A GUIDE TO STARTING A CAREER IN CYBER SECURITY

STATIONX

2024 EDITION

A Guide To Starting a Career in Cyber Security

Right now, there is a severe shortage of talent in the Cyber Security industry.

Globally, an estimated 3.4 million more cyber security workers are needed to meet the needs of employers.

This growing skills gap represents a great opportunity: By taking the right steps now, you can quickly gather the skills to qualify for one of these jobs and advance your career.

But with all of this opportunity, there comes a problem:

How do you know where to start? Fortunately, you're in the right place.

In this guide, you're going to learn a simple 5-step process for getting started in Cyber Security.

By reading through each of these 5 steps, you'll become educated and familiar with the requirements of a job in this industry.

About the Author

Hi, I'm **Nathan House,** a leading cyber security expert and founder of the StationX. The #1 Cyber Security Training and Career Development Platform, I have over 30 years of experience in cyber security and won the AI - Cyber Security Educator of the Year.

Trust me, I understand how overwhelming this industry can be, which is why I launched StationX to help people just like you to study Cyber Security at their own pace, online.

The following 5 steps in this guide are my #1 recommendations for anyone getting started in this exciting and rewarding career.

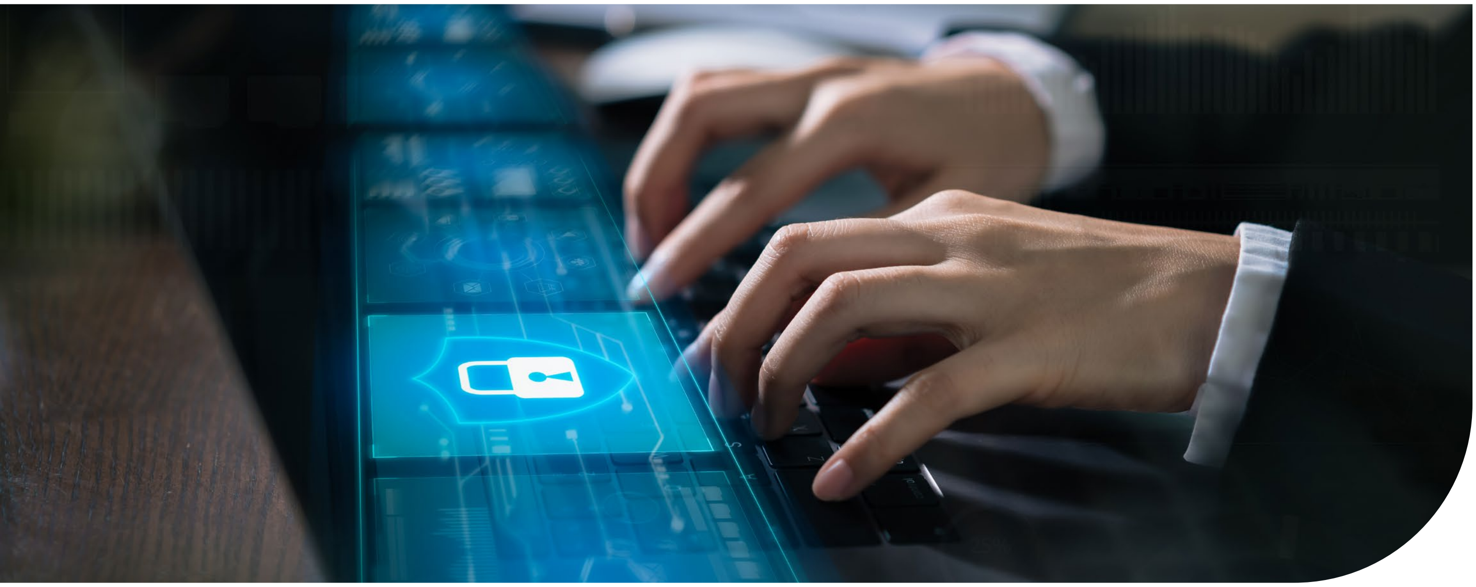
1
Step

Get to Know the Cyber Security Industry and What Jobs are on Offer

Often people believe that cyber security is all about technology and hacking. This is somewhat true, but cyber security is much more than that.

