FREE EXCERPT - 2 FULL CHAPTERS OUT OF 22

The Map: Cybersecurity Foundations

The 90-day plan and how to choose your path: two full chapters from the guide, so you can start today.

by Eduardo Solis

Security engineer with 5+ years defending Fortune 500 and global infrastructure - WAF, CDN, attack surface, and vulnerability management. I went from Costa Rica to the enterprise front line. This is the map I wish I'd had.

linkedin.com/in/edusolis

Why I wrote this

I didn't grow up with a clear path into cybersecurity. I started in Costa Rica, taught myself how systems really work, and worked my way onto the front lines of enterprise security - architecting protection at Akamai (one of the companies that keeps a huge slice of the internet online and safe), leading attack surface and vulnerability management for global clients, and defending Fortune 500 infrastructure.

Nobody handed me a roadmap. I built one the hard way - through fundamentals, reps, and a lot of late nights breaking things in a lab until they finally made sense.

This guide is that roadmap, cleaned up and structured so you don't have to wander. It won't make you an expert overnight. But if you actually do the work inside it, you'll build the foundation everything else in this field stands on.

If it helps you, I'd love to hear about it - and if you want to go faster, I mentor people walking this exact path. More on that at the end.

- Eduardo Solis

Contents

This excerpt includes the two marked chapters in full. The rest of the index is what the complete guide covers.

How to use this handbook

- Read for understanding first, not memorization.
- At the end of each chapter, complete the study actions.
- Keep your own notes in plain English.
- Revisit the same topics with more depth after you build a home lab.

21. A 90-Day Learning Plan

Most people improve faster with structure. The plan below is not the only valid path, but it is a strong beginner sequence because it builds from computing fundamentals into security reasoning and hands-on practice.

- Days 1-30: logic, Python basics, Linux basics, Windows basics, networking vocabulary, DNS, HTTP, and browser tooling.
- Days 31-60: TLS, web security basics, OWASP concepts, authentication, logging, packet captures, and simple Python automation.
- Days 61-90: vulnerability management, cloud basics, SIEM/log concepts, incident response workflow, and one or two portfolio projects.

> *A structured plan works. But a mentor who has already walked this path can compress months into weeks - keeping you focused on what actually matters and out of the rabbit holes that stall most beginners.*

Why this chapter matters

The key is consistency. Two focused hours every day often beats one huge weekend binge.

Suggested 12-week rhythm

- Weeks 1-2: logic, Python basics, shell basics
- Weeks 3-4: Linux and Windows foundations
- Weeks 5-6: networking, DNS, HTTP
- Weeks 7-8: TLS, authentication, web security basics
- Weeks 9-10: logs, detection, incident response
- Weeks 11-12: vulnerability management, cloud basics, one portfolio project

STUDY ACTIONS

- Time-block your study weeks and keep a visible tracker.
- Review and refine every 2 weeks instead of waiting for perfection.

22. Choosing a Path in Cybersecurity

Cybersecurity is not one job. Different roles emphasize different parts of the foundation. Knowing this early helps you study with purpose.

- SOC / Detection / IR: strong logging, networking, endpoint visibility, and investigation skills.
- Cloud Security: IAM, cloud networking, infrastructure, policy, automation, and architecture.
- Application Security: coding, SDLC, web security, APIs, and threat modeling.
- Security Engineering: systems, automation, architecture, tooling, reliability, and controls.
- Vulnerability Management / Attack Surface Reduction: asset context, exposure, scanning, prioritization, remediation, communication.
- Security Architecture / Solutions: broad understanding, customer communication, trade-offs, and translating risk into practical controls.

> *You don't have to figure this out alone. A conversation with someone who has worked across several of these paths can save you months of guessing - it's one of the most common things people bring to me in mentorship.*

Why this chapter matters

You do not need to choose your forever path immediately. Build broad foundations first, then specialize based on what work genuinely energizes you.

STUDY ACTIONS

- Read a few role descriptions and highlight repeated technical expectations.
- Pick one path to explore deeper for the next 60 days.

What you just read is the ending

The 90-day plan tells you WHAT to study and in what order. The 20 chapters before it are the HOW: the foundations that make that plan actually achievable, explained by someone who uses them every day defending real infrastructure.

The full guide - 22 chapters, 66 study actions

- Part I - Foundation: logic, coding, operating systems and networking.
- Part II - How the internet really works: DNS, HTTP/TLS, APIs, CDNs, proxies, caching.
- Part III - Security: identity, cryptography, controls, attacks, web and API security, vulnerability management, logging and detection, cloud.
- Part IV - Hands-on: tools, a safe home lab and portfolio projects.
- Appendix: glossary and final advice.

The full guide (ES + EN) is included in Torvex Academy. You are not paying for secrets - there are none. You are paying for structure, real feedback and accountability: the work of getting you there.

Your next step

You now have the foundations most people skip. The difference between people who break into cybersecurity - and keep climbing - usually isn't talent. It's direction, feedback, and not wasting months on the wrong things.

That's what I help with.

-> Career Strategy Call

A focused 1:1 session where we map where you are, where you want to go, and your exact next 90 days. You leave with a personalized roadmap.

-> 1:1 Mentorship

Ongoing guidance for people serious about going from foundations to their first role - and from there to senior and enterprise.

Whether you're trying to land your first job or level up to an international role, I've walked the path - and I can help you walk it faster.

Book a call or reach out

Booking: cal.com/torvex/career-strategy

Email: eduardo@torvexsecurity.com

LinkedIn: linkedin.com/in/edusolis

Glossary of Must-Know Terms

Attack surface
The total set of reachable systems, interfaces, and trust paths an attacker may target.

Botnet
A group of compromised devices controlled to perform coordinated malicious or abusive actions.

Exploit
A method or code path used to take advantage of a weakness.

Least privilege
Giving only the access required, nothing more.

Patch
A software update that fixes bugs, weaknesses, or stability issues.

Segmentation
Separating systems or traffic to reduce exposure and blast radius.

Telemetry
Observable data emitted by systems, applications, identities, or networks.

Threat model
A structured way to think about who may attack, what they may target, and how.

Final Advice for the Learner

- Study in layers: concept, observation, safe experimentation, explanation, then automation.
- Take notes in your own words. Copying text feels productive, but explaining is what builds mastery.
- Build projects that are simple, honest, and well documented.
- When stuck, return to fundamentals: what is the system, what is the expected behavior, what changed, and what evidence do I have?
- Strong foundations compound. Do not rush the basics.

One sentence to remember
Cybersecurity gets easier when you stop treating it like a bag of isolated tricks and start treating it like the study of how real systems work, fail, and get defended.