, and mileage expense.

What is the expected annual salary expectation?



- Desktop Support Engineer

  Salary is $75,000 per year

- Network Security Engineer

  Salary is $105,000 per year

- Cybersecurity Analyst

  Salary is $95,528 per year

What are the highest-paid cybersecurity jobs?

- Cloud Network architect

  salary is $150,000 per year

- Cybersecurity Architect - Senior level position

  salary is 135,000 per year

- Chief Information Security Officer

  Salary is $225,000.00 per year

- SecOps/Incident Response Engineer

  salary is $114,893 per year

- Manager/Director Level Security Operations

  salary is $195,000.00 per year

Source: https://www.ziprecruiter.com/Salaries

Importance Of cybersecurity certifications and industry consortiums

Cybersecurity is one of the most crucial areas for ensuring a business's success and longevity. With cyberattacks growing in sophistication, it's essential for business owners to protect their companies by hiring qualified cybersecurity professionals to protect their company assets. Candidates with certifications in information security and cybersecurity with relevant work experience will have many options in the profession.

Becoming part of the growing cybersecurity workforce as a security specialist is full of lifelong choices of opportunity. From being a penetration tester to a role in cybersecurity management, the decision for a candidate to follow a cybersecurity career will be rewarding for years to come.

Here we will break down the top certifications and other guidance you'll need to make the right decision. This will serve as an excellent primer for individuals embarking on a cybersecurity career.

Basics Of cybersecurity

Certifications are an essential part of any career in information security. They're also a good way for employers to identify potential critical hires for their cybersecurity positions.

Cybersecurity certifications provide numerous benefits for employees and companies. In a survey by CompTIA, employers believe that IT certifications give workers an advantage. Certification is a good indicator of a candidate's success. With certifications, you'll be able to stand out from the crowd and open up career options.

Obtaining advanced certifications

Most cybersecurity certifications require a minimum of several years of technology, business, and undergraduate college education. With the rise of online courses and MOOCs (Massive Open Online Courses), there is an increasing demand for non-technical professionals to become certified.

There are specific and very generic cybersecurity certifications. You can get certified to perform a particular job, work with certain products, or be employed by a company. Broad certificates are relevant across job roles and industries and usually enhance someone's existing career. Most certifications require ongoing training, such as the Certified IT Security Professional (CISSP) certification, which requires recertification every five years. The CISA certification must be updated every three years.

Accredited organizations provide cybersecurity certifications that follow and maintain a certain level of industry-accepted standards. Certifications are valued because they are accepted by IT industry accrediting bodies and government agencies that set criteria.

Why do you need a cybersecurity certification?

The global cyber security market is forecast to expand at a compound rate of 10% a year through 2027, which means new jobs — and fierce competition for those high-paying jobs as more and more people try to get into cybersecurity. Every financial, healthcare sector, risk management, and government organization seeks certified professionals to help fill the many cybersecurity job openings.

Certification holders with a solid educational background in cybersecurity will show prospective employers they are ready for the challenge. So ask yourself: Where do you see yourself in three years? Do you want to focus on a company's security infrastructure, or do you want to be on the front lines? Or perhaps you want to be an auditor or pen tester, ensuring current systems work as they're supposed to. For executives, maybe you just want a proper understanding of the systems supporting your company.

Professional Certification Path

Most professional cybersecurity certifications are for those working directly in a technology role, whether in cybersecurity or a related field like information technology or networking.

As for difficulty level, certification exams range from moderate to challenging, depending on the material and type of certificate. For example, the highly technical Certified Ethical Hacker certification requires months of study and years of cybersecurity experience. At the same time, an entry-level certificate like Microsoft's Technology Associate Security Fundamentals might only call for a good general knowledge of computing and how programs and computer networks operate.

These certifications help round out areas of expertise, educate people about new technology and industry methods, and develop domain expertise. Most major cybersecurity certifications fall into this category.

What are the most important certifications for a cybersecurity Candidate?

