The 90-Day Cybersecurity Roadmap

From zero to hired. No degree required.

By Carter Perez | 11 certifications | Cybersecurity Software Engineer | Creator of **CertGames.com**

New to cyber? Follow this start to finish. Already in the field and trying to level up? Skip to Phase 2 and the 10 career tracks at the end, those are built for you.

This is the exact path I would follow if I was starting from zero today with no degree, no experience, and no connections.

I know because I did it.

This roadmap breaks the process into four phases. Each phase builds on the last. Follow it in order, put in the hours, and you will be a competitive candidate in **90 days.**

Phase 1: Get Your First Certification

Weeks 1-5 | Goal: Pass CompTIA Security+

The **Security+** is the single most important certification in cybersecurity. Every entry-level job posting asks for it. It proves you understand the fundamentals, and it will open more doors than anything else you do in these 90 days.

Your daily routine (1-2 hours):

First 30 minutes: Learn one objective. Pick one objective from the Security+ exam outline and actually learn it. Professor Messer's free YouTube series covers every objective in short videos. Watch one, take a few notes, move on.

Next 45-60 minutes: Practice questions. Do at least 25 questions per session. This is where the actual learning happens. You will get questions wrong, and that's the point. Every wrong answer is a gap in your knowledge that you just found before the exam did.

Last 15 minutes: Review what you missed. Go back through every question you got wrong. Read the explanation. Understand WHY the right answer is right and why yours was wrong. This step is what separates people who pass from people who don't.

Resources:

Professor Messer's Security+ videos (free on YouTube, covers every exam objective)

CompTIA Security+ exam objectives checklist (free PDF from CompTIA's website, print it out and check off objectives as you study them)

CertGames.com (most realistic pratice questions and learn modules, daily routine.)

That daily routine above (learn an objective, drill questions, review your misses) is the entire loop, and it's exactly what I built **CertGames** to run. The Learn lessons walk you through each Security+ objective in plain English, then you drill from 25,000+ questions (1,250 for the Security+), and the analytics track every wrong answer so your "review what you missed" step happens for you. It turns *studying into a game* instead of a grind: XP, levels, streaks, leaderboards, and training games like Acronym Avalanche and Protocol Blitz, so you actually open it every day. **FREE**

How to know you're ready to test:

When you're consistently scoring 80% or higher on full practice exams, book your test. Not before. **CertGames** gives you a readiness score that tells you when you're actually at that line, so you're not guessing. A lot of people book too early because they're impatient. Don't waste **$400** on a retake.

> *Weeks 1-2 should feel hard. Weeks 3-4 should feel like things are clicking. Week 5 is review and test prep. If you need a 6th week, take it.*

Phase 2: Build Real Projects

Weeks 6-8 | Goal: 3 real cybersecurity projects you can defend in an interview

A certification says you know the theory. A project says you can actually do the work. Most applicants show up with a certification and nothing else. You're going to show up with proof.

Build these three projects:

1. Honeypot Network A multi-protocol honeypot that simulates real services (SSH, HTTP, FTP, MySQL) and captures every attacker interaction. It maps behavior to MITRE ATT&CK techniques, extracts threat intelligence, and visualizes everything through a real-time dashboard. This shows you understand how attackers operate and how defenders detect them.

2. Binary Analysis Tool A static analysis engine that parses executable files, runs them through an analysis pipeline (imports, strings, entropy, disassembly), and produces a threat score with MITRE ATT&CK mapping. This is what malware analysts do on day one of every investigation. Shows you can triage suspicious files and explain what you found.

3. Credential Enumerator A tool that scans systems for exposed credentials: SSH keys, cloud provider configs, browser data, shell history secrets, and database passwords. Classifies findings by severity based on file permissions and exposure risk. Shows you understand post-access enumeration, which is one of the most common real-world attack techniques.

