T H E C Y B E R S E C U R I S T

HOW TO BREAK INTO CYBERSECURITY FROM A NON-TRADITIONAL BACKGROUND

The step-by-step breakdown: what to study, what to skip, and what hiring managers actually look for.

Dr. Olutobi Oyinlade | Crownstone Strategy Group
PhD • AI Engineer • Cybersecurity Strategist

crownstone.io | @thecybersecurist

First, a reality check.

You're reading this because you're thinking about cybersecurity but you didn't come from a traditional tech background. Maybe you're in healthcare, education, finance, operations, or the military. Maybe you're self-taught in tech but don't have the degree.

I'm going to give you the version of this guide I wish someone had given me. Not the "just get certified" advice you've already heard. The real sequence. What actually matters, what doesn't, and how to make your non-traditional background your biggest advantage instead of your biggest insecurity.

I made this transition myself: research science to cloud engineering to cybersecurity to AI. None of it was planned. All of it compounded. So this isn't theory. It's what I've lived, and what I've seen work for other people making the same move.

Step 1: Understand what cybersecurity actually is (and isn't).

Most people picture hackers in hoodies when they think cybersecurity. That's a fraction of the field. The industry is enormous, and most of the jobs don't require you to write code.

Cybersecurity is about protecting systems, data, and people from threats. That includes:

- Governance, Risk, and Compliance (GRC): policies, frameworks, audits
- Security Operations (SOC): monitoring, detection, incident response
- Identity and Access Management (IAM): controlling who can access what
- Security Awareness: training humans to not be the weakest link
- Cloud Security: securing infrastructure in AWS, Azure, GCP
- Application Security: finding vulnerabilities in software
- Threat Intelligence: understanding who's attacking and how

Why this matters for you: GRC, security awareness, and IAM are the most accessible entry points for career changers. They reward communication skills, process thinking, and attention to detail. Things you probably already have.

Step 2: Audit what you already bring.

Your background isn't a gap. It's a translation problem. Here's how to reframe what you've already done:

Your Background	Cybersecurity Translation	Best-Fit Roles
Nursing / Healthcare	Triage, incident response mindset, working under pressure, HIPAA compliance awareness	GRC, Incident Response, Healthcare Security
Teaching / Education	Breaking down complexity, security awareness training, documentation	Security Awareness, Technical Writing, GRC
Accounting / Finance	Audit thinking, risk assessment, compliance, attention to detail	GRC, Compliance, Risk Management
Project Management	Cross-team coordination, governance, dependency tracking, stakeholder communication	GRC, Security Program Management
Military / Law Enforcement	Discipline, threat assessment, chain of custody, classified information handling	Threat Intelligence, SOC, Incident Response
Customer Support / Ops	Troubleshooting, process documentation, pattern recognition, empathy under pressure	SOC Analyst, IAM, Security Operations

Action: Write down 3 specific situations from your current or past work where you identified a problem before it became visible, communicated something complex to a non-expert, or improved a process. These are your cybersecurity stories. You'll use them in interviews.

Step 3: Build the right foundation (and skip the noise).

The internet will tell you to get 5 certifications, learn Python, build a SIEM, and start a blog. All at once. That's a recipe for burnout. Here's the actual sequence that works:

Phase 1: Vocabulary and Foundations (Months 1–3)

Your first job is to stop feeling lost when people talk about cybersecurity. You need the vocabulary.

Pick one:

1. **CompTIA Security+**: $404 for the exam. The industry standard entry cert. Takes about 3 months of focused study. Use Professor Messer (free on YouTube) or Jason Dion's course on Udemy (~$15 on sale).
2. **Google Cybersecurity Certificate**: On Coursera. About 6 months at a relaxed pace, faster if you push. Covers broad fundamentals. Good if you want a structured learning path.

Do not try to do both at once. Pick one, finish it, move on.

Phase 2: Hands-On Skills (Months 3–6)

Certification gives you vocabulary. Hands-on gives you something to talk about in interviews.

1. **Build a home lab.** You don't need expensive equipment. A free-tier AWS account, VirtualBox on your laptop, or TryHackMe/Hack The Box (free tiers available). The goal: get comfortable with real tools in a real environment.
2. **Pick a platform and do 20–30 exercises.** TryHackMe has structured "paths" for beginners. The "Intro to Cyber Security" and "Pre-Security" paths are solid starting points.
3. **Document what you do.** Every lab you build, every exercise you finish, write a short summary of what you learned. Put it on LinkedIn, a blog, or even just a Google Doc. This becomes your portfolio.

Phase 3: Specialize and Position (Months 6–9)

By now you have vocabulary, some hands-on experience, and (ideally) a certification. Time to pick a direction.

1. **Choose 1–2 areas to go deeper.** Don't try to learn everything. If GRC interests you, start reading NIST frameworks. If SOC work appeals to you, practice with Splunk (free tier) or learn basic log analysis. If cloud security calls to you, get an AWS or Azure fundamentals cert.
2. **Start telling your story publicly.** Post on LinkedIn about what you're learning. Not performatively. Just share what's surprising, confusing, or interesting. Hiring managers notice this.
3. **Connect with people in the field.** Join cybersecurity groups, local meetups (BSides events are free or cheap), Discord communities, and LinkedIn groups. Don't pitch yourself. Ask questions. Be genuinely curious.

Step 4: Know what hiring managers actually look for.