It is a discipline of managing risk, which might happen to have technology as a solution. This means roles in security can vary massively from simply managing a team or performing a basic audit, to computer forensics and other highly technical work like ethical hacking.

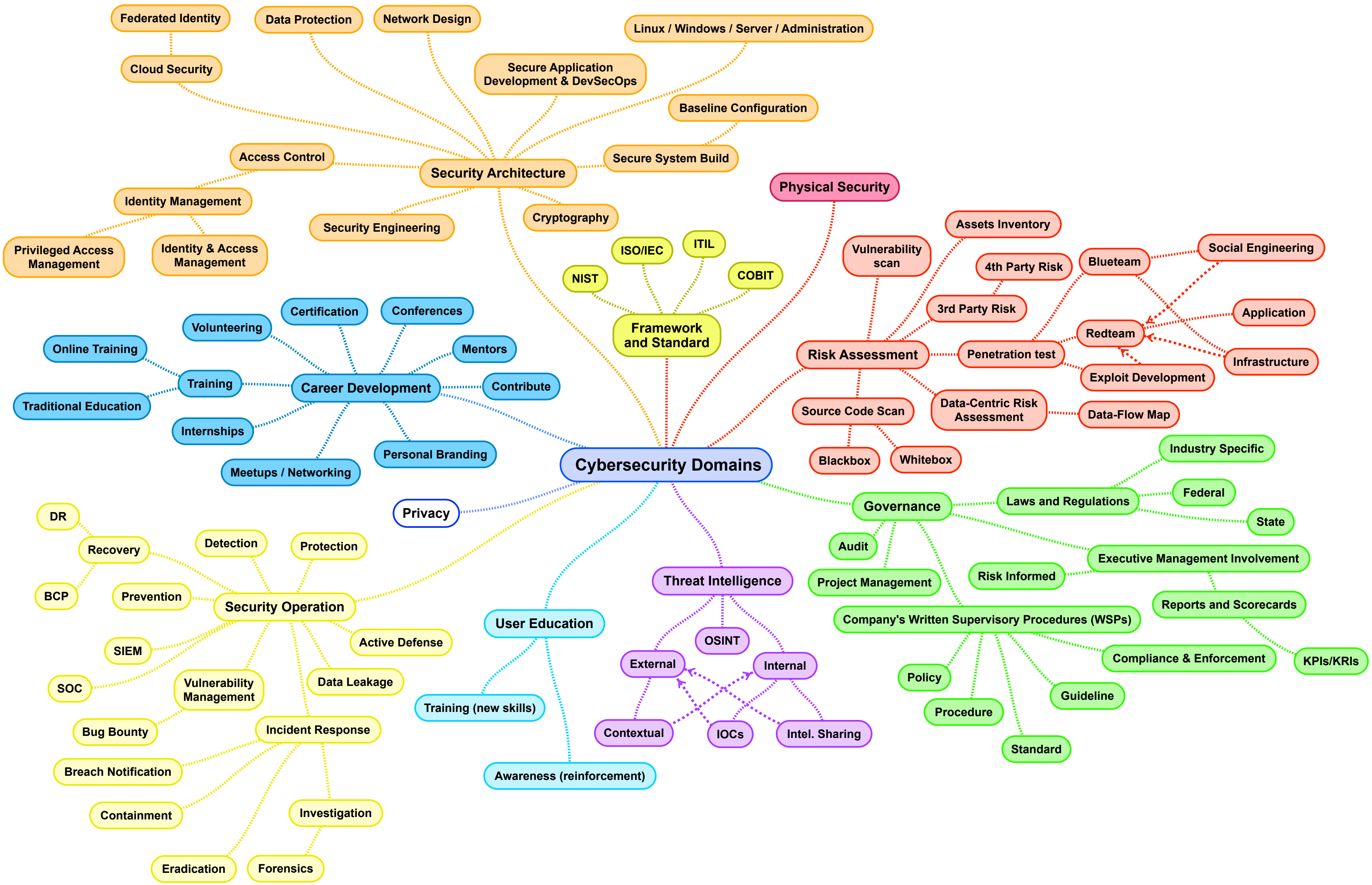
There are many types of jobs you could do within cyber security. If you look at the Cyber Security Domains diagram below you will see the many different domains that exist under the umbrella known as cyber security.



