ThriveDX | For Enterprise

Cyber Academy Syllabus

Futureproofing Your Cybersecurity Workforce

ThriveDX's comprehensive cybersecurity bootcamp is an accelerated training program designed to successfully prepare people with little or no background in IT for entry-level jobs in cybersecurity.

Built upon military training methodologies and hands-on learning, our training adheres to the globally recognized NICE-NIST 800-181 framework. It equips learners not only with technical knowledge but also with the practical cybersecurity skills necessary for career excellence.

ThriveDX's Methodology

ThriveDX's learning methodology focuses on teaching the specific skills required for success. This is achieved through:

Practical and theoretical knowledge delivered through demos, real-world examples, videos, infographics, quizzes, and games	Technical skills, frameworks, and tools taught through hands-on exercises in a safe virtual environment	Essential soft-skills training – from teamwork to mindset – embedded throughout the program

Instructional Format

Our bootcamp offers best-in-class content in flexible formats:

- Full time, 3 months: 4 hours daily with the bootcamp facilitator and 4 hours individual online work
- Part time, 6 months: Classes occur only twice a week, 4 hours each day
- Hybrid, 6 months: Live classes are replaced by async fascilitator support and students learn on their own schedule as according to weekly goals

All learners gain access to a training platform consisting of 300+ virtual labs and 1000+ hours of quality content, as well as hands-on experience with real-world simulation practices that accurately reflect the constantly evolving nature of cybersecurity.

Structured Flexibility: In the full-time format, the bootcamp offers an immersive learning experience, allowing students to deeply engage in daily sessions with the bootcamp facilitator and 4 hours of independent online work. The part-time and hybrid formats provide flexibility for learners to accommodate work-life schedules while providing essential structure and support for successfully completing the training.

ThriveDX | For Enterprise

Bootcamp Structure

1

Prework

Prior to the start of the bootcamp, learners will complete the self-paced Prework module, whose objective is to bring everyone to the same level of technical expertise.

2

Foundational Modules

The first part of the bootcamp covers the foundations of cybersecurity. This includes the modules bootcamp Introduction, Network Administration, Cybersecurity Fundamentals, Network and Application Security, and Incident Handling.

3

Midterm

After the first part of the bootcamp, learners will take a midterm exam.

4

Advanced Modules

The second part of the bootcamp dives deeper into advanced topics and introduces learners to different areas of specialization. These modules include Forensics, Malware Analysis, Ethical Hacking and Incident Response, Secure Design Principles, Risk Management, and Threat Intelligence.

5

Final Assessments

During the last module, bootcampers will complete several final scenarios and a final exam.

Syllabus

Prework

Prior to the start of the bootcamp, learners are required to complete the self-paced Prework module, whose objective is to bring everyone to the same level of technical expertise. Learners will review topics including operating systems, networks, and the basics of cybersecurity. The Prework can take anywhere from 10-40 hours depending on the learner's technical background.

Topics Covered:

- The cybersecurity field, the main challenges in the industry, and why a career in this field is a wise choice.
- The cybersecurity mindset and “learning how to learn".
- Computer fundamentals, operating systems (Windows, Linux, macOS), and command line utilities.
- Computer networks, the OSI model, and main network protocols.
- MITRE ATT&CK Framework tactics and techniques.

Tools: Wireshark, Putty

I. Bootcamp Introduction

The Bootcamp Introduction provides learners with the tools required to make the bootcamp an enjoyable and efficient learning experience. During this module, they will learn how the bootcamp will be structured as well as the basics of computers.

Topics Covered:

- Overview of bootcamp and Cybersecurity Industry
- Cybersecurity Career Paths
- Prework Content Review

II. Network Administration

In the Prework module, bootcampers are taught the fundamental principles and concepts of networking. This module dives even deeper and focuses on designing, configuring, and troubleshooting networks. bootcampers will learn the necessary skills for running and monitoring a network in an insightful manner.

Topics Covered:

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

Tools: Cisco Packet Tracer, Nmap, Windows PowerShell

III. Cybersecurity Fundamentals

This module covers what cybersecurity is, its importance, and how organizations apply cybersecurity. bootcampers will learn about vulnerabilities, exploits, and threats, as well as how they work. They will also learn about famous hackers from the 1950s to the present. This module will then look at different types of attackers, their motivations, capabilities, strategies, and the various types of malware they use 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 Cyber-Attacks
- Famous Cyber Incidents In The Industry

IV. Network and Application Security

In this module, bootcampers will learn about network and application security defense methodologies. They will be able to identify which tools are required based on the network and the needs of the organization. The module will also cover the construction of secure network architectures. For each method, bootcampers will learn how to detect and eventually block malicious actors from carrying out cyber-attacks 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

V. Incident Handling

This module will teach bootcampers about the most common cybersecurity attack types in the web, domain, and malware areas. They will learn the goal of each type, how they work, their impact, and how to detect them. Then, they will practice detection and analysis of incidents in security applications as they learned in the Network & Security Application module and will practice the role of a cybersecurity analyst in real life.

