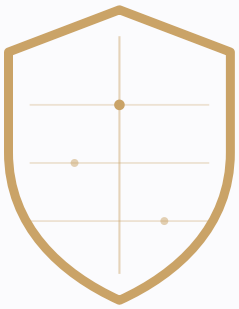
cyberwithjohann



FREE · 2026 EDITION

The Cybersecurity Career Roadmap.

One page that ends the confusion. The five real ways into cybersecurity, what to learn in what order, and how to turn it into your first job.

JOHANN LAHOUD · OFFENSIVE SECURITY LEAD · ISO 27001 · CEH

The Cybersecurity Career Roadmap.

A structured path from total beginner to your first role in cybersecurity. No prior experience assumed. No tabs to drown in. Just the sequence.

“You do not need to know everything to begin. You only need to know what comes first.”

CONTENTS

What's inside.

BEFORE YOU BEGIN

How to use this roadmap.

This is not a list of tools to download or certs to collect. It is a way of thinking about how a cybersecurity career is actually built, in the order it is built.

READ THIS FIRST

Most people try to enter cybersecurity backwards. They chase tools, hoard certifications, and binge tutorials, hoping a career emerges from volume. It rarely does. What emerges is a confused beginner with 500 open tabs and no direction. This roadmap fixes the one thing that actually keeps people out: **no sequence.**

THE FOUR MOVES

01 **See the whole game.**
Understand the field and the five real ways in before you spend a cent or an hour.

02 **Choose one path.**
Commit to a single direction that fits how you think. Not all five. One.

03 **Build the skills under it.**
Foundations first, then the path-specific layer. In order. No skipping.

04 **Turn learning into proof.**
A documented portfolio beats a stack of certificates every single time.

The people who get in fastest are not the smartest.
They are the ones who stop guessing and follow an order.

01 · THE HONEST PART

The real reason you feel stuck.

Let me tell you how almost everyone starts. Maybe it is exactly how you started.

You decided cybersecurity was the move. Good pay, real demand, a field that matters. So you opened YouTube. One creator said start with the SOC. The next swore by OSCP. A third said cloud is the only future. A fourth told you to learn to code first. A fifth said coding does not matter at all.

So you did what any reasonable person does. You collected. A course here, a free lab there, twelve browser tabs, three Discord servers, a certification roadmap with forty boxes on it. You worked hard. You watched hours of content. And months later you felt **exactly as lost as the day you started.**

HERE IS THE TRUTH NOBODY SAYS

You were never behind. You were never incapable.
You were being sent in circles by an internet that hands beginners infinite advice and zero sequence.

I know this because I lived it. When I started, the field felt enormous and I doubted, constantly, whether I belonged. What I eventually learned is that nobody feels ready at the start. The people who make it are simply the ones who find an order and refuse to stop.

This roadmap is that order.
The next 15 pages are the map I wish someone had handed me.

What cybersecurity actually is.

Forget the hoodie-in-a-dark-room image. Cybersecurity is the work of keeping digital systems, the data inside them, and the people who depend on them, safe from harm.

Nearly everything now runs on connected systems: banking, hospitals, power, government, your phone. That created enormous value and enormous risk. The global workforce gap runs into the millions of unfilled roles, which is why employers increasingly hire on demonstrated skill, not just degrees. For someone starting today, that is a rare and genuine advantage.

THE ONE IDEA THAT UNLOCKS THE FIELD

Tools detect. Humans decide.

Software can flag an anomaly. It cannot understand context, weigh business risk, anticipate an adversary, or explain to a frightened executive what to do next. That judgement is human, and it is why this career resists automation and rewards people from every background, technical and not.

FOUR KINDS OF PEOPLE THE FIELD NEEDS

Investigators	Like piecing scattered clues into a picture.	SOC · INTEL · DFIR
Builders	Like making systems run and automating the rest.	ENG · CLOUD
Breakers	Like puzzles and finding the gap nobody noticed.	PENTEST · RED
Communicators	Like strategy, writing, and working with people.	GRC · RISK

Only one of those four is about “hacking.” Cybersecurity is far bigger than the stereotype, and that is the good news.