Although a popular certification, the CISSP isn't for beginners because passing the exam requires extensive cybersecurity knowledge and field experience. It is intended for experienced cybersecurity administrators, managers, and executives. One key benefit of the certification is that it's vendor-neutral, so you can get experience managing and launching security programs without being tied to a single product or platform.

As each candidate decides on which domain within cybersecurity they wish to pursue, the following certifications are recommended:

- **CompTIA Sec+**
- **CEH - Certified Ethical Hacker**
- **AWS Security Specialty**
- **Microsoft Azure Security Engineer**
- **Amazon Cloud Security Architect**

  Highly recommended for candidates pursuing a career as a cloud security architect. This role focuses on building, designing, and installing security systems for cloud-based computing and data storage systems.

- **CISSP**

  Certified Information Systems Security Professional (Highly recommended after the candidate has at least two years of practical experience in a cyber security role.

- **SANS GIAC**

  The GIAC Security Expert (GSE), recently ranked the highest-value certification in the industry, is widely recognized as one of the most challenging and meaningful credentials in cybersecurity

- **CISM**

  Certified Information Security Manager - Highly recommended if the candidate pursues a career path towards IT or SecOps management.

- **CISA**

  Certified Information Security Auditor - Highly recommended if the candidate considers a career as an internal or external IT auditor.

- **CCNA**

  Cisco Certified Network Associate - Recommended for all candidates to demonstrate basic knowledge of networking principles.

- **CCNP**

  Certified Cisco Networking Professional - Highly recommended for candidates with one year of experience in networking, security operations, or cloud services.

- **MCAA**

  Microsoft Certified Azure Architect -Microsoft Certification validates your abilities to stay current and perform in job roles for a modern digital business. Ninety-one percent of certified technical experts believe that the effort employees put into acquiring new skills contributes to their success.

Being active in industry consortiums

In addition to continuous education, candidates are encouraged to participate in various industry consortiums and user groups. For candidates new to the cybersecurity space, being active in the local consortiums helps make connections and networks with technologies and experts in the field. Many experts will speak at industry events to share their experiences, knowledge, and best practices across several disciplines with the cybersecurity place. Many vendor representatives from Microsoft, CompTIA, Citrix, Cisco Systems, F5 Networks, and IBM often speak at these events and provide sponsorship.

Being active in industry consortiums

Public-Private Partnership
Industry consortiums are an excellent opportunity for candidates to network with other people to discover which companies are hiring. The sponsoring technology company and other prospective employers will also hold job fairs during consortium events. Candidates can learn firsthand what companies are looking for, what positions are available, the expected salary, and the timeline for the job needing to be filled.

Top Cybersecurity Industry Usergroups and Consortiums

The cybersecurity market host several industry user groups, consortium, and conferences. Many of these user groups are specific to particular domains and areas of interest within the cybersecurity consortium.

Here is a list of regional and national groups all candidates should participate in:

- **ISSA**
  International Systems Security Association(regional and national)
- **WiCYS**
  Woman in Cybersecurity
- **WSC**
  Woman's society of CyberJutsu
- **ACIC**
  Automotive Cybersecurity Industry Consortium
- **ISACA**
  Information Systems Audit and Control Association (regional and national)
- **RSA Conference**
  Yearly conference - a global industry consortium.
- **SANS.Org**
  SANS focuses on continuous certification and learning for cyber professionals.
- **ISC2**
  (ISC)^2 was founded in 1989 as the International Information System Security Certification Consortium, Inc. Our founders saw the need for standardization and certification in the cybersecurity industry. Since then, our founders and members have been shaping the information security profession.
- **AISP**
  Association of Information Security Professionals

How To Develop A Successful Career In The Cybersecurity Field

Cybersecurity jobs continue to grow as more regulation and security incidents impact people's lives. As technology continues to become an integral part of our daily lives, it'll be essential to protect the technology that makes it possible. The cybersecurity industry suffers from a lack of qualified candidates to deal with the constant attack on organizations' security systems and assets.

Cybersecurity is in every facet of a life well beyond the board room

It's no wonder many analysts regularly identify cybersecurity threats as one of the top two issues facing business today—failing to keep data security risks, fines from government entities, and damage to reputations.