Topics Covered:

- Types Of Attacks in The Web Area (DDOS, SQL Injection, XSS, LFI, Command FInjection)
- Types Of Attacks in The Domain Area (Typo Squatting, Domain Hijacking, Pass The Hash, Pass The Ticket, LDAP Reconnaissance, Brute Force)
- Types Of Attacks in The Malware Area (Ransomware, Virus, Worm, Trojan Horse, Adware)
- Practicing The Role of SOC Analysts by Detecting And Analyzing Alerts And Incidents In Splunk, SIEM, And EDR
- Analyzing Malicious Indicators Using Virus Total and Do cumenting the Findings
- Group and Individual Incident Report Writing

Tools: Splunk, In-House SIEM, Wazuh, VirusTotal, Powershell, Wireshark

VI. Forensics

In this module, bootcampers learn digital forensic processes for analyzing threats in digital devices. This includes 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

VII. Malware Analysis

Bootcampers will learn different techniques for analyzing malicious software and understanding its behavior. This will be achieved using several malware analysis methods such as reverse engineering, binary analysis, and obfuscation detection, as well as by analyzing real-life malware samples.

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

VIII. Ethical Hacking and Incident Response

As future cybersecurity analysts, bootcampers must understand cyber warfare's offensive methodologies. In Ethical Hacking, participants will learn how to perform cyber-attacks, providing them insights into cyber defense best practices, vulnerability assessments, forensics, and incident response processes. In Incident Response, bootcampers will learn the relevant response methodologies used once an attack has occurred. They will overview identifying cybersecurity breaches, insider/outsider threats, incident response life cycles, performing relevant assessments, and developing protection plans.

Topics Covered:

- What is Hacking and Ethical Hacking and the Penetration Testing Frameworks
- Ethical Hacking Phases: Reconnaissance, Scanning, Obtaining Access, Maintaining Access, Covering Tracks, and The Cyber Kill Chain.
- Network Hacking - Metasploit Framework
- Web Application Hacking - OWASP Top 10 – XSS, SQL Injection, Manual and Automated Attacks
- Post-Incident Activities
- Capture the Flag Challenge

Tools: Metasploit, SQLMap, Nmap, OSINT Framework, CUPP, Hydra, Recon-ng, Burp Suite

IX. Secure Design Principles

In this module, bootcampers will learn about trend analysis and how to perform it. They will become familiar with the newest cybersecurity trends, threats and more. Furthermore, bootcampers will learn 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

X. Risk Management

In this module, bootcampers will learn about risk management, and dive into the cybersecurity aspects involved. In today's world,every action we take can become a potential risk. Therefore, bootcampers will learn risk management methodologies and processes that will 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

Tools: ThriveDX Security Awareness Training

XI. Threat Intelligence

One of the ways to protect your organization is to know your enemy. In this module, participants will learn the 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: Elasticsearch, Kibana, Webhose data (logs from the darkweb), Web Scraping, Tor Browser, IntSights Threat Intelligence Platform

XII. Final Scenarios

The final module includes real-life scenarios of cybersecurity incidents and a final exam covering all the content learned along the bootcamp. Learners will present group projects which were worked on throughout the course. In addition, bootcampers will dive into the day-to-day work performed by five distinct cybersecurity roles that students have been prepared for since the beginning of the bootcamp. These roles, meticulously modeled on the NIST framework, include Cyber Defense Infrastructure Support Specialist, Network Operations Specialist, Cyber Defense Analyst, Cyber Defense Forensics Analyst, and Cyber Defense Incident Responder.

Topics Covered:

- Finale exam`
- Cybersecurity Roles: To foster a unique interest and enthusiasm within the learning experience, we portray these roles as cybersecurity superheroes, each with unique powers and responsibilities.
- Real-World Scenarios: We've unveiled five immersive scenarios, mirroring the daily work of the five Cyber Defenders. These scenarios give students a chance to apply their skills to real-world challenges and build a robust portfolio.

Optional: CompTIA@ Security+ Certification Exam Prep Course

The ThriveDX Cyber Academy training bootcamp includes an 8-week elective CompTIA® Security+ exam prep course designed to prepare learners for this valuable industry certification. It also provides a voucher for the CompTIA® Security+ certification exam upon completion. This course equips students with the essential knowledge required in the field. It is offered in a flexible format, allowing participants to learn at their own pace asynchronously, even after work hours.