

# LAND YOUR FIRST CYBER SECURITY JOB FAST

THE COMPLETE BLUEPRINT FOR BEGINNERS WITH NO EXPERIENCE



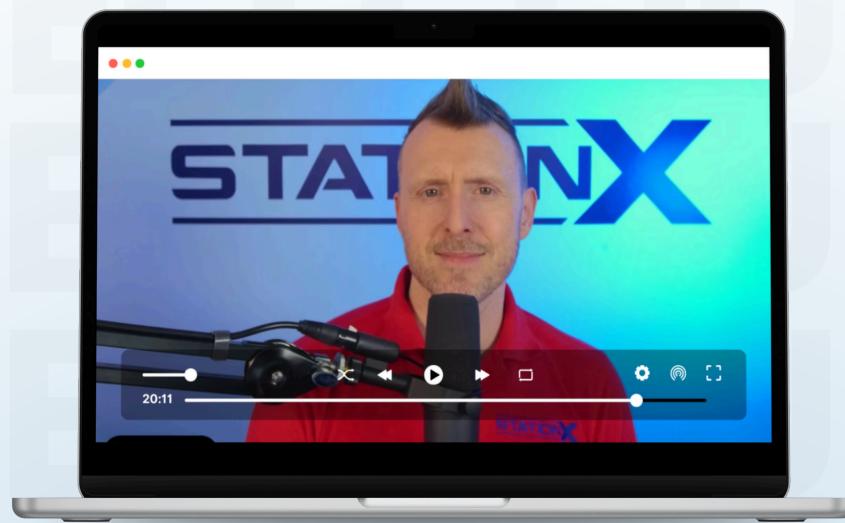
NATHAN HOUSE

STATIONX



**WAIT!**

# Get the FREE Video Course!



## PREFER WATCHING OVER READING?

Access the step-by-step **VIDEO COURSE**  
version of this book for **FREE!**

- ✓ Easy-to-follow video lessons
- ✓ Accelerate your path into cyber security

**CLAIM YOUR FREE ACCESS NOW**

<https://www.stationx.net/book-course>

# Land Your First Cyber Security Job Fast — The Complete Blueprint

The cyber security field faces a critical workforce shortage—approximately [3.4 million](#) positions remain unfilled globally. This creates an amazing opportunity for you.

By building the right skills now, you can quickly enter a field offering both job satisfaction and stability.

## How do you begin?

This guide provides five clear steps to launch your cyber security career:

1. **Explore the Industry** — Understand cyber security jobs and find your fit
2. **Get Educated** — Learn the essential technical & soft skills
3. **Get Certified** — Earn credentials that employers recognize
4. **Gain Practical Experience** — Apply your skills in real-world scenarios
5. **Show Your Value** — Demonstrate your expertise and passion

Each section includes targeted resources to accelerate your progress. The embedded links connect you to resources, videos, and articles that work.

Ready to secure your future? Turn the page.

## About the Author



**Nathan House**, is a leading cyber security expert and founder of StationX, the #1 Cyber Security Training and Career Development Platform. He has 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 break into the field.

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



# 1

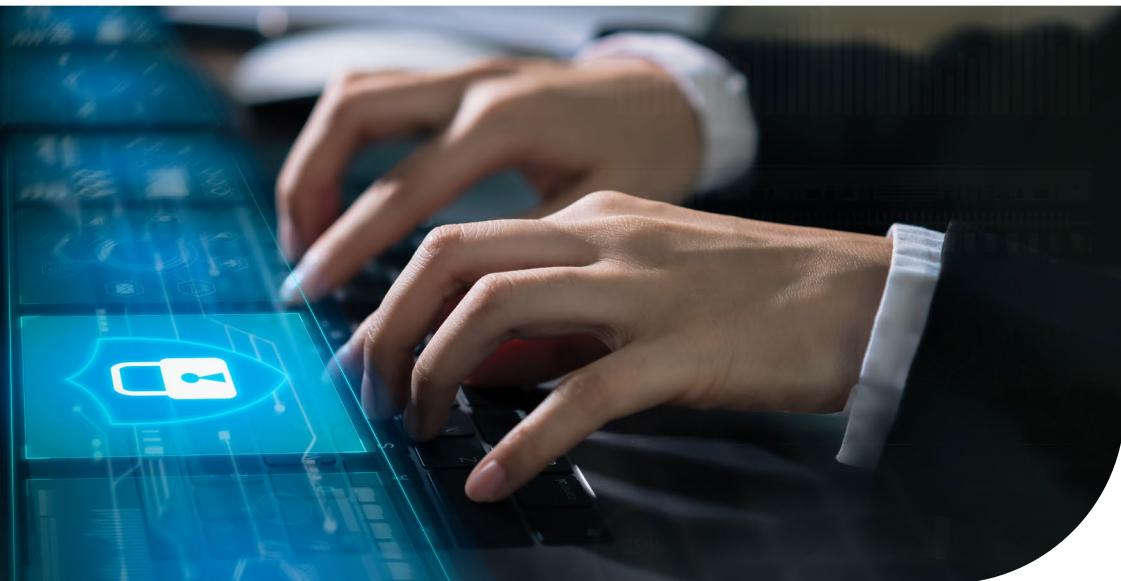
Step

## Explore the Industry — Understand cyber security jobs and find your fit

Cyber security goes beyond technical skills and hacking. It's fundamentally about managing risk, with technology serving as just one tool in a broader strategy.

