ThriveDX™

ThriveDX Cybersecurity Impact Bootcamp

Transform Your Future in Just 24 Weeks

The ThriveDX Cybersecurity Impact Bootcamp is an accelerated, non-credit training program designed to take you from beginner to job-ready in just over 24 weeks, even if you have little to no background in information technology (IT). When you're done with this program, you'll be ready for entry-level jobs in cybersecurity—one of the most in-demand technology fields.

Delivered remotely through self-paced classes, our bootcamp enables learners to gain the job-ready skills they need to enter the growing cybersecurity industry.

There are over 750,000 open cybersecurity jobs in the USA. When you're done with this program, you'll be ready to make one of them your own.

Overview

Format

Online
Self-Paced

Duration

24 Weeks
480 Hours

Schedule

Recommended Pace:
20 Hours x Week

Career

Aligned with the National Initiative for Cybersecurity Education

Opportunity

Over 750,000 Cybersecurity Positions Unfilled in the US*

Price

$9,995
Payment Plans & Funding Available

* Source: Cyberseeek.org

Methodology

The ThriveDX Cybersecurity Impact Bootcamp uses an accelerated, hands-on model to train students to enter the cybersecurity industry, with an emphasis on teaching the specific skills required for success. This is accomplished with:

Practical and theoretical knowledge delivered through over 100 hands-on labs and real-world scenarios.

Technical skills, frameworks, and tools taught through interactive exercises in a safe virtual environment.

Essential career-focused and soft-skills training—from teamwork to interview prep—embedded throughout the program.

Aligned with NICE Framework

The National Initiative for Cybersecurity Education (NICE) framework was developed by the National Institute of Standards and Technology (NIST) to define cybersecurity jobs, and the skills learners need to acquire to qualify for them.

The **ThriveDX Cybersecurity Impact Bootcamp** aligns with the NICE framework, which means that our curriculum is designed to prepare you for the most in-demand jobs in cybersecurity.

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

	Learner Outcome	Courses
Intro to Cyber	Gain the fundamentals of cybersecurity, discover the different roles in the field, and learn how each makes an impact.	
Foundational Courses	The first part of the program covers the most common vulnerabilities, risks, and threats in cybersecurity, as well as the fundamentals of networking and network security.	Bootcamp Introduction Network Administration Cybersecurity Fundamentals Network and Application Security Incident Handling
Midterm	Halfway through the program, you will take a midterm exam that covers information from the first part of the bootcamp, with a grade of 60% needed to pass.	
Advanced Courses	During the second part of the program, you will dive deeper into advanced cybersecurity topics and acquire skills related to different areas of specialization.	Forensics Malware Analysis Ethical Hacking and Incident Response Secure Design Principles Risk Management Threat Intelligence
Final Assessment	Now, with all of your knowledge from the course, you will complete several final scenarios and a cumulative final exam. An overall grade of 60% on these final assessments is needed to earn a certificate of completion, and to ensure you feel prepared to sit for the CertNexus CFR certification.	

Bootcamp Syllabus

01 | Intro to Cyber

In just 30 hours, learn the cybersecurity basics, from malware and the OWASP Top 10 to risk management and career paths. Understand attackers and tools like SIEM & firewalls, and learn about the potential career paths in this booming field.

Topics Covered:

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

02 | Bootcamp Introduction

The Bootcamp Introduction will give you the tools you need to make the program an efficient and fulfilling learning experience. During this course, you will learn how the program is structured alongside the basics of computers.

Topics Covered:

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

03 | Network Administration

This course focuses on designing, configuring, and troubleshooting networks so you 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

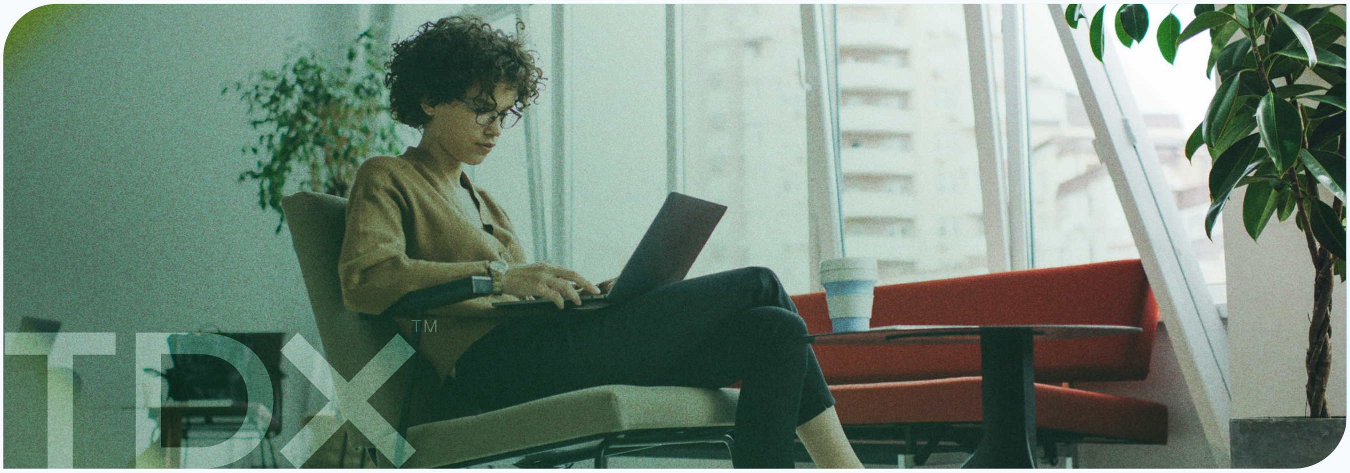
TOOLS: Cisco Packet Tracer, Nmap, Windows PowerShell

04 | Cybersecurity Fundamentals

The next stage of the bootcamp defines cybersecurity and how organizations utilize it. This is when you will acquire knowledge about vulnerabilities, exploits, and threats, then dive into different types of attackers, their motivations, capabilities, strategies, and the kinds of malware used to target their victims.

