C.A.R.E
CYBER AWARENESS AND RESPONSE EDUCATION

C.A.R.E Cybersecurity Bootcamp

CARE Cybersecurity Bootcamp is a hands-on, immersive training program designed to prepare individuals for entry-level cybersecurity positions in 24 weeks.

Overview

Delivery Methods

Online Self-Paced + Optional Facilitator-Led Weekly Sessions

Recommended Pace

24 Weeks | 20 Hours x Week

NICE Framework Job-Ready Positions

Participants emerge ready for five entry-level roles

Why C.A.R.E

CARE utilizes immersive, hands-on training to equip participants with the skills needed to succeed. We have partnered with academic institutions, corporations, and government entities worldwide to deliver comprehensive professional development programs through:

Comprehensive Learning:

Practical and theoretical knowledge delivered through hands-on labs and real-world scenarios.

Flexible Learning Models:

Blended learning options combining in-person and self-paced formats with facilitator support.

Cohort-Based Engagement:

An online, self-paced program enhanced by a supportive, community-based learning environment.

Interactive Training:

Technical skills and frameworks are taught through exercises in a safe virtual setting.

Career-Ready Skills:

Essential soft skills, like teamwork, are integrated throughout the program to prepare participants for real-world careers.

The NICE Framework

The National Initiative for Cybersecurity Education (NICE) framework was developed to define cybersecurity jobs and the skills individuals need to acquire to qualify for them. Our curriculum is designed to prepare participants for five entry-level cybersecurity positions, which align with globally recognized NICE standards.

Upon completion, learners can expect to qualify for entry-level roles such as:

- **Cyber Defense Analyst**
- **Cyber Infrastructure Support Specialist**
- **Cyber Forensics Analyst**
- **Network Operations Specialist**
- **Cyber Incident Responder**

Bootcamp Structure

Onboarding Activities

Participants learn how to navigate the platform and review expectations to maximize success

Intro to Cyber

Examine cybersecurity fundamentals and discover different roles in the field.

Foundational Courses

Review common vulnerabilities, risks, and threats in cybersecurity, as well as the fundamentals of networking and network security.

Courses:
Bootcamp Introduction
Network Administration
Cybersecurity Fundamentals
Network and Application Security
Incident Handling

Advanced Courses

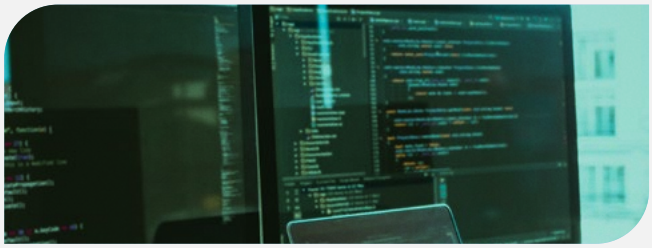
Dive deeper into advanced cybersecurity topics and acquire skills related to different areas of specialization.

Courses:
Forensics
Malware Analysis
Ethical Hacking and Incident Response
Secure Design Principles
Risk Management
Threat Intelligence

Exams

Midterm
Final Assessment

A grade of 60% is needed for each exam to earn a certificate of completion



Bootcamp Syllabus

01 | Intro to Cyber

Participants learn cybersecurity basics, including risk management, cyber tools, and popular career paths.

Topics Covered:

- The Cybersecurity World and Crime
- Attackers and APTS
- Mitigating Risk and Taking Control

02 | Bootcamp Introduction

Participants review the program structure and how to get the most out of their learning experience.