Security professionals at all levels not only know the most current security concepts and industry trends, but they also know the most recent privacy and security regulations. For example, the new California Consumer Privacy Act of 2020, which gives consumers more control over their data, goes into effect on Jan. 1, 2021. When a security incident occurs, companies are often fined, executives are fired, customers may leave, and an organization's reputation takes a hit. Cybersecurity experts help companies avoid the headaches of a cyberattack by keeping their security strategy and operations up to date.

Valuable soft skills essential to all cybersecurity professionals

A successful career requires soft skills, flexibility, and acceptance of a trial and error culture. There are several reasons why companies cannot find the skilled cybersecurity professionals they need. First, there are not enough qualified cybersecurity professionals with technical and soft skills.

Organizations will change their product offerings, services, and locations based on cybersecurity breaches and ongoing threat assessments.

How do you stay up with the constant change in cybersecurity?

To start, you'll want to develop good work habits, including the capacity to work methodically (in a detail-oriented manner).

The following critical skills also come in handy:

- Flexibility
- Continuous education
- Being a scrum member

An eye for integration skills

Any good cybersecurity professional knows how to holistically examine a company's security setup, including threat modeling, specifications, implementation, testing, and vulnerability assessment.

They also understand security issues associated with operating systems, networking, and virtualization software.

Knowledge gained is knowledge earned.

Organizations will create new jobs for cyber security engineers based on needs following a security attack. Cybersecurity positions within organizations are not static.

- Knowledge of Risk Management - Foundation Skills in risk, compliance, and auditing helpful
- Knowledge of Network Security - Hands-on experience helpful
- Knowledge of Network Protocols - Relevant Experience in Network protocols and
- portsUnderstanding of incident Response - Analytical skills helpful
- Knowledge of Intrusion Detection - Technical background in IDS, IPS, and Host-based helpful
- Understanding of System Administration - Background in Security Concepts helpful

Knowledge, past experiences, the latest educational investments in workshops, and attending lectures will all bring value to the candidate:

- Read - Knowledge of Security Models, Encryption, and cyber-attack stages
- Watch Youtube Videos - Classes Of Attacks, Diagnostic tools, and networking concepts.
- Read More

Security vendors are constantly refreshing YouTube and other online content. Blogs, whitepapers, and ebooks get released each week. The candidate is encouraged to bookmark specific vendors, industry groups, and experienced cyber warriors. By following their blogs, candidates can pick up a first-hand account of a security breach or hear about the latest email security and encryption.

Embracing trial and error in cybersecurity careers

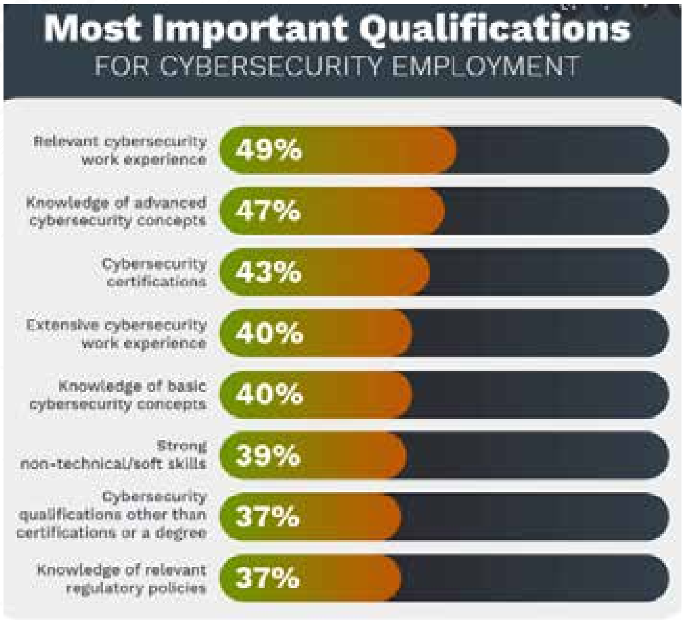
Accepting the concept of trial and error is critical for any cybersecurity candidate. Like other career paths, many people in the early days of cybersecurity did not attend a formal school to learn the craft. Many early practitioners learned cybersecurity by picking up a manual or learning as they went along. In the late 1990s, the idea of a firewall looked more like an extended access control list on a Cisco router. Setting up a firewall looks similar to loading a server application in a single computer device with two cables coming in and out—one for the "clean" and the other for the "dirty" network. There was no formal education around deploying firewalls, not even a youtube video.

