



CYBER COMPLIANCE ACADEMY

Break Into Cybersecurity: The Starter Guide

5 things you need to know before you spend another hour
studying

Written by a Senior GRC Cybersecurity Analyst

FREE EDITION

EDUCATE · COMPLY · PROTECT

CYBER-COMPLIANCE-ACADEMY.COM

Before You Spend Another Hour Studying

Most people trying to break into cybersecurity fall into the same trap: they consume content for months, stack certifications, and still don't get callbacks. It's not because they're not smart enough. It's because the standard advice floating around online is generic, incomplete, and often written by people who never actually worked the job.

This short guide gives you five things to understand before you go any further, whether you're just starting out or you've already got a cert or two and feel stuck. It's written by a Senior GRC Cybersecurity Analyst who has done this work and sat on the hiring side of the table.

ONE QUICK NOTE

This is the free starter version. It'll get you pointed in the right direction. If you want the full system, projects, 90-day plan, templates, and progress checklist, that's covered at the end.

What's actually inside

Five things, and only five. Not because there's nothing else worth knowing, but because these are the five that create the most wasted time and false starts when people get them wrong. Get these right first, and everything else you learn after this will click into place a lot faster.

- The myths keeping people stuck in a loop of studying without ever applying
- How to pick a lane in a field that's really eight different careers wearing one name
- Which certification actually matters when you're just getting started
- Why proof beats credentials, and what that means for what you do next
- Where entry-level roles actually get posted, since most people are searching the wrong titles

Who this is for

This is written for anyone trying to break into cybersecurity without an inside connection, whether that's someone starting completely from scratch or someone who already has a cert or two and still isn't getting callbacks. If that's you, keep reading.

Why this matters right now

The entry-level cybersecurity job market is more competitive than it was a few years ago, which means the margin for wasted effort is smaller than ever. Every month spent chasing the wrong certification or applying with a generic resume is a month a more prepared candidate is using to actually get noticed. The good news is that most of your competition is making the same handful of mistakes covered in this guide, which means fixing them puts you ahead of most people applying for the same roles.

1. Five Myths Keeping You Stuck

You need to be a hacker or love coding

Most cybersecurity jobs, especially in GRC (governance, risk, and compliance), involve almost no coding. You need to understand risk, controls, documentation, and how to communicate with both technical and non-technical people.

You need a pile of certifications first

Certifications prove you can pass a test. They don't prove you can do the job, and hiring managers know it. One relevant cert plus real evidence of applied skill beats five certs and nothing to show for it.

You have to start in help desk or IT for years first

This used to be closer to true. It's less true now, especially for GRC roles, which value writing, analytical thinking, and attention to detail more than deep technical troubleshooting experience.

REALITY CHECK

Nobody is going to hand you a job because you finished a course. Employers hire people who can show, not just tell, that they understand the work.

You need a computer science degree

Plenty of people in GRC roles come from business, healthcare administration, the military, or no degree at all. What matters more is whether you can demonstrate you understand risk and process, not what your diploma says.

You have to move to a big city for opportunities

Remote and hybrid GRC roles are common, especially outside of cleared defense work. The work is documentation and analysis heavy, not hands-on-keyboard incident response, which makes it one of the more remote-friendly corners of the field.

THE PATTERN HERE

Almost every myth on this list comes from applying advice meant for one lane of cybersecurity (usually SOC or pentesting) to the entire field. Once you pick a lane, most of these myths stop applying to you at all.

2. Pick Your Lane

Cybersecurity isn't one job, it's a collection of very different careers. Here's a quick look at the field.

Lane	What you actually do	Good fit if you...
GRC	Assess systems against frameworks, write risk assessments, support audits	Like writing and structured thinking, don't need to love code
SOC Analyst	Monitor alerts, triage incidents, work shifts	Like fast-paced, reactive work. CCNA is a common starting cert for this lane.
Penetration Testing	Simulate attacks to find vulnerabilities	Love hands-on technical hacking
Cloud Security	Secure cloud infrastructure and identity	Have or want cloud/IT background
Identity & Access Management	Manage who has access to what, access reviews, least privilege	Like process-driven work across many teams
Application Security	Review code and applications for vulnerabilities	Have or want a development background
Incident Response / DFIR	Investigate breaches after they happen	Like investigative, detail-heavy work
Privacy / Data Protection	Ensure data handling meets regulations like GDPR	Like legal/regulatory reasoning mixed with technical understanding

THE HONEST RECOMMENDATION

If you're torn, default to GRC. It's less saturated with beginner content, less technically gatekept, and it's the lane where a strong portfolio piece can do more heavy lifting than almost any other track.

