Skills-First Cybersecurity Bootcamp

With Cybersecurity jobs projected to **grow 30%+ by 2033***, organizations face a critical **shortage of qualified talent**. While traditional training programs emphasize **theoretical knowledge**, they often **fail to develop the practical skills** employers actually need.

Cert4Tech's Skills-First Cybersecurity Bootcamp bridges this gap with a hands-on approach that builds **job-ready capabilities**. Meticulously aligned with the **NICE Cybersecurity Workforce Framework**, our program transforms beginners into professionals with the **practical skills** demanded in today's security landscape.

Who Is This Bootcamp Good For?

- Individuals aspiring to enter a Cybersecurity Entry-Level Role.
- IT Professionals looking to transition into Cybersecurity.
- IT Operations staff looking to expand their skills domain.
- Organizations seeking to develop a Cybersecurity Workforce.

Skills-First Cybersecurity Bootcamp Objectives

- Develop in-demand, real-world **Cybersecurity skills** through a **hands-on, learn-by-doing** approach.
- Equip learners with a **Cybersecurity Mindset** by teaching both foundational theory and 'How to Think like a Cybersecurity Analyst'.
- Offer schedule flexibility and consistent progress through a fully **online, self-paced micro-course format**.

This Bootcamp features:

- Over 100 hours of instruction in video, lecture, and hands-on practice formats.
- 55 practical, interactive, scored labs.
- Chapters broken down into micro-lessons to support learning.
- Chapter review quizzes and module-level scored knowledge checks.
- Locked chapters that require learners to meet prerequisites (complete all lessons and pass labs and exams).
- Accessible content designed to support diverse learning needs.

Certification

Upon successful completion of the Bootcamp, learners will obtain the **"Skilled Cybersecurity Analyst"** Certification from Cert4Tech.

CERT4TECH
SKILLED
Cybersecurity
Analyst

***Source:** U.S. Bureau of Labor Statistics (BLS) https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Skills-First Cybersecurity Bootcamp Contents

Contents	NICE Skills Supported in Module
Preamble: ◦ Overview and Terminology ◦ Problem Solving ◦ Foundations for Cybersecurity	◦ Solving problems ◦ Collaborating with internal and external stakeholders ◦ Performing risk assessments
Module 1: Computing & Operating System Fundamentals ◦ Chapter 1: Introduction to Computing Systems ◦ Chapter 2: Operating System Essentials ◦ Chapter 3: File Systems and Storage Management ◦ Chapter 4: Command Line Interface and System Administration ◦ Chapter 5: Network Configuration and Troubleshooting ◦ Chapter 6: System Recovery and Performance Management	◦ Operating IT systems/maintaining IT systems ◦ System performance troubleshooting/optimization ◦ Protecting network against malware ◦ Configuring computer protection components ◦ Troubleshooting client-level problems
Module 2: Network Fundamentals & Security ◦ Chapter 1: Introduction to Computer Networks ◦ Chapter 2: Network Addressing & Configuration ◦ Chapter 3: Network Infrastructure & Command Line Tools ◦ Chapter 4: Network Connectivity & Remote Access ◦ Chapter 5: Advanced Network Security & Cloud Infrastructure	◦ Establishing routing schema ◦ Securing network communications ◦ Operating network equipment ◦ Executing command line tools ◦ Operating network systems ◦ Configuring network devices ◦ Installing network devices ◦ Applying subnet techniques ◦ Interpreting traceroute results ◦ Troubleshooting network equipment
Module 3: Security Fundamentals ◦ Chapter 1: Core Security Concepts and Principles ◦ Chapter 2: Understanding Security Threats ◦ Chapter 3: Security Controls and Defense Mechanisms ◦ Chapter 4: Network Security Assessment	◦ Identifying software communications vulnerabilities ◦ Evaluating security products ◦ Recognizing vulnerabilities ◦ Categorizing types of vulnerabilities ◦ Assessing organization's threat environment ◦ Collaborating with stakeholders
Module 4: Operating System Security Administration ◦ Chapter 1: Windows Security Administration Fundamentals ◦ Chapter 2: Linux Security Administration Fundamentals ◦ Chapter 3: Security Policies and Access Control	◦ Applying host/network access controls ◦ Applying hardening techniques ◦ Managing account access rights ◦ Developing/implementing user credential management ◦ Implementing enterprise key escrow systems ◦ Assessing security controls
Module 5: Network Security Implementation ◦ Chapter 1: Network Security Architecture and Fundamentals ◦ Chapter 2: Access Control and Authentication ◦ Chapter 3: Network Protection and Encryption	◦ Developing/testing network infrastructure contingency plans ◦ Implementing established network security practices ◦ Configuring network protection components ◦ Implementing network infrastructure contingency plans ◦ Encrypting network communications ◦ Tuning network sensors
Module 6: Security Operations & Monitoring ◦ Chapter 1: Introduction to Security Operations ◦ Chapter 2: Log Management Fundamentals ◦ Chapter 3: Network Traffic Analysis Tools	◦ Deploying continuous monitoring technologies ◦ Detecting host and network-based intrusions ◦ Reviewing logs ◦ Identifying evidence of past intrusions ◦ Performing log file analysis ◦ Troubleshooting cyber defense infrastructure anomalies