Technology is far from perfect. Configuration mistakes happen daily to SecOps, DevOps, and NetOps team members. Sometimes, these mistakes aren't recognized for several months after deployment. When things do break, and they will, a good cybersecurity professional will focus on experience, knowledge of the product, and remember the fundamentals of all solutions; they will break, and rebooting doesn't always fix the problem. Solving the problem through trial and error for the cybersecurity professional is a good thing. Sometimes, there are many ways to solve a cybersecurity issue. Multiple team members from DevOps, SecOps, and NetsOps will often collaborate to develop options to solve the problems. Together, the teams learn from each other.

How to gain more cybersecurity experience

Many cybersecurity professionals are driven to learn about the daily applications, systems, and networks they protect. More often, a SecOps, DevOps, or Netops person will volunteer their time in other parts of the information technology to gain more knowledge of the organization's digital landscape. Some will block out time on their weekly calendar to help out in the IT helpdesk helping out with trouble tickets. Some cybersecurity team members will volunteer to help with weekend network cutovers or system upgrades. The cybersecurity professionals will learn more about the organization's technology environment and become more well-rounded teammates to others in the IT department.

How To Apply For A Job In Cybersecurity?



Today, the cybersecurity job market is near near-zero unemployment, and organizations across the industry offer high salaries for top cybersecurity talent. Salaries for jobs in cybersecurity are high compared to other fields.

The job outlook for cybersecurity practitioners is highly positive, making it an excellent option for anyone looking for a career in cybersecurity. According to ISC2.org, approximately 2.93 million cybersecurity positions are open around the globe.

Applying for a job in cybersecurity is familiar to other career fields. Employers are looking for people with technical skills, relevant experience, and a solid foundation of knowledge in the area.

Candidates should consider several factors before applying for various entry-level positions:

- For the first step in applying for entry-level cybersecurity jobs, the applicant needs to build a list of the top 3 domains they plan to focus on. Are you preparing for a career as network security, application security developer, or security operations manager?
- The applicants must be honest and assess their cybersecurity skill set, education, and career expectations. Cybersecurity is no different.
- Seek mentors to help build the three positions' shortlist and advise which companies will most likely be hiring. The field is filled with experienced cybersecurity professionals who love to mentor others.
- Landing the first role in cybersecurity is only the start. Experienced cybersecurity warriors did not start as senior incident directors on day one. The journey within cybersecurity is dynamic.

What do all candidates need to have ready before applying for a job?

Understanding Industry terms:

All applicants should be well versed in industry terms and acronyms for cybersecurity. These acronyms for cybersecurity roles include:

SecOps - Security Operations and Security Engineering

NetOps - Network Operations and Network Engineer Role

DevOps - System Operations and Software Developers

APPDev - Application Development and Software Engineering

CISSP - Certification Information Systems Security Professional

Complete Academic Courses:

An associate's or bachelor's degree in computer science, cybersecurity, and application development are essential to entering the cybersecurity industry. Having a solid foundation of knowledge to complement your hands-on experience will help you obtain the dream job you seek.

Continue with all your certification courses:

Another critical component in the journey in the cybersecurity job market is earning advanced industry certifications. CompTIA Security+, Cisco CCNA, and Microsoft Azure fundamentals should be a focus for the applicant to achieve before and during the job search.

Network:

A great way to discover an entry-level job in cybersecurity is to network with professionals in the industry. Networking at vendor seminars, Linkedin groups, and job fairs is a great way to learn about companies currently hiring.