You don't have to pick forever

Your first job in this field is not your career. GRC analysts move into audit, security architecture, privacy, and even leadership. SOC analysts move into threat hunting or GRC. Pick a lane to get in the door, not a lane you're locked into for 20 years. The full guide breaks down what a typical day looks like in each of these lanes if you want more detail before deciding.

QUICK GUT CHECK

Do you enjoy writing and explaining things in plain language, or do you enjoy building and breaking things hands-on? The first points toward GRC or privacy. The second points toward pentesting, AppSec, or cloud security. That one question resolves most people's indecision.

3. Certifications: Start Broad, Then Specialize

People burn months debating certifications. Here's the short version.

CompTIA Security+ is the most common starting point for most people, it's broadly recognized and referenced as a baseline requirement in a lot of job postings. But it's not the only reasonable place to start. If you're headed toward networking-heavy security work, starting with CCNA instead can make sense. The right starting cert depends on the lane you're targeting.

Domain	Certification
General	Security+ is the most common starting point. If you're a true beginner who wants a structured, guided path that walks the basics through step by step, start with the Google Cybersecurity Certificate.
Networking	CCNA, Network+
GRC / Compliance	CySA+, CGRC

Domain	Certification
Cloud	AWS Cloud Practitioner, Azure AZ-900
Offensive Security	PenTest+, OSCP

One more to know about, even though it's not for right now: CISSP is the senior-level standard. Worth it once you have a few years of real experience behind you (years 3-5), not a starting cert.

DON'T DO THIS

Don't stack ten certs back to back with nothing else to show. 3 to 5 relevant certs paired with real project work is a reasonable sweet spot early in your career.

4. Proof Beats Credentials

This is the single biggest thing separating candidates who get callbacks from candidates who don't. Anyone can say "I understand NIST 800-53." Almost nobody applying for entry-level roles can show it.

The fix: build one small, real work sample. Pick a fictional company and document how a handful of security controls would be implemented for it. Even 10-15 well-documented controls is a legitimate, impressive artifact that most other applicants simply won't have.

What this looks like in practice

Control: AC-2 (Account Management)

Implementation: New accounts are provisioned through a documented request and approval workflow. Access is reviewed quarterly by system owners.

Evidence: Access review logs, account provisioning tickets

That's one control, written up in about four lines. Repeat that pattern across 10-15 controls and you have a real portfolio piece that almost none of your competition will have. The full guide walks through this project step by step, along with two more like it.

5. Job Titles to Search For

Entry-level GRC roles hide behind a lot of different titles. If you only search "GRC Analyst" you'll miss most of the openings.

- Information Security Analyst
- Compliance Analyst
- IT Risk Analyst
- Security Compliance Specialist
- Junior GRC Analyst / GRC Associate
- Third-Party Risk Analyst

Company career pages for regulated industries (healthcare, finance, insurance, SaaS companies pursuing SOC 2) tend to have consistent GRC hiring needs. Don't ignore mid-size companies either, a 200-person healthcare SaaS company often has just as real a GRC need as a Fortune 500, with less competition for the role.

Want the Full System?

This starter guide covers the fundamentals. The full guide, The Cybersecurity Fast Track, is the complete step-by-step system: everything you need to actually execute, not just understand the theory.

What's inside The Cybersecurity Fast Track

- ✓ The full 90-day, week-by-week sprint plan
- ✓ Three portfolio projects with worked examples (control documentation, risk assessment, gap analysis)
- ✓ Resume and LinkedIn rebuild guidance with real examples
- ✓ 5 real interview scenarios with what they're actually testing
- ✓ Fill-in worksheets and a full master progress checklist
- ✓ Glossary, salary expectations, and a job title cheat sheet

Get the full guide

Get it at cyber-compliance-academy.com

Join the Cyber Compliance Academy Discord

Free community with recurring content built for people on exactly this path:

Mock Scenario Monday · Watchdog Wednesday · Flashcard Friday

Join at discord.gg/DzyXJHaSpE

More free resources

Videos, podcast episodes, and everything else: cyber-compliance-academy.com

BEFORE YOU GO

The gap between people who break into this field and people who stay stuck isn't talent. It's whether they actually do the work instead of just reading about it. Whichever path you take from here, start now, not once you feel ready.

Cyber Compliance Academy · Educate. Comply. Protect.