All three have full source code AND learning documentation in my open-source repo (**3500+ stars**): ***github.com/CarterPerez-dev/Cybersecurity-Projects***

The learn/ folder walks you through every concept behind each tool, not just the code but the security principles that make it work. Study it, build your own version, modify it, break it, fix it. When an interviewer asks you about your project, you need to be able to explain it like you built it yourself. Because you did.

If you'd rather be guided than reverse-engineer a repo: **CertGames** now has ***guided Project courses*** that walk you through building real security tools from scratch, step by step, with the concepts explained as you go. Same outcome, less getting stuck. You finish with something on your **GitHub** you can actually talk through, which is the whole point of this phase.

Phase 3: Fix Your Resume and LinkedIn

Week 9 | Goal: A resume and profile that get responses

Most people in cybersecurity have terrible resumes. They list responsibilities instead of results. They use the wrong keywords. Recruiters spend about 6 seconds on each one. Yours needs to survive those 6 seconds.

Your resume:

- A clear target role at the top: "SOC Analyst" or "Cybersecurity Analyst", not "seeking opportunities in the IT field"
- Security+ certification listed prominently (it's your biggest asset right now)
- Your projects described by what they DO, not what they ARE. "Built a honeypot network that captures attacker sessions, maps behavior to MITRE ATT&CK, and generates real-time threat intelligence" beats "Created a Python project for security"
- Use the STAR method for experience and project bullets: Situation, Task, Action, Result. What was the problem, what did you do, what happened? Example: "Deployed a multi-protocol honeypot that captured 500+ attacker sessions in 30 days, identifying 12 unique MITRE ATT&CK techniques and generating blocklists for 200+ malicious IPs."
- One page. No exceptions. If you have 20 years of experience, still one page.

If you're staring at a blank page, **CertGames** has a resume tool that turns your projects and certification into ***STAR-method*** bullets like the ones above. Use it as a starting draft, then make every line yours.

Your LinkedIn:

Headline = what you do, not your current job title. "Cybersecurity Analyst | CompTIA Security+ | Building tools to detect threats" is better than "Student at State University"

Security+ in the certifications section

GitHub projects linked in the Featured section

A short About section written like a person, not a press release

Professional photo (phone camera against a plain wall works fine)

Keywords that matter for entry-level cyber roles:

SIEM, incident response, vulnerability management, log analysis, threat detection, SOC, IDS/IPS, firewall, endpoint security, CompTIA Security+, Splunk, Wireshark, Nessus, NIST, MITRE ATT&CK

Sprinkle these naturally throughout your resume and LinkedIn. Don't keyword-stuff, but make sure they're present. Recruiters search for these terms.

Phase 4: Apply, Network, and Interview

Weeks 10-12 | Goal: 10 applications per day, build connections, land an offer

Where to apply:

LinkedIn Jobs (filter for "SOC analyst", "cybersecurity analyst", "security analyst", "IT security")

Indeed (same filters, broader reach)

ClearanceJobs (if you're US-based, many cyber roles offer or require security clearance. These jobs pay more and have less competition because the clearance is a barrier to entry.)

Company career pages directly (especially MSPs and MSSPs. They hire more juniors than enterprise companies and you'll get exposure to dozens of different environments.)

> **PRO TIP (this one is the cheat code):** Most companies pay their own employees a referral bonus for bringing in a good hire. When I was on the inside, ours ran $1,000 to $3,000 depending on the job title. Here's why that matters to you: referring someone costs the employee nothing if it doesn't work out, and a referred application lands at the top of the pile, right under internal candidates. So don't just cold-apply into the void. Before you apply, find people who actually work at the company on LinkedIn, message them, and say: "I think I'd be a strong fit for this opening. Would you be open to referring me in?" You make them money, they move your resume to the front. It is one of the single highest-leverage moves in this entire roadmap.

Roles to target:

SOC Analyst (Tier 1), Security Analyst, Cybersecurity Analyst, IT Security Specialist, Information Security Analyst. Don't limit yourself to exact title matches. Read the job descriptions. If you meet 60-70% of the requirements, apply.