### The Big Picture

Check out the Cyber Security Domains Diagram on the next page. It shows all the different specialties in the field. Don't worry if these look unfamiliar at first—that's completely normal. The important thing to remember is that you have many different ways to enter this field and various specialized roles to grow into as your career develops.



### Job Options

Look through the job list on pages 5 and 6 to see what roles are available and what each involves. As you learn about specific positions, you'll start to understand how they fit into the larger cyber security landscape.

The field offers many different types of jobs requiring various skill sets—creating opportunities for people with diverse backgrounds and strengths.

# Cyber Security Domains Diagram



## **Specialization in Cyber Security**

Most cyber security professionals focus on one or a few specialized domains rather than trying to master the entire field. Understanding these domains helps you navigate the landscape effectively and identify where your skills and interests best align.

### **Common Career Paths**

Here are some common cyber security jobs and the domains they cover. Click the title below for more information:

#### **➤ Penetration Tester & Ethical Hacker**

Trying to hack systems to find vulnerabilities. Reporting any weaknesses found so they can be fixed.

**Salary Range: \$104,000 — \$169,000+**

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

#### **➤ Security Analyst & Specialist**

Performs a variety of security analysis and defensive tasks to help prevent organizations from being compromised by attackers.

**Salary Range: \$91,000 — \$143,000+**

Security Analysts might work in a security operations 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.

**Salary Range: \$117,000 — \$175,500+**

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.

**Salary Range: \$120,000 — \$185,500+**

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

## ➤ **Security Engineer & Architect**

Designs and implements secure systems.

**Salary Range:** \$156,000 — \$234,000+

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.

**Salary Range:** \$1200 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.

**Salary Range:** \$165,000 — \$490,000+

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

## **Planning Your Professional Journey**

Consider which domains and roles match your interests and strengths—not just for entry-level positions, but for your mid-career and long-term goals. Your specialization choice directly shapes your training requirements and certification pathway.

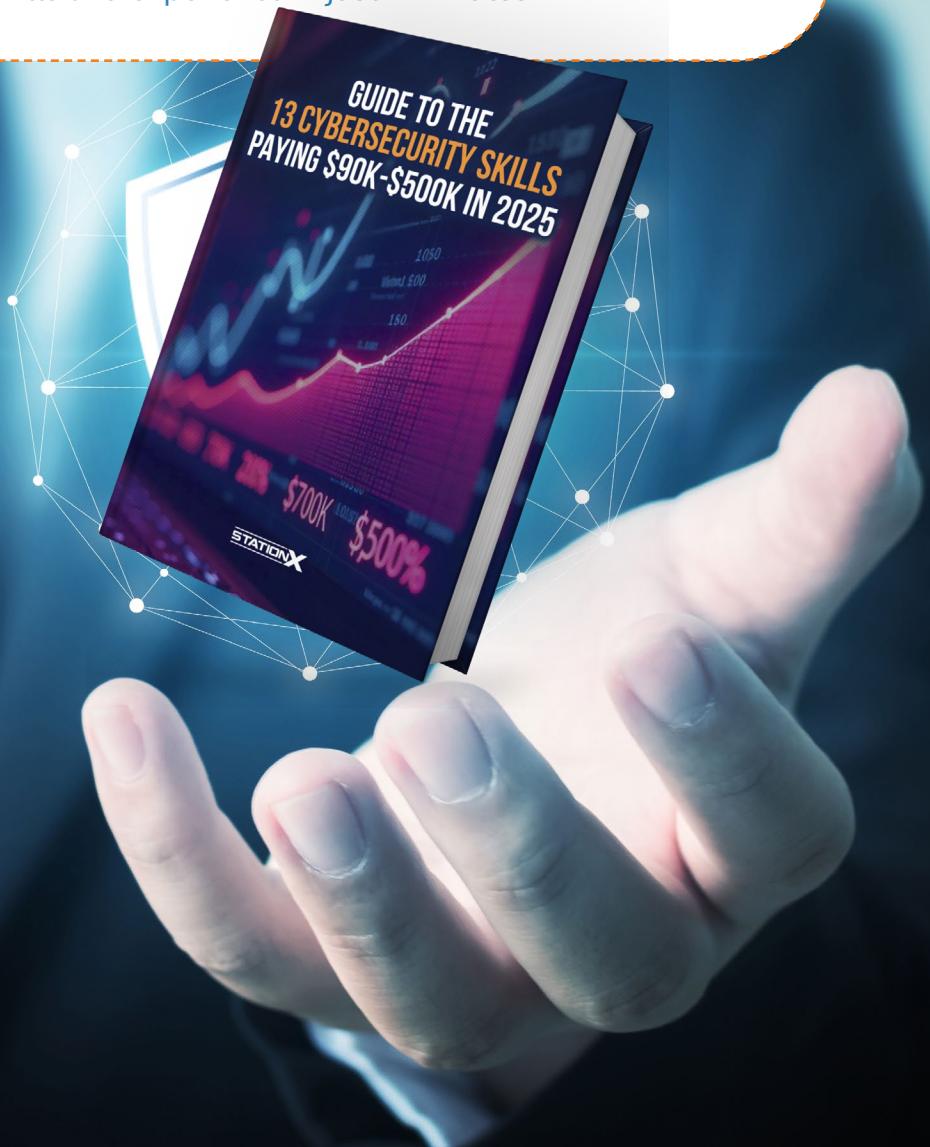
The ideal focus area balances market demand with your natural aptitudes. As you review the list above, note which areas resonate with your existing skills or spark your curiosity.