I've been on both sides of the hiring table. Here's what most career advice gets wrong: hiring managers at the entry level are not looking for someone who knows everything. They're looking for someone who:

1. Can learn fast and doesn't need to be told twice.
2. Communicates clearly. Can explain what they did and why.
3. Shows evidence of self-directed learning (labs, write-ups, projects).
4. Has a genuine interest in the field, not just the salary.
5. Is coachable. Will ask when they don't know something instead of guessing.

What beats a CS degree in an interview: A home lab you can walk them through. A write-up of a CTF challenge or TryHackMe room you completed. A clear explanation of how your previous career taught you to think about risk, systems, or communication. Questions that show you've researched the company and the role.

What doesn't help as much as people think: Stacking certifications before applying for anything. A polished resume with no projects or evidence. Waiting until you feel "ready" (you won't, so apply anyway). Applying to 200 jobs with the same generic resume.

Step 5: The job search (without losing your mind).

Your resume

- Lead with a skills summary, not a chronological job history
- Include a "Projects" section: your home lab, certifications, write-ups
- Translate your previous experience into security language (see the table in Step 2)
- Keep it to one page. Hiring managers spend about 7 seconds on a first pass.

Where to apply

Target roles with these titles: SOC Analyst I, Junior Security Analyst, GRC Analyst, IT Security Analyst, Compliance Analyst, IAM Analyst, Security Operations Specialist.

Look at these companies and sectors:

- Managed Security Service Providers (MSSPs): they hire volume and train people up

- Healthcare and financial services companies: regulatory pressure creates constant demand
- Government and defense contractors: security clearance + entry-level roles available
- Any mid-size company (200–2,500 employees) that just hired their first CISO. They're building teams from scratch.

The interview

Expect a mix of behavioral and technical questions. The behavioral ones are where career changers often have the biggest advantage.

Be ready to answer:

- "Why cybersecurity?" Be specific. Connect it to something real from your experience, not "I'm passionate about protecting people."
- "Walk me through your home lab." They want to see that you can explain what you built and why.
- "How would you handle a situation where you don't know the answer?" The right answer involves asking, researching, and escalating. Not guessing.
- "What's a security topic you've been learning about recently?" Have a real answer. Something specific. Not "AI in security" but more like "I've been reading about how identity-based attacks bypass traditional perimeter defenses."

Step 6: The 90-day plan (so you keep momentum).

Pin this somewhere visible. Adjust the timeline to your life, but keep the sequence.

Timeframe	Focus	Deliverable
Weeks 1–4	Pick your certification path. Start studying.	Study plan created. 30 min/day minimum.
Weeks 5–8	Continue cert study. Set up a basic home lab.	Home lab running. First 5 TryHackMe rooms done.
Weeks 9–12	Finish cert or hit the 75% mark. Write your first LinkedIn post about what you're learning.	1 certification (or exam scheduled). 1 public post. Resume draft started.

Months 4–6	Hands-on depth. Choose a specialization. Network.	10+ lab exercises documented. 2–3 LinkedIn connections in the field. Resume finalized.
Months 6–9	Apply. Interview. Iterate.	Applying to 5–10 targeted roles/week. Interview practice done.

What to skip (seriously).

The internet makes this path look harder than it is by telling you to do everything at once. Here's what you can skip or save for later:

Skip This	Why
Learning to code first	You don't need Python to get an entry-level security role. You can learn scripting after you're employed. It's nice to have, not required.
Getting a master's degree	A master's won't help you get your first role. Experience and certifications matter more at entry level. Consider it later for leadership positions.
Stacking multiple certifications before applying	One cert + hands-on projects beats 3 certs with no practical experience. Get Security+ and start applying.
Building a personal website/brand first	LinkedIn is enough. Don't spend 2 months designing a portfolio site when you could be learning and applying.
Waiting for the "perfect" time	There isn't one. Start with 30 minutes a day. Momentum compounds.

The real numbers.

Because I promised no gatekeeping:

Item	Cost	Notes
CompTIA Security+ exam	$404	Sometimes discounted through employer or military programs
Professor Messer study material	Free	YouTube. Comprehensive. This is genuinely all you need. I used it and it is good!

Jason Dion Udemy course	~$15	Wait for Udemy sales, which happen constantly
TryHackMe (free tier)	Free	Premium is $10/month if you want more labs
Google Cybersecurity Certificate	~$49/month	Coursera subscription. Financial aid available.
Home lab (VirtualBox + free OS images)	Free	Runs on any laptop made in the last 5 years
AWS free tier account	Free for 12 months	Enough to learn cloud security fundamentals
BSides conference	Free–$25	Best networking in cybersecurity. No corporate gatekeeping.

Total realistic cost to break in: $400–$500. That's the Security+ exam and a Udemy course. Everything else has a free path.

One last thing.

3.5 million cybersecurity positions are unfilled globally. The industry doesn't need more people with the same background. It needs people who think differently. People who've navigated complex systems in healthcare, education, finance, government, and service industries.

Your non-traditional path isn't a weakness. It's the thing that will make you see what everyone else misses.

Stop waiting until you feel ready. Start with 30 minutes today.

Want more? Follow @thecybersecurist on LinkedIn and Instagram for weekly breakdowns on cybersecurity careers, AI, and practical security frameworks.

Questions? DM me or comment on any post. No question is too basic. This page is a judgment-free zone.

— Dr. Tobi Oyinlade | The Cybersecurist