Topics Covered:

- Overview of the Bootcamp and Cybersecurity Industry
- Cybersecurity Career Paths

03 | Network Administration

Participants explore how to design, configure, and troubleshoot networks so they can acquire the necessary skills for running and monitoring a network with confidence

Topics Covered:

- Network Configuration – LAN, WAN
- Segmentations, VLANs, and Subnetting
- Network Mapping Tools and Network Devices
- Troubleshooting and Monitoring Networks
- Telecommunication
- System Administration

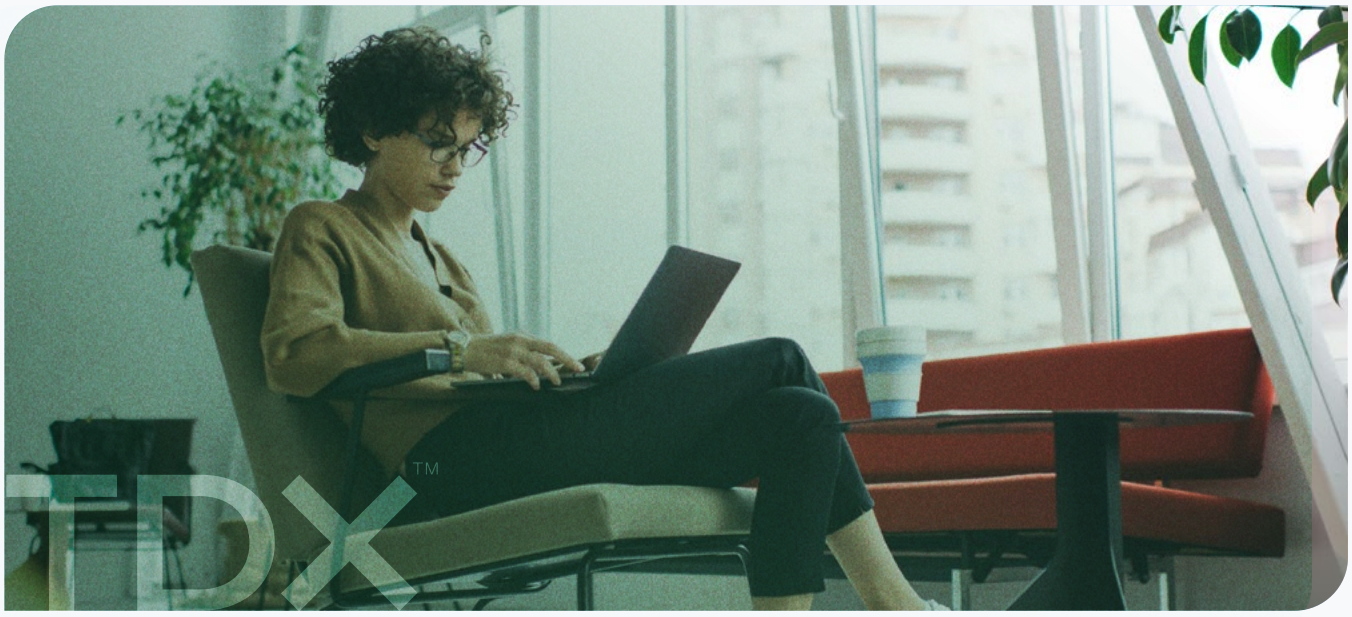
TOOLS: Cisco Packet Tracer, Nmap, Windows PowerShell

04 | Cybersecurity Fundamentals

Participants gain knowledge of vulnerabilities, exploits, threats, and attacker motivations, capabilities, and strategies.

Topics Covered:

- Most Common Vulnerabilities, Risks, and Threats
- The Main Concepts in Cybersecurity
- Types of Malware and Attackers
- NIST & International Cybersecurity Framework
- Most Common Cyberattacks
- Famous Cyber Incidents in the Industry



05 | Network and Application Security

Participants learn about network and application security defense methodologies and construction of secure network architectures.