Follow the action steps below and click the title for more information.

## Action Steps

-  [\*\*\[WATCH FUNDAMENTALS VIDEO\]\*\*](#) - Explore our comprehensive introduction to cyber security essentials. Gain clarity on security domains, threat landscapes, and career opportunities in just 15 minutes.
-  [\*\*\[WATCH VIDEO\]\*\*](#) - Access “13 Cyber security Skills Paying \$90K-\$500K” and download the full report. See exactly which skills are commanding top salaries in today’s market.
-  [\*\*\[TAKE ASSESSMENT\]\*\*](#) - Complete the Cyber Security Career Match Maker to find your ideal role. Get personalized career guidance based on your unique skills and experience in just 2 minutes.



# 2

Step

## Get Educated — Learn the essential technical & soft skills

When pursuing an education, consider these pathways based on your circumstances, learning style, and career goals.

### 1. University Degree

A formal degree provides comprehensive theoretical knowledge and creates networking opportunities, though it may not always focus on practical job skills.

- > **Price:** \$30,000 - \$50,000+
- > **Time Investment:** 3-4 years
- > **Probability of Success:** Moderate to High
- > **Pros:** Structured learning environment, industry recognition, networking opportunities, broad foundation
- > **Cons:** Often theory-heavy, expensive, no work experience gained, may not keep pace with rapidly evolving threats and technologies



### 2. Hybrid Programs

These structured programs combine university-style instructor led guidance with the flexibility of self-study, typically including expert mentorship, a curated curriculum, and certification support. Some offer job guarantees and work experience (such as the [StationX Masters Program](#)).

- > **Price:** \$8,500+
- > **Time Investment:** 6-24 months
- > **Probability of Success:** Moderate to High
- > **Pros:** Industry-focused curriculum, mentorship, faster than traditional degrees, often includes practical experience and high chance of success
- > **Cons:** Quality varies significantly, less recognized than traditional degrees

### 3. Workshops and Boot Camps

Intensive, short-duration training typically run by specialized institutions. These programs are designed to rapidly build specific skills or help you earn targeted certifications. [Browse StationX bootcamps.](#)

- > **Price:** \$8,000 - \$15,000
- > **Time Investment:** Days to months
- > **Probability of Success:** Low to Moderate
- > **Pros:** Focused learning, intensive format, networking with professionals, quick completion
- > **Cons:** Limited scope, may be too brief for career changers, minimal ongoing support, no experience gained, usually need more than one
- > **Best for:** Supplementing existing knowledge or learning specific cyber security tools/techniques

### 4. Self-Study

Independent learning using a mix of affordable resources, online subscriptions, and certifications to build skills at your own pace. [Browse StationX courses.](#)

- > **Price:** \$2,500 - \$6,000 (for courses, certifications, labs, and resources)
- > **Time Investment:** 3-5 years (varies by commitment level and background)
- > **Probability of Success:** Low (without significant discipline, structure, and mentor help)
- > **Pros:** Most flexible, cost-effective, customizable to interests
- > **Cons:** Requires exceptional self-discipline, no formal guidance, potential knowledge gaps, no experience gained, slow due to lack of focus
- > **Best for:** Those on a low budget, with technical backgrounds, or highly self-motivated learners with a clear understand of what they need to do