Create a portfolio of your IT and Cybersecurity projects:

While searching for that perfect role in cybersecurity, volunteer or hire on as a contractor within a company to gain valuable hands-on experience—document what you have learned in these contracting engagements without disclosing any sensitive information about the company, the content you create could help during your interview process by showing recruiters and employers firsthand what you have accomplished so far in your journey.

Practice Interviewing with your friends and mentors:

Before any interview, always practice with a friend or mentor. Role-playing is very helpful for you to learn the best to answer cybersecurity questions during an interview. Even with significant experience in cybersecurity, the ability to articulate and communicate effectively is a very positive trait.

Be patient:

Jobs are there. Companies are hiring. It takes time for a company to line up the job role, budget for the salary and benefits, and interview to find the best candidate for the position.

TAKE
THE FIRST STEP.

IT Career Development at CIAT

Building a strong IT career takes hard work and dedication. Whether you're just starting in the field or advancing your career, learning how to create an education plan that aligns with your career goals saves you time and money and delivers the most significant return on your investment.

The IT industry offers both broad and specialized career opportunities. Explore sample job titles below by area of interest to learn more about how to land the dream job you have your eye on.

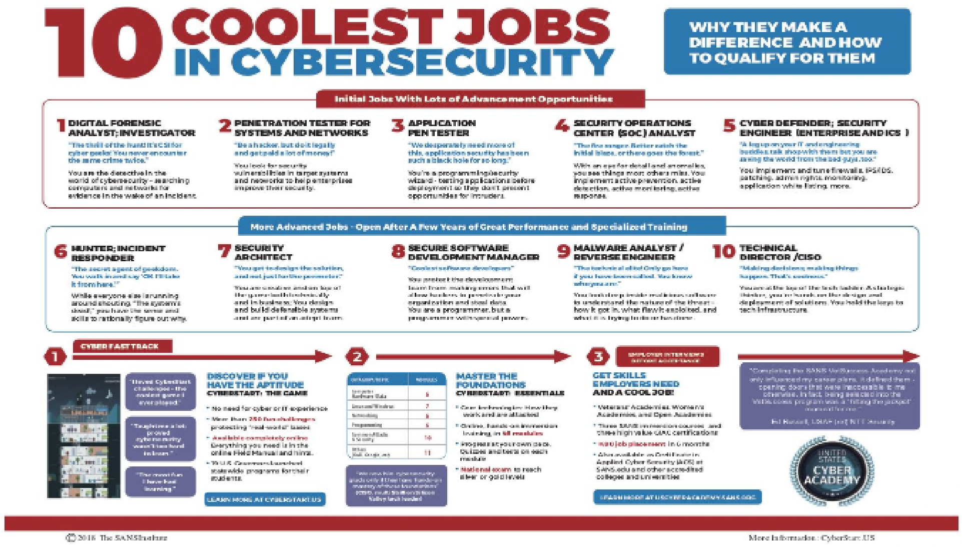
Career Planning

You've chosen an education plan with a goal in mind, and now you're focused on making the most of your educational resources to ensure you're setting yourself up for success in the job market. The most impactful recommendation we give to all new CIAT students in the tech field is not to wait until graduation to start their IT career planning. When you begin your career planning steps from day 1 of your program, you graduate career-ready and are more likely to find your first job quickly, with competitive salary ranges.

- Getting IT Certified
- Building Your Coding Portfolio

Let Us Help You Achieve Your Career Goals

When landing your dream job, CIAT supports its students every step of the way – ensuring you graduate with more than just a degree. Our IT career coaching services focus on professional and personal development to help prepare you for your career. Request support today to get started.



10 COOLEST JOBS IN CYBERSECURITY

WHY THEY MAKE A DIFFERENCE AND HOW TO QUALIFY FOR THEM

Initial Jobs With Lots of Advancement Opportunities

1 DIGITAL FORENSIC ANALYST; INVESTIGATOR
"The thrill of the hunt! It's CSI for cyber geeks! You never encounter the same crime twice."
You are the detective in the world of cybersecurity – searching computers and networks for evidence in the wake of an incident.