Don’t worry if you don’t understand these domains yet. That is to be expected. The key point here is that there is a broad variety of entry points and job types in this industry. Use the Cyber Security Domains diagram as a reference for what roles exist, and what you might do in those positions. As you become more familiar with cyber security these domains will make more sense to you.

The cyber security industry is a huge umbrella of many different types of roles that need different skills and that cover different domains of knowledge.

Cyber Security Domains diagram



- Cybersecurity Domains
  - Security Architecture
    - Cloud Security
      - Federated Identity
    - Data Protection
    - Network Design
    - Secure Application Development & DevSecOps
    - Linux / Windows / Server / Administration
    - Secure System Build
      - Baseline Configuration
    - Access Control
      - Identity Management
        - Privileged Access Management
        - Identity & Access Management
    - Security Engineering
    - Cryptography
  - Physical Security
  - Framework and Standard
    - NIST
    - ISO/IEC
    - ITIL
    - COBIT
  - Risk Assessment
    - Vulnerability scan
    - Assets Inventory
    - 3rd Party Risk
      - 4th Party Risk
    - Penetration test
      - Blueteam
        - Social Engineering
        - Infrastructure
      - Redteam
        - Application
        - Social Engineering
        - Infrastructure
      - Exploit Development
    - Source Code Scan
      - Blackbox
      - Whitebox
    - Data-Centric Risk Assessment
      - Data-Flow Map
  - Career Development
    - Training
      - Online Training
      - Traditional Education
    - Volunteering
    - Certification
    - Conferences
    - Mentors
    - Contribute
    - Internships
    - Meetups / Networking
    - Personal Branding
  - Privacy
  - Security Operation
    - Recovery
      - DR
      - BCP
    - Detection
    - Protection
    - Prevention
    - SIEM
    - SOC
    - Vulnerability Management
      - Bug Bounty
    - Active Defense
    - Data Leakage
    - Incident Response
      - Breach Notification
      - Containment
      - Eradication
      - Investigation
        - Forensics
  - User Education
    - Training (new skills)
    - Awareness (reinforcement)
  - Threat Intelligence
    - External
      - Contextual
    - OSINT
    - Internal
      - IOCs
      - Intel. Sharing
  - Governance
    - Laws and Regulations
      - Industry Specific
      - Federal
      - State
    - Audit
    - Project Management
    - Executive Management Involvement
      - Risk Informed
      - Reports and Scorecards
        - KPIs/KRIs
    - Company's Written Supervisory Procedures (WSPs)
      - Policy
      - Procedure
      - Standard
      - Guideline
      - Compliance & Enforcement

Most people will specialise in one or a number of domains within cyber security. Below is a list of example common roles within cyber security and possible domains the role might cover. Click on any job title below to be taken to current live job ads from Cyber Security Jobs.

Penetration Tester & Ethical Hacker

Trying to hack systems to find vulnerabilities. Reporting any weaknesses found so they can be mitigated.
Average Salary: $102,000

A penetration tester might specialise in domains such as red team, infrastructure penetration testing, or application testing, exploit development and social engineering.

Security Analyst & Specialist

Performs a variety of security analysis and defensive tasks to help prevent organizations from being compromised by attackers.
Average Salary: $85,000

Security Analysts might work in a security operating centre (SOC) and specialise in the domain of security operations and vulnerability management. Or any of the other domains within security operations. The titles of security analyst & specialist are quite general so you might find roles with these titles involved in many different domains.