**Certified Information Systems Security Professional (CISSP)**



**CompTIA Security+**



**Offensive Security Certified Professional (OSCP)**



**CompTIA PenTest+**

Path	Cost (USD)	Time Investment	Success Likelihood	Strengths	Drawbacks	Ideal For	Overall ★
<b>University Degree</b>	\$30 k – \$50 k+	3 – 4 years	Moderate → High	<ul style="list-style-type: none"> <li>Structured, accredited learning</li> <li>Broad theoretical base</li> <li>Strong alumni / industry networking</li> </ul>	<ul style="list-style-type: none"> <li>Heavy on theory, less hands-on</li> <li>High tuition cost</li> <li>No work experience gained</li> <li>Curriculum can lag behind new threats</li> </ul>	Those who want a traditional academic credential and campus experience	★★★★★
<b>Hybrid Program (e.g., StationX Master's)</b>	\$8.5 k+	6 – 24 months	Moderate → High	<ul style="list-style-type: none"> <li>Industry-focused, current curriculum</li> <li>Mentorship &amp; job-search support</li> <li>Practical projects / possible work experience</li> </ul>	<ul style="list-style-type: none"> <li>Recognition varies by provider</li> <li>Quality not uniform</li> </ul>	Career changers or up-skillers seeking guided, faster, job-ready preparation	★★★★★
<b>Workshops / Boot Camps</b>	\$8 k – \$15 k	Days → Months	Low → Moderate	<ul style="list-style-type: none"> <li>Highly focused, intensive learning</li> <li>Rapid completion &amp; certification prep</li> <li>Networking with peers</li> </ul>	<ul style="list-style-type: none"> <li>Narrow scope; may need several</li> <li>Minimal ongoing support</li> <li>Little or no real-world experience</li> </ul>	Filling specific skill gaps or earning targeted cyber security certs	★★★★★
<b>Self-Study</b>	\$2.5 k – \$6 k	3 – 5 years	Low	<ul style="list-style-type: none"> <li>Maximum flexibility &amp; low cost</li> <li>Tailored to personal interests</li> <li>Learn at your own pace</li> </ul>	<ul style="list-style-type: none"> <li>Requires exceptional discipline</li> <li>No formal guidance / feedback</li> <li>Risk of knowledge gaps &amp; slower progress</li> </ul>	Highly motivated, budget-conscious learners with a clear study plan	★★★★★

Follow the action steps below and click the title for more information.

## Action Steps

- ▶👉 **[SET YOUR LEARNING BUDGET]** - Take time to establish a realistic financial plan for your cyber security education. Remember, skills pay the bills—investing in yourself delivers the highest return on investment of any expenditure. Consider your ideal timeline, preferred learning pace, and carefully evaluate the success rates of different educational pathways to make an informed decision.
- ▶👉 **[SECURE A MENTOR]** - Establish a relationship with an experienced cyber security professional who can provide personalized guidance, insights, and accountability. Statistics show that professionals with mentors are 5x more likely to advance in their careers and earn significantly higher salaries. StationX offers structured mentorship programs tailored to your specific cyber security path.
- ▶👉 **[JOIN A MASTERMIND GROUP]** - Participate in a structured community of like-minded cyber security professionals who share challenges, solutions, and opportunities. Research indicates that mastermind participants achieve their professional goals 91% more frequently than solo learners. StationX provides exclusive mastermind groups led by industry veterans to accelerate your progress.
- ▶👉 **[JOIN WAITLIST]** - Secure your spot on Station X's exclusive Masters Program. Get priority access to the only program that gives you a job guarantee and work experience.

# 3

Step

## Get Certified — Earn credentials that employers recognize

Looking to demonstrate your skills and improve job prospects? Certifications deliver tangible value in cyber security.

Certifications enhance your resume and professional profile, but remember—they're just one component of your career toolkit, not a guaranteed job ticket.

### Focus Your Learnings

Select one certification target initially. This creates a clear learning path focused exactly on what you need to master.

StationX provides:

- [Complete cyber security training programs](#)
- [Live instructor-led boot camps](#)
- [Self-paced online training](#)
- [Exam voucher discounts \(up to 30% savings\)](#)

### Choosing Your First Certification

#### For Beginners

Cyber security requires foundational knowledge in IT basics, operating systems, and networks. If these areas are new to you:

Start with IT fundamentals through [CompTIA Tech+](#) and [CompTIA A+ Core 1 & 2](#) courses.

Build network understanding through [CompTIA Network+](#) and [Cloud+](#) programs.

#### For IT Professionals

If you already possess IT and networking experience, consider skipping foundational certifications unless you specifically want them on your resume.



