

# ESSENTIALS PROGRAM

*A 6-Month Hands-On Cybersecurity Curriculum*  
From Zero Experience to Career-Ready · Modules 1 through 6

6

M O D U L E S

6

M O N T H S

100%

H A N D S - O N

Student Edition · Curriculum Overview · 2025–2026

[cyberinteltraining.com](https://cyberinteltraining.com) · 1-877-292-3755 · [info@cyberinteltraining.com](mailto:info@cyberinteltraining.com)

# Welcome to Your Cybersecurity Career

The CIT Essentials Program is a 6-month, hands-on cybersecurity curriculum built for career changers and complete beginners. No degree required. No prior experience needed — just the drive to build something real.

This document is your module-by-module overview of everything you will learn, build, and prove over the next six months. Each module ends with a real deliverable for your portfolio. By graduation you will have the skills, confidence, and job-placement support to land your first cybersecurity role.

## HOW EACH MODULE IS STRUCTURED

Every module follows the same format used in our official study guides: concept instruction → hands-on labs → comprehension test → real-world scenario exercise → capstone project. You learn by doing — not just reading.

## Program at a Glance

MOD	TITLE	CERTIFICATION PATHWAY
01	Introduction to Cybersecurity	CIG-CSF101 · CompTIA Security+ preparation
02	Linux Fundamentals	CIG-LF101 · CompTIA Linux+ preparation
03	Python Fundamentals	CIG-PY101 · Security scripting
04	Network Research	CIG-CSA · CompTIA Network+ / CySA+
05	Penetration Testing	CIG-CSP · CompTIA PenTest+ / eJPT / CEH
06	SOC Analyst	CIG-SOC-101 · CompTIA CySA+

## M O D U L E 0 1

# Introduction to Cybersecurity

*How to Think and Act Like a Cybersecurity Analyst*

### T O P I C S C O V E R E D

- ▶ Overview of Computer Systems & Number Systems
- ▶ Networking Fundamentals — IP, Ports, Protocols
- ▶ Open-Source Intelligence Tools (OSINT)
- ▶ Cyber Threats and the Threat Landscape
- ▶ Security Frameworks and Best Practices
- ▶ Understanding Terminal Navigation

### L E A R N I N G O U T C O M E

You will develop the analyst mindset and core technical foundation every cybersecurity role requires. You will map your own network, produce a visual infrastructure report, and demonstrate hands-on use of OSINT and network CLI tools.

## M O D U L E 0 2

# Linux Fundamentals

*The Operating Environment of Every Security Professional*

### T O P I C S C O V E R E D

- ▶ Virtualization — Type 1 & Type 2 Hypervisors
- ▶ Linux OS Basics, File System Navigation
- ▶ File Permissions and Access Control
- ▶ Command Line, Text Editors (Nano, Micro, Geany)
- ▶ Logical Text Manipulation and Redirection
- ▶ Bash Scripting and Automation

### L E A R N I N G O U T C O M E

You will gain full Linux command-line fluency. Your capstone script will gather live system intelligence — IP/MAC addresses, CPU and memory usage, running services, and file system status — and present it as a structured report.

## M O D U L E 0 3

# Python Fundamentals

*From Zero to Security Automation*

### T O P I C S C O V E R E D

- ▶ Python Syntax, Data Types, and Modules
- ▶ String Processing and Log Analysis
- ▶ File I/O — Reading and Writing Security Data
- ▶ Conditional Scripting and Control Flow
- ▶ Functions and Building Reusable Tools
- ▶ Python Scripting and Data Manipulation

### L E A R N I N G O U T C O M E

You will build a working Python program that parses real auth logs, identifies brute-force attempts, counts privileged command usage, geolocates suspicious IPs, and generates a comprehensive automated analysis report.

## M O D U L E 0 4

# Network Research

*Scanning, Traffic Analysis, and Network Defense*

### T O P I C S C O V E R E D

- ▶ Kali Linux vs Ubuntu — Choosing Your Platform
- ▶ Network Tools: Wireshark, Nmap, Netcat, OSINT
- ▶ Cyber Attacks: MiTM, LLMNR Poisoning, Trojans
- ▶ TCP/IP Stack, OSI Model, Subnetting
- ▶ Password Attacks: John the Ripper, Hashcat
- ▶ Network Security Best Practices

### L E A R N I N G O U T C O M E

You will become proficient in the core toolset every network security analyst uses daily. Your capstone bash script will anonymize the user and leverage a lab machine as a scanning endpoint — a shareable, reusable tool for any practitioner.

## M O D U L E 0 5

# Penetration Testing

*Authorized Attack Simulation — Recon to Report*

### T O P I C S C O V E R E D

- ▶ Penetration Testing Methodology (5 Phases)
- ▶ Post-Exploitation and Covering Tracks
- ▶ Social Engineering — Psychology and Techniques
- ▶ Information Gathering, Enumeration, Exploitation
- ▶ Tools: Nmap, Netcat, Metasploit Framework
- ▶ Bind/Reverse Payloads — Vulnerability Exploitation

### L E A R N I N G O U T C O M E

You will master the complete penetration testing lifecycle. Your capstone is an automated vulnerability scanning program that identifies network weaknesses, prioritizes findings, and produces a professional pentest report ready for a real client.