Cyber Crime Analyst & Investigator

Examines digital components to determine if illegal actions have taken place. Also can respond to security incidents.
Average Salary: $85,000

This role might cover some or all of the domains such as incident response, investigations, forensics, breach notifications and containment.

Security Consultant

Advises organizations of their security posture.
Average Salary: $85,000

A consulting role can be quite varied so it’s possible they may specialise in something specific such as risk assessment or they might be more of a generalist advisor covering many domains.

Security Engineer & Architect

Designs and implements secure systems.
Average Salary: $108,000

These roles are generally within the domain of security architecture where you are designing and implementing some of the sub-domains within the architecture domain, like a secure network, access control, identity management and so on.

Freelance Consultant & Contractor

Independently advises organizations of their security posture.
Average rate: $1000 per day

A freelance consulting role can also be quite varied. The difference is you are working for yourself. Which means you will specialise in what is in demand.

Chief Information Security Officer (CISO)

This senior-level executive is responsible for establishing and maintaining enterprise security.
Average Salary: $108,000

The CISO is solidly in the domain of cyber security governance with oversight over all the other domains.

Consider what domains and roles you might be interested in, and what role you might ultimately move towards in the middle and the end of your career.

You may choose to specialise in domains such as network security, cloud, security architecture, management and governance, security operations, risk assessment, penetration testing, blue team or others. Where you specialise determines your training and certification needs.

If you were to look at the job boards in your local job market. You will notice the job specs and roles that will cover these domains.

If you are in the US then the recommended job board is Cyber Security Jobs.

Register on Cyber Security Jobs for Job Alerts immediately so you can start to recongnise the skills required in the roles that interest you.

In the UK JobServe, CyberSecurityJobsite, CWJobs and others. When you have the time, spend a few minutes looking at the jobs on these boards and you'll better understand what skills are required for certain job titles.

Key Takeaways

- The cyber security industry is a huge umbrella of many different types of roles that need different skills and cover different domains of knowledge.
- Most people will specialise in one or a number of domains within cyber security.
- Consider what domains and roles you might be interested in, and what role you might ultimately move towards in the middle and the end of your career.

2

Step

Get Educated

The StationX Accelerator Program is uniquely designed based on scientific evidence of what fosters success in the cyber security field. It's not just an educational program; it's a comprehensive success system, integrating mastermind groups, mentorship, community engagement, and the FastTrack program.

Boasting over 1,000 classes and virtual labs, the program covers a wide array of topics from hacking to AI, ensuring your skills are in line with current industry needs. The personalized study roadmap, developed by experienced mentors and accessible through an easy-to-use app, offers a guided, efficient path towards your career objectives.

What truly sets this program apart is its unlimited mentorship, providing bespoke advice and support from professionals in the field. This, along with the StationX community, offers invaluable opportunities for networking, resource sharing, and engaging in enriching discussions.