Five real ways in. You only need one.

Here is the move that separates people who get hired from people who stay stuck: they stop trying to learn all of cybersecurity and commit to **one entry path.**

These five are chosen because they are in high demand, open to career-changers and beginners, scalable into long careers, and valuable even without a university degree. Read all five.

01 **SOC Analyst** — the most common front door

You watch, detect, and respond to threats in real time. The classic first job in cyber.

02 **GRC & Risk Specialist** — the strategic, business-facing path

Where security meets the law, the boardroom, and the business. Little to no coding.

03 **Penetration Tester** — the offensive, hands-on path

You attack systems legally, with permission, to find the gaps before the criminals do.

04 **Security Engineer** — the builder and defender path

You design and run the architecture that keeps attackers out in the first place.

05 **Threat Intelligence Analyst** — the investigative path

You study how attackers think and move, and turn chaos into foresight.

A door you walk through beats five doors you stand in front of.

Same structure, five times.

Each path gets one page, built the same way, so you can compare them honestly and feel where you belong. Here is what each page tells you.

WHAT YOU DO	The actual day-to-day, in plain language. The feel of the work, not the job-ad version.
BEST FOR	The kind of person who thrives here, so you can recognise yourself or rule it out.
PAY RANGE	Realistic entry and experienced figures. Ranges, not promises. They vary by region and sector.
START TODAY	The exact free first steps you can take this week to begin building toward the role.

A NOTE ON THE PAY FIGURES

Salaries are honest ranges drawn from entry to experienced levels across the US, UK, and EU. They move with region, industry, and certification. Finance, healthcare, and government tend to pay more. Treat them as direction, not a contract. **Always verify current local figures before any decision.**

Read all five even if one already calls to you.

The contrast is what turns a guess into a decision you can defend in an interview.

● SOC ANALYST

SOC Analyst.

Watch, detect, respond. The door most people walk through.

A Security Operations Center analyst is the first line of defence. You monitor alerts in real time, investigate the suspicious ones, and escalate the genuine threats with a clear timeline. The work is a queue: separate the meaningful few signals from the noisy many, quickly and accurately. It is the most accessible high-growth entry point in the entire field, and it teaches you fundamentals that transfer everywhere.

BEST FOR

Logical thinkers and investigators who like structure and routine. Early-career people and IT technicians moving into security who want hands-on work without deep programming upfront.

GROWTH PATH

SOC Tier 1 → Tier 2 / Threat Hunter → Incident Responder → SOC Manager or Security Architect.

REALISTIC PAY

REGION	ENTRY LEVEL	EXPERIENCED
United States	$55k – $80k	$85k – $110k
United Kingdom	£35k – £55k	£60k – £85k
Germany / NL	€40k – €60k	€65k – €90k
Remote / global	$35k – $65k	up to $85k+

START TODAY — FREE

- ☑ Build a free lab on TryHackMe, LetsDefend, or Blue Team Labs Online
- ☑ Learn Wireshark and basic log analysis until anomalies stand out
- ☑ Practice with Splunk (free tier) or the ELK Stack
- ☑ Read incident writeups from CrowdStrike, SANS, and Mandiant

● GRC & RISK

GRC & Risk.

Where security meets the business, the law, and the boardroom.

Governance, Risk and Compliance is the strategic side of security. You make sure an organisation's policies and systems meet internal standards and external regulations like GDPR, ISO 27001, and DORA. The work is people and documents, not terminals: risk assessments, audits, clear writing that turns technical detail into decisions leadership can act on. It is one of the most accessible and stable entry points, and it is often overlooked by beginners chasing the hacking image.

BEST FOR

Communicators, organisers, and detail-oriented thinkers. Career switchers from business, finance, law, or operations. Anyone drawn to strategy as much as tools.

GROWTH PATH

GRC Analyst → Senior Risk Analyst → GRC Manager → Information Security Officer → CISO.