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

Here you will learn about network and application security defense methodologies and construction of secure network architectures. When this course is over, you will understand how to detect and eventually block malicious actors from carrying out cyberattacks and crimes.

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

In this course, you will dive into the world of cyberattacks and learn how they work, their impact, and how to detect them. Next, you will practice detection and analysis of incidents in security applications, then roleplay as a real-world cybersecurity analyst.

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

Access digital forensic processes for analyzing threats in digital devices, including identification, recovery, investigation, and validation of digital evidence in computers 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

This course will teach you how to use multiple malware analysis methods, like reverse engineering, binary analysis, and obfuscation detection to analyze real-world malware samples. By the time it's over, you will have 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, Exelnfo PE, ProcDOT, HashCalc, FileAlyzer, PDFStreamDumper, HxD, Wireshark, UPX

09 | Ethical Hacking and Incident Response

Here you will dive into the world of hacking by performing cyberattacks and practicing relevant response methodologies. This means learning to identify cybersecurity breaches, insider/outsider threats, incident response life cycles, and perform relevant assessments to develop protection plans.

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

The world of cybersecurity is always changing. That's why this course will help you understand trend analysis and learn how to perform it while becoming familiar with the newest cybersecurity threats. Additionally, you will gain an understanding of cybersecurity design best practices, as well as how to assess and detect security design flaws.

Topics Covered:

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

11 | Risk Management

In today's world, almost any action can become a potential risk. In this course, you will study risk management and related methodologies and processes that assist in effectively managing such risks – while understanding that not all risks can be eliminated immediately.

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

One of the ways to protect your organization is to know your enemy. In this course, you will discover different methods, processes, techniques, and tools involved in gathering 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: ThriveDX Security Awareness Training (Formerly Lucy)

13 | Final Scenarios and Interview Prep

This is where it all comes together. This final course includes real-life scenarios of cybersecurity incidents and a final exam covering all the content learned along the bootcamp. You will present a group project which you worked on throughout the course, then review technical and soft-skill preparation for job interviews.

Included in Our Bootcamp

Hands-on Skills Training

Learn job-ready skills with 60+ unique labs and 100+ different exercises. Technical skills, frameworks, and tools are taught through hands-on exercises in a safe virtual environment.

Flexible Learning

Our online platform allows learners to study and practice at their own pace. The cohort-based concept provides a supportive community environment that maximizes engagement.

Accelerated Program

Our accelerated learning methodology and streamlined curriculum focus on teaching the specific skills needed to hit the ground running in the cyber industry.

Industry Leading Certifications

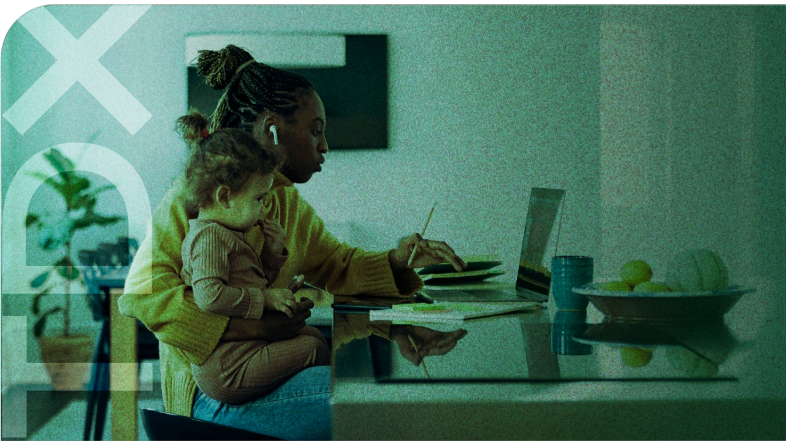
Our curriculum is aligned with CertNexus for CyberSec First Responder®. A discount for CertNexus® certifications and prep material is available to learners upon completion of the bootcamp.

Career Services and Support

Our dedicated team of career success professionals provides guidance and support throughout the job-seeking process. Upon completion, learners also connect to a global alumni network and community.

Staying Ahead of the Curve

We regularly update our curriculum to keep pace with the latest in cybersecurity, including AI and new technologies.



A Learn-From-Anywhere Program for a Work-From-Anywhere Career

The next cohort is starting soon, contact admissions today at (212) 448-4485 to learn more about getting started.

About ThriveDX

ThriveDX is the global leader in cybersecurity education, and an expert in providing cybersecurity training to upskill and reskill lifelong learners. Our teams are made up of military-trained cyber experts, industry veterans, and seasoned educators united to close the worldwide skills and talent gap in cybersecurity. Operating in two divisions–education and enterprise–ThriveDX's award-winning solutions exist to bridge the skills gap and impact the talent shortage in the cybersecurity and overall tech industry.

For more information, visit https://thrivedx.com/