# Intermediate Certificates

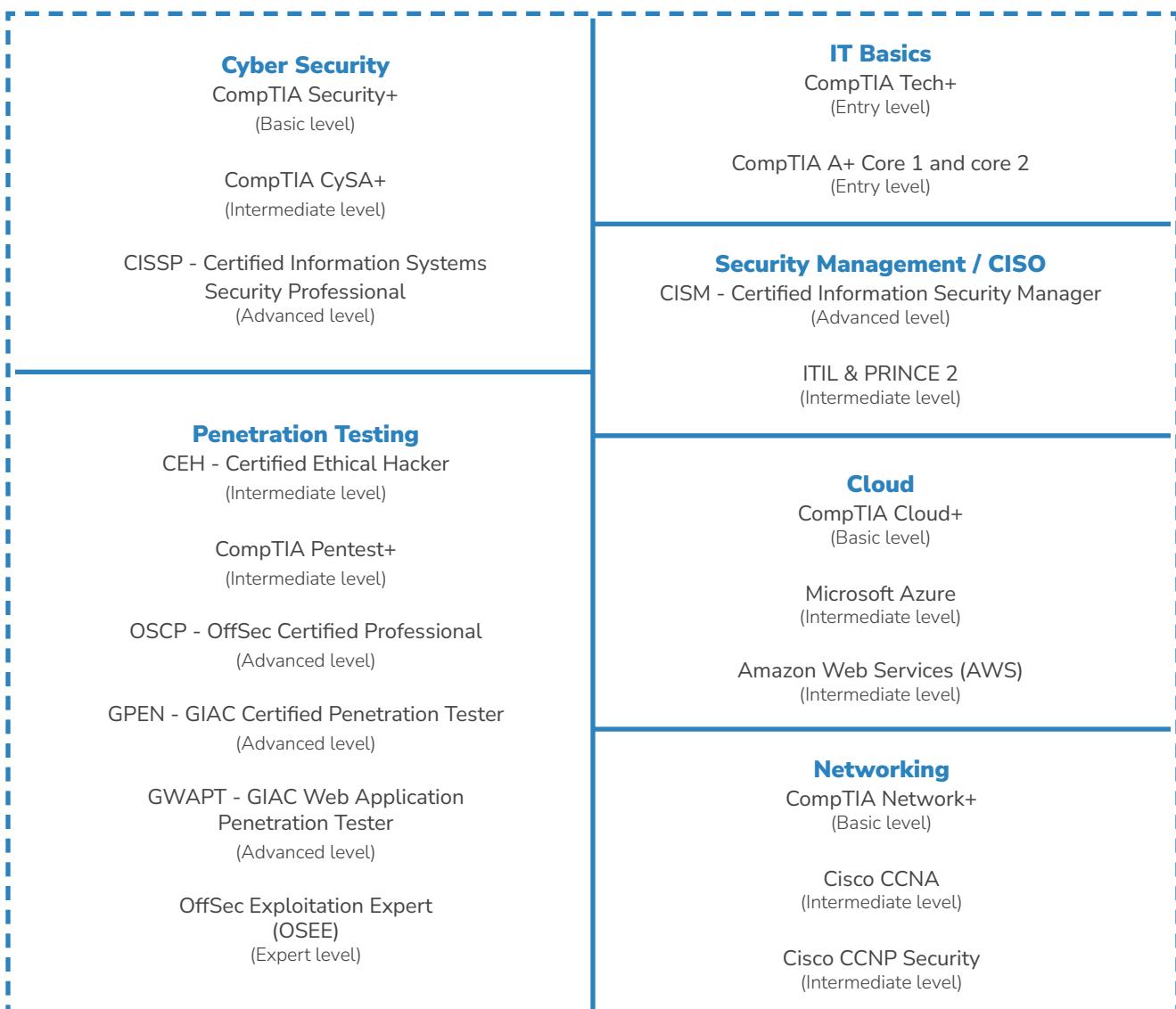
After establishing IT and networking foundations, focus on cyber security fundamentals.

Our [CompTIA Security+ Course](#) provides comprehensive coverage, complemented by free [Security+ guides](#) on our website.

Next, align your certification path with your career goals. Select training that develops skills specific to your target position:

- For security operations roles, consider the [CompTIA CySA+ \(Cyber Security Analyst\)](#)
- For network security positions, the [Cisco CCNA](#) provides relevant specialized knowledge

Well-chosen certifications significantly expand employment opportunities, validate technical competencies, and frequently serve as minimum requirements for interview consideration.



# Advanced Certificates:

The ★ [CISSP \(Certified Information Systems Security Professional\)](#) represents the industry's most requested credential.

While it requires five years of professional experience, you can:

1. Complete the examination immediately after training
2. Earn the required experience within six years
3. Hold Associate status in the interim (include this designation on your resume)

CISSP holders command an average annual salary of \$171,775 according to Glassdoor.

Our specialized [podcast](#) & [blog](#) provides valuable CISSP insights for examination success.

Consider pursuing ★ [CISA \(Certified Information Systems Auditor\)](#) shortly after CISSP completion. The substantial content overlap creates efficiency when these certifications are obtained in sequence. [CISA articles here](#).

For ethical hacking specialists, the ★ [OSCP \(OffSec Security Certificate\)](#) provides hands-on penetration testing validation. Our dedicated [OSCP](#) podcast & [blog](#) offers effective preparation strategies.

For those targeting security management roles, the ★ [CISM \(Certified Information Security Manager\)](#) certification delivers exceptional value. CISM holders earn approximately \$157,189 annually based on Skillsoft research. [CISM articles here](#).