REALISTIC PAY

REGION	ENTRY LEVEL	EXPERIENCED
United States	$65k – $95k	$100k – $140k
United Kingdom	£40k – £65k	£70k – £90k
Germany / NL	€50k – €80k	€85k – €110k
Remote / global	$40k – $70k	$85k+

START TODAY — FREE

- ☑ Study the NIST Cybersecurity Framework (free)
- ☑ Download the ISO 27001 controls and map them to simple IT examples
- ☑ Learn the common audits: SOC 2, ISO 27001, PCI DSS
- ☑ Practice writing a sample policy, then a one-page risk assessment

● PENETRATION TESTER

Penetration Tester.

Protect by breaking first. Hack legally, with permission.

A penetration tester, or ethical hacker, simulates real attacks on applications, systems, and networks to find weaknesses before criminals do. You think like an attacker to expose blind spots, then write a report clear enough that the gaps actually get fixed. It is highly technical, creative, and hands-on, and beginners are often surprised how much of it is methodical documentation and writing. The best testers are not the ones with the flashiest exploits, but the ones whose reports drive real change.

BEST FOR

Problem solvers, builders, and tinkerers. Creatives who love puzzles and real-world scenarios. Self-motivated learners willing to experiment, fail, and try again.

GROWTH PATH

Junior Pentester → Mid / AppSec → Red Team Operator → Senior Consultant or Researcher.

REALISTIC PAY

REGION	ENTRY LEVEL	EXPERIENCED
United States	$80k – $110k	$120k – $160k
United Kingdom	£45k – £70k	£75k – £110k
Germany / NL	€50k – €90k	€95k – €130k
Freelance / bounty	project based	$200/hr+

START TODAY — FREE

- ☑ Build skills on TryHackMe, Hack The Box, and PortSwigger Web Security Academy
- ☑ Run Kali or Parrot OS inside a free virtual lab
- ☑ Join Capture the Flag events to solve real puzzles
- ☑ Start scripting basic tools in Python, and read public pentest reports

● SECURITY ENGINEER

Security Engineer.

Build, defend, automate. The backbone of cyber defence.

A security engineer designs, builds, and maintains the tools and systems that protect an organisation. Where analysts monitor and testers break, engineers create the architecture that keeps attackers out and makes detection possible. The work is equal parts design, automation, and troubleshooting, and it is especially valued in cloud-first companies. Good security engineering is invisible when it works, which suits people who get satisfaction from building something that quietly protects everyone every day.

BEST FOR

Technically minded, hands-on learners. IT professionals moving into security. Tinkerers who enjoy scripting and automation and want to build, not just respond.

GROWTH PATH

Junior Engineer → Security Engineer → Senior Engineer → Security or Cloud Architect.

REALISTIC PAY

REGION	ENTRY LEVEL	EXPERIENCED
United States	$85k – $120k	$130k – $160k
United Kingdom	£50k – £75k	£80k – £110k
Germany / NL	€60k – €90k	€95k – €130k
Remote / global	$70k – $100k	$120k+

START TODAY — FREE

- ☑ Set up a home lab with free virtual machines or cloud free tiers
- ☑ Learn to deploy and secure both Linux and Windows
- ☑ Study the CIS Benchmarks and practice hardening a system
- ☑ Automate one security task with Bash or PowerShell, then deploy a SIEM (Wazuh / ELK)

THREAT INTELLIGENCE

Threat Intelligence.

Anticipate the adversary. Turn noise into foresight.

A threat intelligence analyst turns raw data into actionable insight about how attackers operate, from criminals to nation states. Rather than working inside firewalls, you track real campaigns, analyse malicious infrastructure, and connect technical events to bigger patterns, then communicate what matters to the right audience. The skill is not collecting information, which is easy, but judging what is relevant and explaining why, which is hard. It rewards strong readers and even stronger writers.

BEST FOR

Investigative thinkers fascinated by cybercrime, geopolitics, and adversary psychology. Strong writers who enjoy research and connecting dots others miss.

GROWTH PATH

Intel Analyst → Senior Intel Lead → Threat Researcher / CTI Manager → Director of Threat Strategy.