Network. Seriously.

Cold applications only get you so far. Most jobs get filled through connections, referrals, and people who already know your name. You need to be doing both: applying AND networking at the same time.

- Go to local cybersecurity meetups and job fairs. Show up, introduce yourself, hand out your resume. These events exist in almost every metro area.
- Reach out to people on LinkedIn who work in roles you want. Don't ask for a job. Ask for 15 minutes of their time: "I'm getting into cybersecurity and would love to hear about your path." People are surprisingly willing to help.
- Join cybersecurity Discord servers, Reddit communities (r/cybersecurity, r/ITCareerQuestions), and local ISSA/ISACA/OWASP chapters. Be active. Answer questions. Help others. The people you meet here will DM you when their team is hiring.
- Post about your journey on LinkedIn. Share what you're learning, your projects, your Security+ pass. Hiring managers scroll LinkedIn too.

How to talk about your projects in interviews:

Don't say "I built a honeypot." Say "I built a multi-protocol honeypot network that simulates SSH, HTTP, and FTP services to attract real attackers. It captures every session, maps behavior to MITRE ATT&CK techniques, and generates threat intelligence I can export as blocklists. I can walk you through the architecture and what I learned about how attackers actually operate." Connect every project back to real-world security work.

Expect questions about Security+ topics. If you studied properly in Phase 1, you already know this material. The interview is not a second exam. It's a conversation about whether you can think like a security professional.

> *Apply every single day. 10 applications minimum. Most won't respond. That's normal. You only need one yes.*

Beyond 90 Days: 10 Career Paths

This roadmap gets you hired. But cybersecurity is a deep field with many directions you can take after you land that first role. I created detailed certification roadmaps for 10 career tracks, all free and open source:

SOC Analyst • Penetration Tester • Security Engineer • Incident Responder • Cloud Security Engineer • GRC Analyst • Threat Intelligence Analyst • Application Security • Security Architect • Network Engineer

github.com/CarterPerez-dev/Cybersecurity-Projects/ROADMAPS

Want it more guided than a markdown file? I also built these career roadmaps into **CertGames**, so you can follow your track step by step and line the right certifications up against the practice and projects you already have going.

One place to run all of this:

Every phase above points back to the same platform on purpose. **CertGames** is the engine I built so you don't have to duct-tape ten free tools together to do what this roadmap asks.

> **Phase 1:** Learn lessons that teach every objective, 25,000+ practice questions to drill them, analytics that track your weak areas, and a readiness score that tells you when you're actually ready to test.
>
> **Phase 2:** Guided Project courses that walk you through building real security tools from scratch, so you finish with portfolio proof you can defend.
>
> **Phase 3:** A resume tool that turns your certification and projects into recruiter-ready bullets.

It covers 20 certifications: CompTIA (A+, Network+, Security+, CySA+, PenTest+, Linux+, Cloud+, Data+, Server+, Security X, SecAI+), ISC2 (CISSP, CC), AWS (Cloud Practitioner, Solutions Architect), Microsoft (AZ-900, AZ-500) and Cisco (CCNA, CCNP). And it's built to make studying something you want to open every day (gamified learning - exactly how I studied) instead of something you force yourself through.

And if you never join CertGames, you're still covered.

Look back at everything this roadmap pointed you to. The open-source repo with all the projects and the learn/ folder. The 10 career roadmaps. The practice questions. The resources. A lot of it I built myself, and all of it is free. That's not bait. You can run this entire 90 days without spending a dollar and get hired, and I'd be genuinely happy if you did.

CertGames is just the optimized version: the same path with the grind taken out and everything in one place. It's there for people who like my work and want it done with them instead of figuring it out alone. If that's you, come in. If not, you already have everything you need above. ***Go use it.***

> ***Good luck!*** 🧙

certgames.com | github.com/CarterPerez-dev | @carterperez.dev