Topics Covered:

- Security Tools–Firewalls, Antivirus, IDS/IPS, SIEM, DLP, EDR
- Honeypots and Cyber Traps
- Cryptography–Symmetric vs. Asymmetric Keys
- Encryption/Decryption, Hash Functions
- Security Architecture
- Access Control Methods, Multi-factor Authentication, Authentication Protocols

TOOLS: Kali Linux, Splunk, Snort IDS, Active Directory, Nmap, OpenVPN, Windows Firewall, Linux, Iptables

06 | Incident Handling

Participants examine the world of cyberattacks and learn how they work, their impact, and how to detect them as real-world cybersecurity analysts.

Topics Covered:

- Types of Attacks in the Web, Domain, & Malware Areas
- Practicing the Role of the SOC Analyst by Detecting Alerts, and Analyzing Alerts and Incidents
- Analyzing Malicious Indicators and Documenting the Findings
- Group and Individual Incident Report Writing

TOOLS: Splunk, In-House SIEM, Wazhu, VirusTotal, Powershell, Wireshark

07 | Forensics

Participants acquire skills to analyze threats in digital and other media devices.

Topics Covered:

- Computer Memory Forensics, Memory Dump Analysis
- FTK Imager, Autopsy, Redline, and RAM capturing
- Digital Evidence Acquisition Methodologies
- Registry Forensics
- Windows Timeline Analysis and Data Recovery
- Network Forensics, Anti-Forensics, and Steganography

TOOLS: Volatility Framework, FTK Imager, Autopsy, NetworkMiner, Wireshark, OpenStego, ShellBags Explorer, winmd5free, Magnet RAM Capture, Redline, HxD

08 | Malware Analysis

Participants investigate multiple malware analysis methods to study real-world malware samples and gain the skills to analyze malicious software and understand its behavior.

Topics Covered:

- Dynamic Malware Analysis, Reverse Engineering, and Malware Obfuscation
- Fileless Malware Analysis
- Containment, Eradication, and Recovery Malware Stages
- Analysis Using Sysinternals

TOOLS: Procexp, Procmon, Autoruns, TCPView, PuTTY, ExeInfo PE, ProcDOT, HashCalc, FileAlyzer, PDFStreamDumper, HxD, Wireshark, UPX

09 | Ethical Hacking and Incident Response

Participants dive into the world of hacking by performing cyberattacks and practicing relevant response methodologies.

Topics Covered:

- Hacking, Ethical Hacking, and the Penetration Testing Frameworks
- Ethical Hacking Phases
- Network Hacking (Metasploit Framework) and Web Application Hacking (OWASP Top 10)
- Post-Incident Activities
- Capture the Flag Challenge

TOOLS: Metasploit, SQLMap, Nmap

10 | Secure Design Principles

Participants review cybersecurity design best practices, how to assess and detect security design flaws, and trend analysis.

Topics Covered:

- Trend Analysis
- Artificial Intelligence in Cybersecurity
- Zero-Trust Policy
- Best Detection Methodologies
- Incident Impact Mitigation

11 | Risk Management

Participants study risk management and related methodologies and processes that assist in effectively managing such risks.

Topics Covered:

- Risk Management Processes
- Analyzing, Prioritizing, Evaluating, and Monitoring Severity of Internal and External Risks
- Risk Management Policies, Procedures, Standards, and Guidelines
- Security Models

12 | Threat Intelligence

Participants discover different methods, processes, techniques, and tools to gather intelligence about potential threats such as hackers and attack vectors.

Topics Covered:

- Threat Intelligence Cycle Methodology and Industry Implementation
- Google Hacking – Operators, Finding Sensitive Data, Directory Listing, Devices and Hardware
- Dark Web and Dark Market Investigation
- Online Anonymity using Metadata, Google Cache, VPN, and Tor
- Trend Analysis, Basic Excel Data Analysis
- Industrial Tool Practice in Real Environments

TOOLS: C.A.R.E Security Awareness Training (Formerly Lucy)

13 | Final Scenarios and Interview Prep

Participants access real-life scenarios of cybersecurity incidents, present a group project, and review technical and soft-skill preparation for job interviews.

7034_10212024