REALISTIC PAY

REGION	ENTRY LEVEL	EXPERIENCED
United States	$75k – $100k	$110k – $140k
United Kingdom	£45k – £65k	£70k – £100k
Germany / NL	€55k – €85k	€90k – €120k
Intel vendors	$70k+	$150k+ cleared

START TODAY — FREE

- ☑ Read public threat reports from Mandiant, Talos, Microsoft, CrowdStrike
- ☑ Study MITRE ATT&CK and map real attacks to tactics and techniques
- ☑ Practice OSINT with Maltego, SpiderFoot, and Shodan
- ☑ Write short threat summaries to practice clear, concise reporting

Where do you actually fit?

If you have read this far and still feel unsure, that is normal. Answer these five honestly and your starting path usually becomes obvious. There is no wrong answer, only a wrong reason to skip choosing.

Q1 What kind of work energises you most?

→ Investigating clues → SOC or Threat Intel. Building things → Engineering. Breaking things → Pentesting. Strategy & writing → GRC.

Q2 How do you feel about pressure and pace?

→ Thrive on urgency and shifts → SOC. Prefer a steadier rhythm → GRC or Engineering.

Q3 How do you feel about code?

→ Love scripting and automation → Pentest or Engineering. Rather not → GRC or SOC are very accessible without it.

Q4 What is your honest starting point?

→ From IT → head start toward SOC or Engineering. From business, law, or PM → GRC lets you add value almost immediately.

Q5 Reading or doing?

→ Deep reading and writing → Threat Intel or GRC. Hands-on terminals and labs → SOC, Pentest, Engineering.

THE ONLY RULE

The path does not need to be permanent. It only needs to be a start.

You can pivot later carrying everything you learned. What matters now is choosing, and beginning.

The skills under every path.

Whatever path you pick, the same foundation sits under it. Build this first. Skip it, and everything above becomes memorised steps you cannot reason about.

NETWORKING

How systems talk. The OSI model, TCP/IP, common ports and protocols, IP addressing, and the TCP handshake. This is what lets you tell normal traffic from a real compromise.

OPERATING SYSTEMS

Fluency in both Linux and Windows from the command line. File permissions, processes, services, logs. Attackers target both, so you must understand both.

SECURITY CONCEPTS

The CIA triad, common threats and tactics, defence in depth, least privilege, and the attack lifecycle. The shared language every role speaks.

YOUR HOME LAB

A free virtual environment where you break things safely. Kali as attacker, a Windows or Ubuntu target, isolated from your real network. This is where skill is actually made.

THE THREE FRAMEWORKS YOU WILL SEE EVERYWHERE

FRAMEWORK	WHAT IT IS FOR
NIST CSF	The big-picture map of a security program: Identify, Protect, Detect, Respond, Recover.
MITRE ATT&CK	The attacker's playbook. How real adversaries behave, in a shared language.
ISO/IEC 27001	The governance structure. How security is managed, documented, and audited.

Tools change every year. These foundations compound for a career.

The ones that actually matter.

Certifications validate skill. They do not replace it. Earn the skill first, then let a respected credential confirm it. Here is the sensible sequence by path, no collecting required.

YOUR PATH	SENSIBLE PROGRESSION
SOC Analyst	Security+ → CySA+ → vendor SIEM certs
GRC & Compliance	ISC2 CC → Security+ → CISA or CISM
Penetration Tester	Security+ → eJPT → OSCP
Security Engineer	Network+ → Security+ → CySA+ or cloud security
Threat Intel	Security+ → GIAC GCTI or GCFA

BEST FIRST CERT FOR MOST

CompTIA Security+. Globally recognised, structured, around 2–3 months. The default starting credential for SOC, GRC, and support-to-security moves.

FREE & BEGINNER FRIENDLY

Google Cybersecurity Certificate and **ISC2 CC** (often free for first-timers). Real labs, job-ready focus, ideal for absolute beginners.

THE MISTAKE TO AVOID

Do not collect certificates to feel like you are progressing. A cert you rushed without building the underlying skill is a liability in an interview. Hiring managers can tell the difference between someone who earned Security+ after real lab practice and someone who memorised a dump. **Quality always beats quantity.**

Build proof before you have a job.