## M O D U L E 0 6

# SOC Analyst

*From Detection to Response — Security Operations*

### T O P I C S C O V E R E D

- ▶ Role of SOC Analysts — L1, L2, L3 Tier Structure
- ▶ IDS/IPS — Snort, PfSense, Windows Domain Controllers
- ▶ Incident Response Phases and Log Analysis
- ▶ SIEM Tools: ELK Stack, Kibana, Splunk
- ▶ Threat Detection, Threat Hunting, and ATT&CK
- ▶ Real-World Security Events and Forensics

### L E A R N I N G O U T C O M E

You will build the complete SOC analyst skill set. Your capstone project simulates and detects live malicious activity in a lab environment — the exact hands-on experience that employers actually hire for.

# Certifications You'll Be Ready For

Every module you complete builds directly toward one or more industry-recognized certifications. By the time you finish all six modules you will be prepared to sit for the following exams — the same credentials hiring managers look for.

## CIG Internal Certifications

CODE	CERTIFICATION	MODULE	WHAT IT VALIDATES
CIG-CSF101	Cyber Security Fundamentals	Module 01	Foundations of networking, OSINT, and the analyst mindset.
CIG-LF101	Linux Fundamentals	Module 02	Linux command line, scripting, permissions, and security operations.
CIG-PY101	Python for Cybersecurity	Module 03	Security scripting, automation, and log analysis in Python.
CIG-CSA	Cyber Security Analyst	Module 04	Network analysis, scanning, traffic capture, and defense.
CIG-CSP	Cyber Security Practitioner	Module 05	Full penetration testing methodology and professional reporting.
CIG-SOC-101	SOC Analyst	Module 06	SIEM, IDS/IPS, threat hunting, and incident response.

## CompTIA Certification Pathway

CODE	CERTIFICATION	MODULE	WHAT IT VALIDATES
Security+ SY0-701	CompTIA Security+	Mods 01–02	The most recognized entry-level cybersecurity cert. Required for most security roles. Elite students receive an exam voucher.
Linux+ XK0-005	CompTIA Linux+	Module 02	Validates Linux admin skills — command line, scripting, and security. Essential for every cybersecurity career path.
Network+ N10-009	CompTIA Network+	Module 04	Validates TCP/IP, OSI model, scanning, and network defense fundamentals.
CySA+ CS0-003	CompTIA CySA+	Mods 04–06	Cybersecurity analyst cert covering threat detection, SIEM, and incident response. Target cert for SOC roles.
PenTest+ PT0-002	CompTIA PenTest+	Module 05	Validates penetration testing methodology from planning through professional reporting.

## Additional Industry Certifications

CODE	CERTIFICATION	MODULE	WHAT IT VALIDATES
eJPT	eLearnSecurity Junior Penetration Tester	Mods 04–05	Fully hands-on entry-level pentest exam on a real network. No multiple choice.
eCPPT	eLearnSecurity Certified Professional Pentester	Module 05	Intermediate credential covering exploitation, pivoting, and professional reporting.
CEH v12	EC-Council Certified Ethical Hacker	Mods 04–05	One of the most globally recognized ethical hacking certs. Full attack lifecycle.

### ELITE ENROLLMENT — SECURITY+ EXAM VOUCHER INCLUDED

Elite students receive a CompTIA Security+ exam voucher (SY0-701) as part of their enrollment package — one of the most in-demand certifications in cybersecurity, included at no additional cost. Talk to your instructor about targeting your first cert from day one.

# Included Perks & Benefits

---

*Everything you need to succeed — built in from day one.*

## ✓ Tests & Extra Practice

Every major topic is followed by hands-on labs and a comprehension test to lock in your learning before you advance. Extra practice goes beyond the fundamentals — so you are always building, never just reviewing.

## ⚡ Real-World Scenarios

One scenario exercise per module puts you in the analyst's seat. You apply everything you have learned to problems that mirror real workplace situations — same decision-making, same tools, same stakes.

## ★ Capstone Projects

Every module ends with a comprehensive capstone project — a real deliverable, not a worksheet. Network maps, automation scripts, pentest reports, SOC incident analyses. Portfolio-ready from day one.

## 🌐 Community Access

Immediate access to our Discord communities. Network with fellow students, alumni, and CIT instructors. Ask questions, share wins, and stay connected with people on the same journey.

## ➤ Career IO — Your Job Launch Engine

From month two, Career IO activates: recruiting partners, interview prep, mock interviews, AI-driven interview psychology coaching, LinkedIn optimization, resume building, and a job guarantee.

## 🔹 TryHackMe Live Lab Environment

Practice on the same platform used by working security professionals worldwide — real servers, guided rooms, gamified labs. Hands-on practice that is engaging, not a chore.

---

### DISCLAIMER

*This document contains privileged and/or confidential information intended solely for the use of the individual or entity to which it is addressed. Any unauthorized review, use, disclosure, reproduction, or distribution is strictly prohibited and may be unlawful.*