The Cybersecurity Field Guide

Hands-On Skills for Real-World Defense

Albert Halfmann

📘 Free Sample Edition

This is a sample of **The Cybersecurity Field Guide**. The complete book includes 7 comprehensive chapters, hands-on exercises, production-ready Python tools, practice datasets, and complete lab setup guides.

Get the full book at: leanpub.com/cybersecurityfieldguide

Table of Contents

Preface

Welcome to Real-World Cybersecurity

If you picked up this book, you're probably tired of cybersecurity training that feels disconnected from reality. You've sat through presentations about theoretical attack vectors and watched demos of tools in sanitized lab environments. You've memorized framework acronyms and compliance requirements. But when Monday morning comes and real alerts start firing, you still feel like you're missing something fundamental.

You're not wrong. There's a massive gap between cybersecurity education and cybersecurity practice.

This field guide exists to bridge that gap. It's not about passing certification exams or impressing people at conferences. It's about building the practical, hands-on skills you need to be effective in real security operations from day one.

Why This Approach Works

Traditional cybersecurity education teaches tools in isolation—here's AWS, here's Python, here's Splunk, each in their own neat chapter. But real security work doesn't happen in isolation. When you're investigating a potential breach at 2 AM, you don't get to use just one tool. You need to pivot fluidly between cloud consoles, command lines, scripts, and SIEM queries, often within the same investigation.

This guide teaches you to think like a security professional, not just use security tools. Every chapter builds toward the comprehensive scenarios in Chapter 7, where you'll see how everything connects in practice.

Who This Guide Is For

This book is written for:

- IT professionals transitioning into cybersecurity roles
- Developers who need to understand security beyond secure coding
- Junior security analysts who want to accelerate their practical skills
- Anyone who's tired of surface-level security training

You don't need to be a programming expert or a networking guru, but you should have basic technical literacy. If you're comfortable with command lines, understand fundamental networking concepts, and can read code without panic, you're ready for this guide.

How to Use This Guide

Each chapter is designed to be immediately practical:

- Learn the concepts behind each tool and framework
- Understand the why behind security best practices
- Practice with realistic examples that mirror real-world scenarios
- Build working solutions you can adapt to your environment

The early chapters give you foundational skills. The final chapter shows you how professionals combine these skills to solve complex, real-world problems.

Don't just read this guide—work through it. Set up the tools, run the commands, modify the scripts. The difference between knowing about cybersecurity and being able to do cybersecurity is practice.

Let's Get Started

Cybersecurity can feel overwhelming when you look at the entire field at once. But it becomes manageable when you break it down into practical, learnable skills. By the end of this guide, you'll have a toolkit of capabilities that will serve you throughout your security career, regardless of how the technology landscape evolves.

Ready to stop being a consumer of security tools and start being a creator of security solutions? Let's dive in.

Chapter 1: AWS for Cybersecurity Professionals

This chapter will introduce cloud security concepts using Amazon Web Services as the primary example. We will cover core AWS services and their security implications, moving from basic identity management to advanced threat detection.

Section 1: Introduction to Cloud Security and AWS

Cloud computing has fundamentally changed how we approach cybersecurity. No longer are our assets confined to physical data centers with clearly defined perimeters. In AWS, your infrastructure is code, your perimeter is identity, and your security controls are API calls.

This shift requires a new mindset. The good news? Cloud platforms like AWS provide security capabilities that would be impossibly expensive to build on-premises. The challenge? You need to know how to use them effectively.

Understanding the Shared Responsibility Model

The most critical concept in cloud security is the Shared Responsibility Model. AWS is responsible for security "of" the cloud—the physical infrastructure, hypervisors, and foundational services. You're responsible for security "in" the cloud—your data, applications, identity management, and network controls.

Think of it like renting an apartment. The building owner ensures the locks work, the structure is sound, and the fire alarms function. But you're responsible for locking your door, not leaving windows open, and protecting your valuables inside.

Core AWS Services for Security

Throughout this chapter, we'll explore the essential AWS services every security professional needs to understand:

- **IAM (Identity and Access Management):** The foundation of AWS security
- **VPC (Virtual Private Cloud):** Your network isolation and segmentation
- **CloudTrail:** The audit log for everything happening in your account
- **GuardDuty:** Intelligent threat detection using machine learning

- **Security Hub:** Centralized security findings and compliance

A Practical Example: Detecting Suspicious API Calls

Let's start with something concrete. Imagine you need to detect when someone tries to access AWS resources from an unusual location. Here's how you'd approach it:

```
# Example CloudTrail event pattern for detecting unusual API calls {
"source": ["aws.cloudtrail"], "detail-type": ["AWS API Call via
CloudTrail"], "detail": { "eventSource": ["iam.amazonaws.com"],
"eventName": [{ "exists": true }], "sourceIPAddress": [{ "anything-
but": ["10.0.0.0/8", "172.16.0.0/12"] }] } }
```

This EventBridge rule pattern would trigger whenever IAM API calls come from IP addresses outside your corporate network. It's a simple example, but it demonstrates the power of AWS's native security tools.

This is where the sample ends.

The full book continues with detailed, hands-on coverage of:
• Complete IAM policy creation and management
• Building secure VPCs from scratch
• Automated incident response with Lambda
• Real-world security scenarios and solutions
• Plus 6 more comprehensive chapters!

Get the complete book with all bonus materials at:
leanpub.com/cybersecurityfieldguide

About the Author

Albert Halfmann is a Senior Security Engineer at Chicha Technology, LLC, where he leads the development of next-generation cybersecurity solutions. With seven years of hands-on experience in cybersecurity and eight years of military service in the Army Reserves, Albert brings a unique blend of technical expertise and operational discipline to the field.

Albert's professional journey spans multiple domains of cybersecurity, from digital forensics and OSINT analysis to SOC engineering and cloud security. He has held progressive roles at leading defense contractors, where he managed teams, investigated complex cases, and directly influenced senior leadership decision-making processes.

His technical certifications include AWS Data Engineer, CompTIA SecurityX (formerly CASP+), CompTIA Cybersecurity Analyst+, and multiple AWS cloud certifications, reflecting his commitment to staying current with evolving technology landscapes.

When not engineering security solutions, Albert contributes to the cybersecurity community through knowledge sharing and mentorship. The Cybersecurity Field Guide represents his commitment to bridging the gap between theoretical knowledge and real-world application.

Find Albert on GitHub at **github.com/clearblueyellow**