Cybersecurity Bootcamp for IT Professionals

SYLLABUS

The Cybersecurity Bootcamp for IT Professionals powered by ThriveDX Impact is a 280-hour cybersecurity training program designed to prepare individuals with previous experience in IT to transition into a new and exciting career in cybersecurity, a highly in-demand and lucrative profession.

THRIVEDX'S METHODOLOGY

The Bootcamp was developed under the principle of "everything you need to know but only what you need to know." ThriveDX's accelerated learning methodology – based on military bootcamps – focuses on teaching the specific skills required for success. This is accomplished with:

- 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 communication – embedded throughout the program.

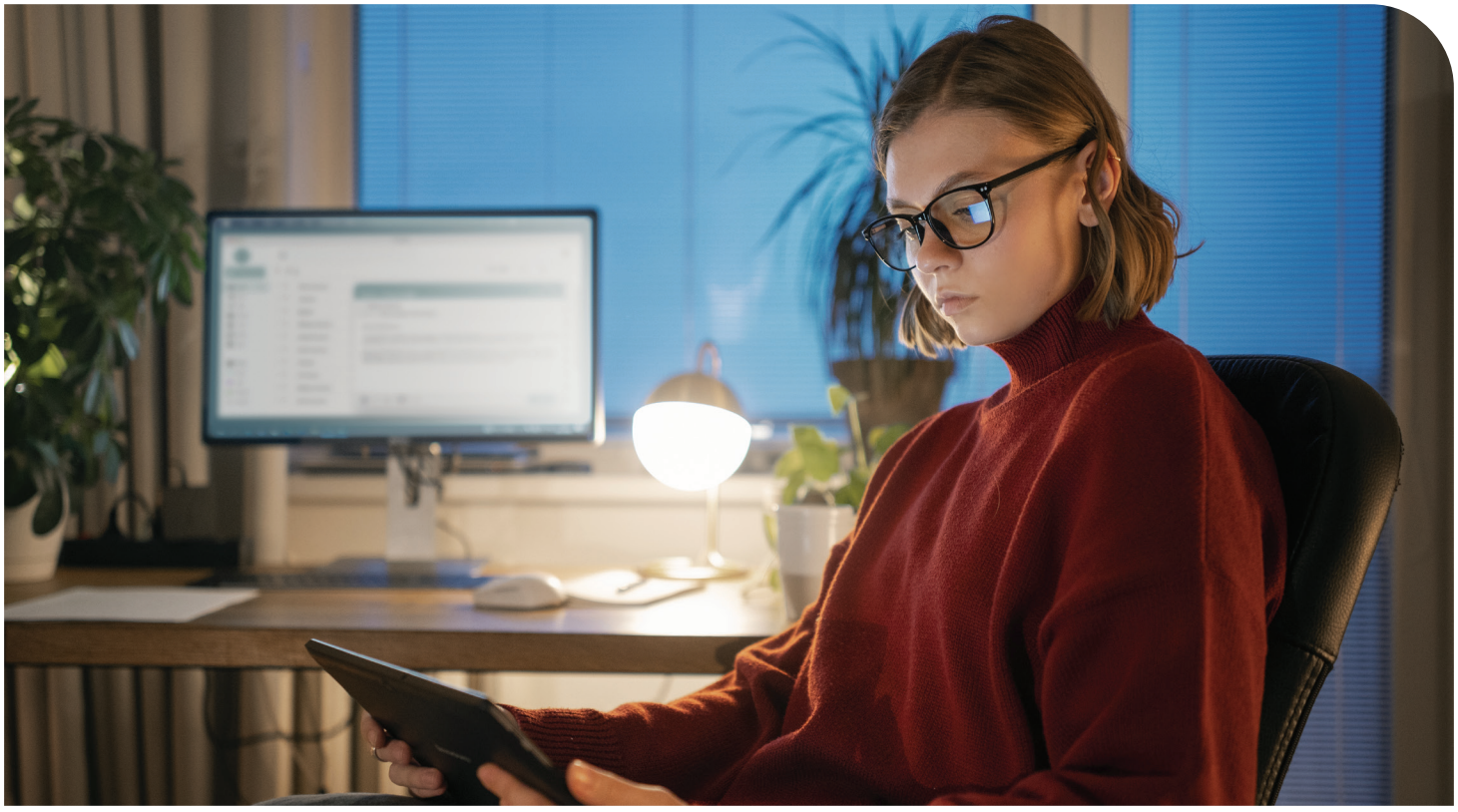
BOOTCAMP STRUCTURE

01
PREWORK
Before the start of the Bootcamp, learners are required to complete a self-paced refresher module, which reviews topics on Network Administration. After passing its exam, learners can begin the Bootcamp.

02
FOUNDATIONAL MODULES
Before the start of the Bootcamp, learners are required to complete a self-paced refresher module, which reviews topics on Network Administration. After passing its exam, learners can begin the Bootcamp.

03
ADVANCED MODULES
Before the start of the Bootcamp, learners are required to complete a self-paced refresher module, which reviews topics on Network Administration. After passing its exam, learners can begin the Bootcamp.