## Action Steps

-  [\[EXPLORE CERTIFICATION MAP\]](#) - Navigate the complete cyber security certification landscape with our comprehensive visual diagram. Understand different focus areas, complexity levels, and career paths at a glance.
-  [\[FIND YOUR IDEAL CERTIFICATION\]](#) - Take our quick quiz to discover which cyber security certification perfectly matches your skills, experience level, and career aspirations. Stop guessing and start your targeted certification journey today.
-  [\[ACCESS FREE RESOURCES\]](#) - Explore our library of hundreds of expert-written guides covering all major cyber security certifications. Get valuable exam prep strategies and career insights at no cost.
-  [\[SAVE 30% ON EXAM FEES\]](#) - Access exclusive CompTIA certification vouchers at significantly reduced prices. Why pay full price when you can save up to 30% on your certification exams? Limited vouchers available.

# 4

Step

## Gain Practical Experience — Apply your skills in real-world scenarios

My strong recommendation: Start by setting up your own local lab. It's a critical part of your learning journey. You'll gain practical experience with virtual machines, operating systems, networking, and troubleshooting—things you must know in the field.

### Build Your Own Lab (Highly Recommended)

Best for: Real-world skill-building, deep understanding, total control

Platform	OS Support	Cost	Setup	Notes
VirtualBox	Windows, macOS (Intel), Linux	Free	Easy	Great for beginners. Doesn't support Apple Silicon. Performance is moderate.
VMware Workstation Player	Windows, Linux	Free	Easy	More stable than VirtualBox. Good performance. Great networking features.
VMware Fusion	macOS (Intel)	Free (Player) / Paid (Pro)	Easy	Better integration with macOS. Not ideal for Apple Silicon. Performance is good.
Parallels Desktop	macOS (Intel & Apple Silicon)	Paid	Very easy	Best option for M1/M2 Macs. Seamless experience. Very good performance.
UTM	macOS (Apple Silicon)	Free	Easy	Solid free alternative to Parallels. Performance is moderate.
TurnKey Linux	Any (via VM)	Free	Very easy	Prebuilt VMs for apps like LAMP and WordPress. Saves setup time. Good performance.
VulnHub / Metasploitable / DVWA / Juice Shop	Any (via VM)	Free	Moderate	Must download and import. Great for offensive practice. Performance depends on host system.

#### ✓ Pros:

- Deep learning through hands-on setup
- Totally free if you already have a machine
- Works offline, no cloud required
- More realistic than browser-only labs

#### ✗ Cons:

- Initial setup takes time
- Needs moderate system resources (RAM/CPU)
- You'll need to learn how to troubleshoot

## VPS or Cloud Labs (Easy, Flexible, Remote)

Best for: Remote access, cloud experience, minimal local setup

Platforms	Cost	Ease	When to use it	Notes
DigitalOcean / Linode / Vultr	\$5-\$20/mo	Easy	When you want remote labs or can't run VMs locally	Quick setup, fixed pricing, good documentation. Watch out: no real free tier, not full-feature cloud platforms.
AWS EC2 / Lightsail	\$0-\$100+/mo	Medium	When practicing cloud security or AWS tools	Lets you learn IAM, VPC, S3, etc. Watch out: billing is complex, easy to forget and overspend.
Hetzner / OVH (Bare Metal)	\$30-\$100+/mo	Medium	When you want a full-time remote lab server	Full control and flexibility. Watch out: ongoing cost, unnecessary for most beginners.

Cloud labs are great—but not always necessary for beginners. Here's when it makes sense:

### ✓ Pros

- Easy to deploy virtual machines with full remote access
- Great for learning cloud security concepts and services (IAM, S3, networking)
- Useful for red team setups (C2 infrastructure, phishing servers, VPNs)
- Ideal when local machine resources are limited or shared labs are needed
- Access labs from anywhere, on any device

### ✗ Cons

- Ongoing monthly costs, especially if machines are left running
- Not essential for beginners focused on tool usage or local setup
- Cloud billing models can be confusing and lead to unexpected charges
- Overkill for basic practice environments that work locally
- Some platforms restrict the use of certain hacking tools



Google Cloud



IBM Cloud

## Online Lab Platforms (Plug-and-Play)

**Best for:** Immediate access to structured, guided cyber security exercises without the need for local setup.

Platform	When	Cost	Notes
StationX Labs	For job-focused training with full support ecosystem	Only available within programs	2,000 Labs & 28,000 courses designed to help land a job, not just learn skills. Includes lab books for building your own labs. Paid access includes mentorship, career support, and practical paths.
TryHackMe	For guided skill-building in offensive or defensive security	\$14/month or \$126/year	Gamified, good for learning specific tools and techniques. Focused on building hacking and blue team skills. Watch out: free content is limited compared to paid tiers.
Hack The Box	For guided skill-building in offensive or defensive security	\$14/month or \$135/year. VIP+ at \$20/month or \$203/year.	Gamified, good for learning specific tools and techniques. Focused on building hacking and blue team skills. Watch out: free content is limited compared to paid tiers.
CyberDefenders	For blue team training and incident response practice	Free	Excellent for defensive scenarios and SOC-style investigations. Watch out: fewer structured learning paths.
OverTheWire / PicoCTF	For sharpening problem-solving and Linux command-line skills	Free	Lightweight, great for foundational challenges. Watch out: lacks full lab environments or practical system interaction.