2 PENETRATION TESTER FOR SYSTEMS AND NETWORKS
"Be a hacker, but do it legally and get paid a lot of money!"
You look for security vulnerabilities in target systems and networks to help enterprises improve their security.

3 APPLICATION PEN TESTER
"We desperately need more of this, application security has been such a black hole for so long."
You're a programming/security wizard – testing applications before deployment so they don't present opportunities for intruders.

4 SECURITY OPERATIONS CENTER (SOC) ANALYST
"The fire ranger. Better catch the initial blaze, or there goes the forest."
With an eye for detail and anomalies, you see things most others miss. You implement active prevention, active detection, active monitoring, active response.

5 CYBER DEFENDER; SECURITY ENGINEER (ENTERPRISE AND ICS)
"A leg up on your IT and engineering buddies, talk shop with them but you are saving the world from the bad guys, too."
You implement and tune firewalls, IPS/IDS, patching, admin rights, monitoring, application white listing, more.

More Advanced Jobs - Open After A Few Years of Great Performance and Specialized Training

6 HUNTER; INCIDENT RESPONDER
"The secret agent of geekdom. You walk in and say 'OK I'll take it from here.'"
While everyone else is running around shouting, "The system's dead!," you have the sense and skills to rationally figure out why.

7 SECURITY ARCHITECT
"You get to design the solution, and not just for the perimeter."
You are creative and on top of the game both technically and in business. You design and build defensible systems and are part of an adept team.

8 SECURE SOFTWARE DEVELOPMENT MANAGER
"Coolest software developers"
You protect the development team from making errors that will allow hackers to penetrate your organization and steal data. You are a programmer, but a programmer with special powers.

9 MALWARE ANALYST / REVERSE ENGINEER
"The technical elite! Only go here if you have been called. You know who you are."
You look deep inside malicious software to understand the nature of the threat – how it got in, what flaw it exploited, and what it is trying to do or has done.

10 TECHNICAL DIRECTOR /CISO
"Making decisions; making things happen. That's coolness."
You are at the top of the tech ladder. A strategic thinker, you're hands on the design and deployment of solutions. You hold the keys to tech infrastructure.

1 CYBER FAST TRACK

"I loved CyberStart challenges – the coolest game I ever played."

"Taught me a lot, proved cybersecurity wasn't too hard to learn."

"The most fun I have had learning."

DISCOVER IF YOU HAVE THE APTITUDE
CYBERSTART: THE GAME
- No need for cyber or IT experience
- More than 250 fun challenges protecting "real-world" bases
- Available completely online. Everything you need is in the online Field Manual and hints.
- 19 U.S. Governors launched statewide programs for their students.

LEARN MORE AT CYBERSTART.US

2

[illegible]	[illegible]
Computer Hardware Hubs	6
Linux and Windows	7
Networking	6
Programming	6
System and Web Security	16
[illegible]	11

[illegible]

MASTER THE FOUNDATIONS
CYBERSTART: ESSENTIALS
- Core technologies: How they work and are attacked
- Online, hands-on immersion training, in 58 modules
- Progress at your own pace. Quizzes and tests on each module
- National exam to reach silver or gold levels

3 EMPLOYER INTERVIEWS [illegible]

GET SKILLS EMPLOYERS NEED AND A COOL JOB!
- Veterans' Academies, Women's Academies, and Open Academies
- Three SANS immersion courses and three high value GIAC certifications
- [illegible] job placement in 6 months
- Also available as Certificate in Applied Cyber Security (ACS) at SANS.edu and other accredited colleges and universities

LEARN MORE AT USCYBERACADEMY.SANS.ORG

"Completing the SANS VetSuccess Academy not only influenced my career plans, it defined them – opening doors that were inaccessible to me otherwise. In fact, being selected into the VetSuccess program was a "hitting the jackpot" moment for me."

[illegible], USMC (ret) [illegible]

UNITED STATES CYBER ACADEMY

© 2018 The SANS Institute

More Information: CyberStart.US