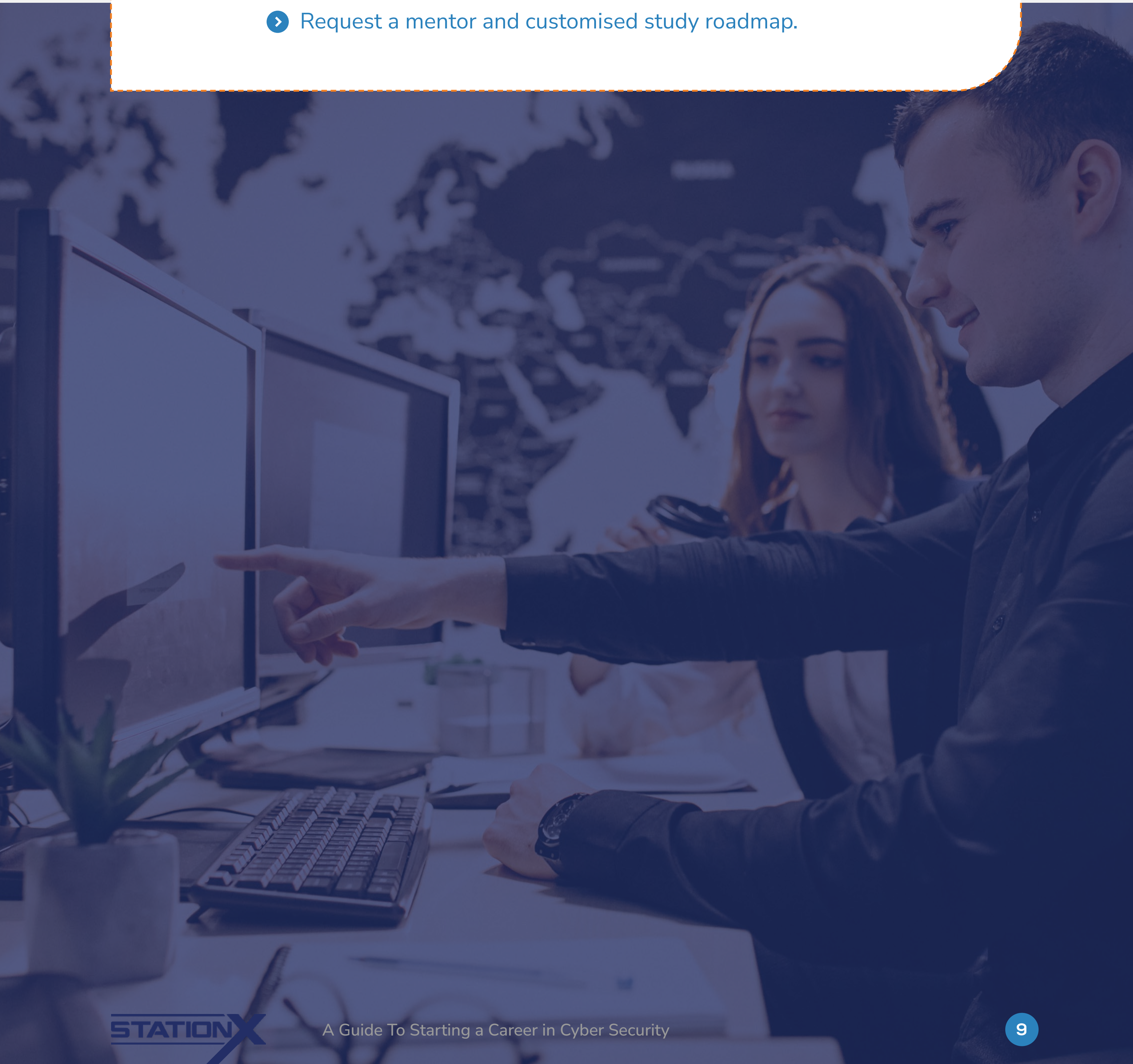
The FastTrack program within the Accelerator offers an accelerated learning curve for those eager to make rapid progress in their cyber security career. Alongside this, the StationX exam simulators are essential for preparing for crucial certifications, ensuring you're well-equipped for these important assessments.

The Career Toolkit is another standout feature, with over 50 modules that go beyond cyber security basics, covering everything from perfecting your resume to mastering job interviews, setting you up for successful job placement.

In essence, the StationX Accelerator Program is a robust, all-encompassing platform for anyone serious about pursuing a career in cyber security, blending top-notch educational content with strategies proven to drive success.

Key Takeaways

- It is no longer necessary to have a college degree, but you will need to self-educate.
- Join the StationX Cyber Security Career Accelerator.
- Request a mentor and customised study roadmap.



3

Step

Get Certified and Qualified

One of the easiest ways to educate yourself, showcase your skills and improve your employability is to acquire certificates.

In the field of cyber security, there are a number of certificates you can get that will look great on your resume or portfolio. To acquire these certificates, all you need to do is sit an exam.

By identifying a certificate you would like to get, you can narrow the focus of your education on learning only the skills required for one certificate at a time. This makes your learning path much more linear while reaching valuable milestones along the way.