### ✓ Pros

- Instant access—no setup required
- Useful for focused tool or topic practice
- Accessible on any OS or device
- Some platforms offer gamified learning to keep engagement high
- Complements your own lab well as a secondary resource

### ✗ Cons

- Limited control over the environment
- Doesn't teach system setup, networking, or troubleshooting
- Not all platforms are aligned with job-readiness
- Paid tiers typically needed for full content access
- Can give a false sense of readiness if used alone

# The Value of Projects

Hands-on projects are essential for developing practical cyber security skills. Include these experiences prominently on your resume to demonstrate technical abilities to potential employers.

Choose projects that align with your target role and highlight them in job applications. Explore StationX's [guide to cyber security projects](#) for effective resume-building options.

Practical experience is essential in cyber security, which is why the [StationX Masters Program](#) makes it a core component of our curriculum. We've designed three progressive levels of hands-on experience to build your expertise systematically.

## StationX Master's Program

Our masters program integrates practical experience through a three-tier approach:

- **Foundation building** - develop skills through cyber ranges, interactive labs, and scenario-based training
- **Supervised application** - apply knowledge in guided projects with expert feedback
- **Real-world implementation** - gain legitimate work experience through the StationX consultancy

This structured progression provides valuable resume experience and interview talking points.

The collage illustrates the three-tier approach of the StationX Master's Program:

- Foundation building:** Two technicians working in a server room, representing scenario-based training and practical experience.
- Supervised application:** A technician working at a computer monitor displaying code, representing guided projects with expert feedback.
- Real-world implementation:** A screenshot of the 'CompTIA' software interface showing a task to connect a monitor to a computer, and a 3D floor plan of a corporate office layout with various workstations and server racks, representing legitimate work experience through the StationX consultancy.

# Breaking the Experience Barrier

The experience paradox in cyber security—needing experience to get hired but needing a job to gain experience—can be overcome.

Strategic self-initiated projects demonstrate your capabilities and problem-solving skills to employers. For professional-grade experience in industry environments, consider the [StationX Masters program](#) as your pathway to career readiness.

Alternatively, implement the experience strategies highlighted in this section.

## Action Steps

- **[BUILD VIRTUAL LABS]** - Set up your own cyber security testing environment to gain crucial hands-on experience. Focus on labs specific to your target role—defensive security labs for blue team positions or hacking labs for penetration testing careers. Tailor your practical learning to maximize career relevance.
- **[COMPLETE REAL PROJECTS]** - Work on guided cyber security projects that solve actual problems. Build an impressive portfolio that demonstrates your capabilities and makes your resume stand out to hiring managers.
- **[GAIN VOLUNTEER EXPERIENCE]** - Explore volunteer opportunities and internships in the cyber security field. Get real-world experience while making valuable industry connections that can lead to job offers.
- **[APPLY TO MASTERS PROGRAM]** - Submit your application to StationX's prestigious Masters Program. Get structured work experience, personalized mentorship, and a clear path to high-paying cyber security positions.

# 5

Step

## Show Your Value — Demonstrate your expertise and passion

To land your first cybersecurity job, you must demonstrate both your abilities and enthusiasm. Build a public professional profile that highlights your talents and dedication to the field.

### Take Action Relevant to Your Target Role

Choose activities aligned with your career goals:

- Conduct and document security research
- Participate in [bug bounty](#) programs (ideal for aspiring penetration testers)
- Answer technical questions in the [StationX Community](#)
- Write [security posts](#) and [white papers](#)
- Contribute to open-source security projects

These are examples of activities—select those most relevant to your chosen specialty.