This is the single most important move for a career-changer. You do not wait for permission to have experience. You build it, you document it, and you present it like the real thing, because it is.

ONE PORTFOLIO PROJECT PER PATH

SOC	Build a mini-SIEM with ELK or Splunk, parse logs, create custom alerts for suspicious behaviour.
GRC	Write a security policy for your lab network and a risk assessment mapped to NIST or CIS controls.
PENTEST	Document a full workflow from recon to report, and reproduce a known vulnerability safely in your lab.
ENGINEER	Harden a system to a CIS Benchmark, automate it with a script, and write up before and after.
THREAT INTEL	Use OSINT to research a target and write a threat report mapped to MITRE ATT&CK.

WHERE TO PUT IT

GitHub for code and writeups. A simple blog for project overviews. Your LinkedIn Featured section to tie it together.

THE HABIT

After every lab, write three short paragraphs: what you set out to do, what you found, what you concluded. Save it with a screenshot.

A documented portfolio is evidence no certificate alone can match.

Your first 90 days.

A goal without a schedule is a wish. This turns the whole roadmap into a sequence you can start tomorrow. It assumes a few focused hours most days, not a full-time commitment. Adjust the pace, keep the order.

DAYS 1–30 · FOUNDATIONS

- ☑ Complete one structured networking course end to end
- ☑ Live in a Linux terminal daily until basics feel natural
- ☑ Build your home lab with two or three machines
- ☑ Solve one beginner lab per week and document it

DAYS 31–60 · SKILLS & DIRECTION

- ☑ Work through key security concepts until the CIA triad is second nature
- ☑ Choose your one path from the five and commit
- ☑ Begin focused study toward one entry certification
- ☑ Start a public presence: GitHub or a simple blog

DAYS 61–90 · PROOF & POSITIONING

- ☑ Complete one portfolio project matched to your path
- ☑ Book or sit your entry certification
- ☑ Write your CV and rebuild your LinkedIn profile
- ☑ Connect with ten people in your target field and start applying

Consistency beats intensity. One focused hour a day for 90 days beats occasional ten-hour weekends. Protect the streak.

The mistakes that keep you out.

Most people do not struggle from lack of intelligence. They struggle from a handful of structural errors. Name them honestly and you move past almost everyone still making them.

× Trying to learn all five paths at once

Breadth without depth produces a CV nobody can place. Pick one. Go deep. Pivot later if you want.

× Chasing tools before foundations

A scanner in the hands of someone who does not understand the network produces noise, not insight.

× Collecting certifications instead of skill

Exams validate knowledge. They do not prove you can reason through an unfamiliar problem in an interview.

× Passive learning

Watching videos feels like progress and builds almost nothing. If you learn about firewalls, configure one. If you learn about logs, read them.

× Never documenting anything

The lab you cannot explain is a lab that never happened, as far as a hiring manager is concerned. Write it down.

× Quitting in the boring middle

The dip after the initial excitement is where most people drop out. It is also where the people who get hired keep going.

The barrier is rarely money or genius.
It is the willingness to start before you feel ready.

THE NEXT STEP

The roadmap shows the path. The guide walks it with you.

You now have the map: the five paths, the foundation, the certs, the proof, and a 90-day start. Knowing what to learn is different from knowing how to turn it into a hired role, a salary, and a career. That is the gap the Complete Guide closes.

THE COMPLETE GUIDE TO GET INTO CYBERSECURITY

From zero to hired.

$19.90

PDF + EPUB

99 pages, 16 sections. Every path expanded in depth, a day in the life of each role, the full skills breakdown, the certifications playbook, CV and LinkedIn templates, interview frameworks, hiring-manager expectations, and a complete week-by-week 90-day action plan. 30-day no-questions money-back guarantee.

- INSTANT DOWNLOAD
- LIFETIME UPDATES
- 30-DAY GUARANTEE

cyberwithjohann.com/guide

You do not need to know everything to begin.
You only need to start. And you already have.