At StationX, we provide specific training and practice exams to help you prepare for and pass your certification exams.

But which certificate do you start with?

Beginners Certificates:

Cyber security is a highly-skilled career which requires a solid foundation in IT, operating systems and networking. If you are starting at zero with little to no basic IT knowledge, then you need to get up to speed with the basics first.

My recommendations for anyone starting at zero is to learn your IT fundamentals first. The topics and skills you need are covered well on the courses we have for the CompTIA IT Fundamentals certificate and CompTIA A+ Core 1 & 2 certificates.

Another cornerstone to security is an understanding of networking, the Internet, cloud, routers, switches and so on. My recommendations for this topic are the CompTIA Network+ and CompTIA Cloud+ certifications.

If you are not starting at zero, these courses and certificates may be too simple for you. Skip any that are too easy unless you want the certificate for your CV/Resume/Linkedin.

Intermediate Certificates:

After you have your IT basics down, you want to get a solid overview of the important Cyber Security Domains. To do this, I recommend you take this CompTIA Security+ Course and read these other Security+ resources here.

Then what certificates you should aim to get and skills to acquire will depend on the type of roles and specialisation that interests you. You need to choose training and certificates that cover the Cyber Security Domains that are required for the roles that interest you most.

For example, if you want to become a penetration tester you might look to get the OSCP - Offensive Security Certificate or as a Chief Information Security Officer (CISO) get the CISM - Certified Information Security Manager.

Cyber Security

CompTIA Security+
(Basic level)

CompTIA CySA+
(Intermediate level)

CISSP - Certified Information Systems Security Professional
(Advanced level)

Penetration Testing

CEH - Certified Ethical Hacker
(Intermediate level)

CompTIA Pentest+
(Intermediate level)

OSCP - Offensive Security Certified Professional
(Advanced level)

GPEN - GIAC Certified Penetration Tester
(Advanced level)

GWAPT - GIAC Web Application Penetration Tester
(Advanced level)

Offensive Security Exploitation Expert (OSEE)
(Expert level)

IT Basics

CompTIA IT Fundamentals
(Entry level)

CompTIA A+ Core 1 and core 2
(Entry level)

Security Management / CISO

CISM - Certified Information Security Manager
(Advanced level)

ITIL & PRINCE 2
(Intermediate level)

Cloud

CompTIA Cloud+
(Basic level)

Microsoft Azure
(Intermediate level)

Amazon Web Services (AWS)
(Intermediate level)

Networking

CompTIA Network+
(Basic level)

Cisco CCNA
(Intermediate level)

Cisco CCNP Security
(Intermediate level)

Certificates increase your job opportunities, demonstrate knowledge and skills and are often even required just to secure an interview.

Advanced Certificates:

Long term, you should aim to pass the Certified Information Systems Security Professional (CISSP) certification. The CISSP is the closest the security industry has to a standard in certification.

CISSP requires five years of experience to achieve. But, you can take the CISSP exam without any experience (after doing CISSP training), and then you'll have six years to complete your five years of industry experience. After that, you officially submit your endorsement to become an official CISSP, and then you can start using those letters after your name. In the meantime, you can put on your resume/CV/LinkedIn you have passed the CISSP exam. This will help secure a role.

According to Zip Recruiter, the average annual pay for a CISSP Job in the US is $125,470 a year.

I recommend you to do your CISA shortly after as there is a lot of shared content, so it is easy to do both exams close together. Finally, follow those two with the CISM certificate for security management.

According to Zip Recruiter, the average annual pay for a CISM Job in the US is $137,058 a year.

Key Takeaways

- Certificates increase your job opportunities, demonstrate knowledge and skills and are often even required just to secure an interview.
- Where you choose to specialise determines what training you should do and what certificates you should get.
- Long term, you should aim to pass the Certified Information Systems Security Professional (CISSP) certification.