### Build Your Professional Presence

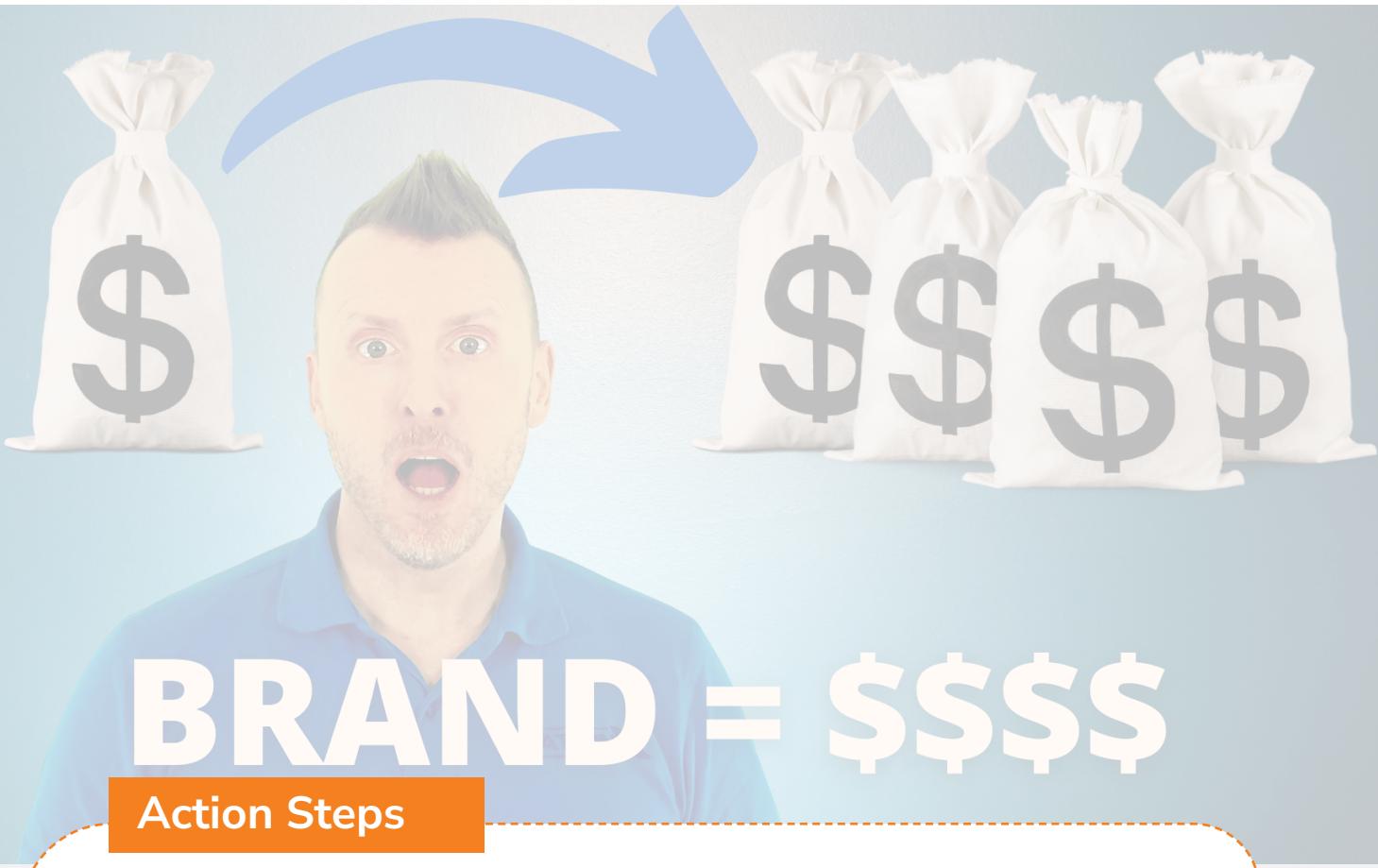
- Create and maintain a focused blog
- Develop professional profiles on LinkedIn and X
- Join the [StationX community](#) and relevant forums
- Connect with me to access my professional network -----> ([LinkedIn](#) and [X](#))
- Engage with security experts on social media

## Network Strategically

- Attend major security conferences ([DEFCON](#), [Black Hat](#), [RSA](#))
- Find local cyber security [meetups](#) in your area
- Focus on building meaningful face-to-face connections
- Explore the [top 10 cyber security conferences](#) for networking opportunities

## Job Search Strategy

Highlight all your skills, training, and practical experiences on your [resume](#) and LinkedIn profile. These demonstrate your capabilities, motivation, and passion—qualities that lead to quick hiring in this talent-hungry field.



### Action Steps

- **[LISTEN TO INDUSTRY EXPERTS]** - Watch our exclusive podcast featuring Ken Underhill, the industry expert on personal branding in cyber security. Gain insider knowledge on what truly sets successful candidates apart in this competitive field.
- **[ELEVATE YOUR PERSONAL BRAND]** - Invest time in crafting a compelling professional narrative and polished resume that showcases your unique value proposition. Stand out from the crowd with strategic personal marketing that gets you noticed.
- **[NETWORK STRATEGICALLY]** - Connect with cyber security professionals both locally and online with clear purpose and goals. Build meaningful relationships in the industry that can lead to mentorship, job referrals, and career advancement opportunities.

# What Next?

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

1. Get to know the cyber security industry and what jobs are on offer.
2. Get educated through cyber security training courses.
3. Gain certificates by studying for and completing exams.
4. Get hands-on practical experience.
5. Demonstrate your abilities and your passion.

You now stand at a crossroads: follow the clear steps I've laid out for real change, or continue with old habits that haven't worked.

As Theodore Roosevelt wisely put it, '**In any moment of decision, the best thing you can do is the right thing, the next best is the wrong thing, and the worst thing you can do is nothing.**'

**Click & follow for more help & advice!**



Nathan House