4 Step

Gain Hands-on Practical Experience

It's easy to gain hands-on practical experience if you go about it the right way. The first thing you must do is to set up a virtual lab. A virtual lab is a simulation of a real environment and can be used for gaining hands-on practical experience. It has never been easier and cheaper to set up a virtual lab than it is today.

Here are your options in order of least expensive to most expensive for setting up your lab.

1. VirtualBox or VMware or similar on a laptop or desktop.
2. VirtualBox or VMware or XCP-ng or similar on a local server.
3. VPS or cloud server hosted online using services such as AWS, Turnkey Linux, Linode, Digital Ocean and others.
4. A dedicated server with XCP-ng or VMware or similar running on it.

If you want to learn how to set up a lab and virtual server, I recommend "How to Create a Virtual Hacking Lab".

In order to sharpen your hands-on practical skills, it's best to study an online course while practising techniques inside of your Virtual Lab.

In your current job (if you have one) you want to ask to take on any security tasks you can, to gain experience and to have something to put on your resume. Anything at all is better than nothing, even simply changing people's passwords is worth doing to gain the experience!

Engage in the StationX Cyber Security Community. There is an active and passionate community who I guarantee would love to meet you. Talk and network with existing security professionals. Learn about the industry.

Consider internships, volunteering, and offer to do free work for businesses and charities.

Key Takeaways

- Setup a virtual lab to get hands-on experience.
- Attend meetups and network actively.
- Take on any cyber security related work you can to gain experience.

5

Step

Demonstrate your Abilities and Passion

To secure your first job, you MUST be able to demonstrate your abilities and passion for the work. To do this, I recommend you to create a public profile and use this as a vehicle to showcase your talent and demonstrate your passion for the industry.

Try doing security research, respond to Call for Papers (CFP), bug bounties (get paid for finding security errors in other systems), answer questions on the StationX community, and write security posts and papers. Contribute to open-source projects and network with the developers.

Create a public profile by writing a blog, Twitter, LinkedIn, joingin the StationX community and other social media accounts and fully document all of your work.

If you're unsure about how this all looks, you can connect with me on LinkedIn and Twitter to share with my network. Chat to experts over social media. Comment on the latest security news. Attend security conferences like DEFCON, Black Hat, RSA conference, ShmooCon, InfoSec and see if you can contribute. Network with the attendants.

Place everything relevant on your resume/CV/LinkedIn when you apply for jobs. Employers do read through all of it and maintaining a professional profile does matter.

Your resume/CV/LinkedIn demonstrates your ability, enthusiasm and passion, which will get you hired very quickly in a market that is desperate for talented individuals!

Key Takeaways

- Create a public profile documenting your skills, knowledge & passion.
- Connect and network with people at events and conferences.
- Interact with the online community. It really does make a difference.

What Next?

Throughout this guide, I've shown you 5 core steps to starting a career in Cyber Security. To repeat those steps, they are:

1. Get to know the cyber security industry and what jobs are on offer.
2. Get educated with online cyber security training and courses.
3. Gain certificates by studying for and completing exams.
4. Get hands-on practical skills by setting up a virtual lab.
5. Demonstrate your abilities and your passion.

This really is a fascinating and exciting industry. I've been working in this field now for 30 years and ever-changing technology presents new and interesting challenges every day.

I hope this is a career that interests you too. Cyber security is a very rewarding and respected occupation with an increasing skills gap and the world needs new people with an interest in cyber security more than it ever has before.

What now? I have 3 tasks that I recommend.

First, **sign up for free to the StationX community.** Once registered, update your profile, introduce yourself, and begin networking. It's important to actively engage and get involved with the community.

Second, **follow me on LinkedIn**. This will allow you to connect with my network.

Lastly, remember that when you feel ready to learn more, you are welcome to join the **StationX Cyber Security Career Accelerator** to get the skills, experience, and mentorship you need to succeed in cyber security. Our comprehensive training library, study roadmaps, mentor access, and career toolkit equip you with the knowledge and expertise to advance in the industry.

Thank you for reading and I look forward to connecting with you.

Kind regards,

Nathan House