04
FINAL ASSESSMENTS
Before the start of the Bootcamp, learners are required to complete a self-paced refresher module, which reviews topics on Network Administration. After passing its exam, learners can begin the Bootcamp.



PREWORK - NETWORK ADMINISTRATION

Prior to the start of the Bootcamp, learners are required to complete the online self-paced Prework module Network Administration, whose objective is to refresh topics for bootcampers as well as provide an opportunity to familiarize themselves with the platform. The module focuses on designing, configuring, and troubleshooting networks. The Prework can take anywhere from 10-40hours depending on the learner's technical background.

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.

NETWORK AND APPLICATION SECURITY

In this module, bootcampers 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. It also covers construction of secure network architectures. For each method, bootcampers learn how to detect and eventually block malicious actors from carrying out cyber-attacks and crimes.

Topics Covered

- Cryptography – Symmetric vs Asymmetric Keys
- Encryption/Decryption, Hash functions
- Security Architecture
- Security Tools – Firewalls, Antivirus, IDS/IPS, SIEM
- Access Control Methods, Multi-factor Authentication, Authentication Protocols
- System Administration

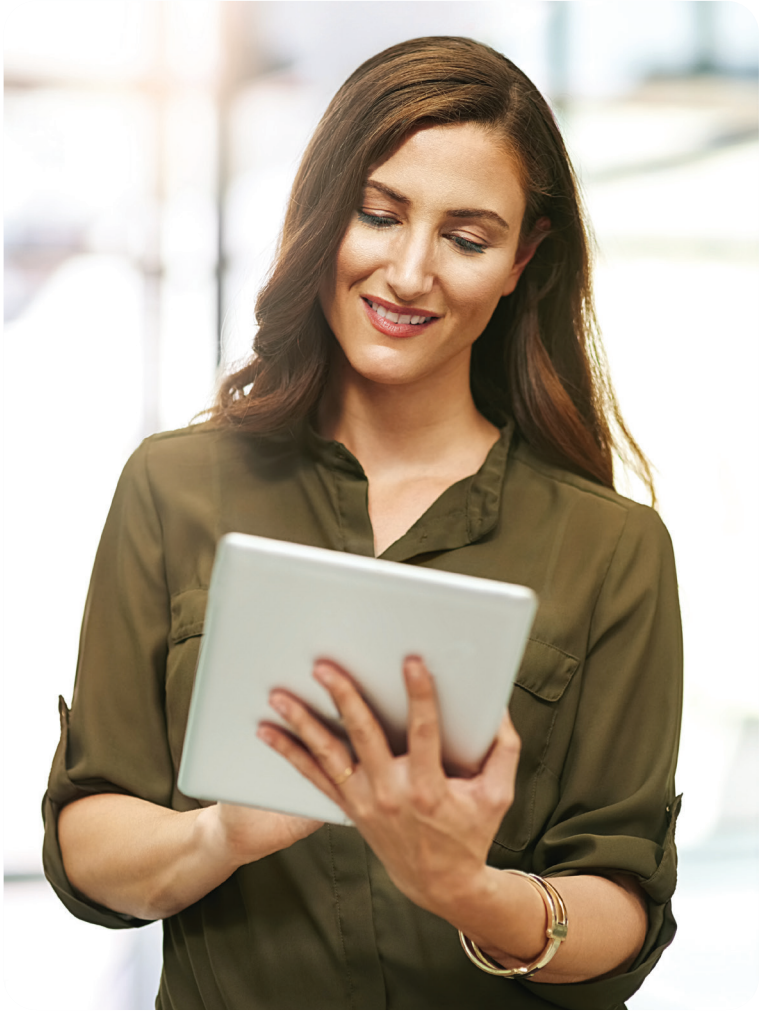
Tools: Kali Linux, Splunk, Snort IDS, Active Directory, Nmap, OpenVPN, Windows Firewall, Linux iptables

CYBERSECURITY FUNDAMENTALS

This module is designed to teach how organizations implement cybersecurity and introduce the different roles in the industry. Additionally, bootcampers will get to know the history of famous hackers from the 1950s until today. The module then explores modern hackers and their motives, capabilities, and techniques, as well as the different typesof malwares they use to attack their victims.

Topics Covered

- NIST Framework
- Malware Types
- Social Engineering
- Vulnerabilities, Risks, and Exploits
- Famous Cyber-Attacks



INCIDENT HANDLING

In this module, bootcampers learn about the most common types of cybersecurity attacks. They will practice detection and analysis of incidents as a Cybersecurity Analyst would in real life. They will also analyze different attack vectorsand their attributes and identify false-positive cases.

Topics Covered

- Detection and Analysis of Cyber-Attacks – DDos/ Dos, Brute-Force
- OSWAP Top 10 Attacks – SQL Injection, Cross-Site Scripting
- Group and Individual Incident Report Writing

Tools: Splunk

ETHICAL HACKING AND INCIDENT RESPONSE

As future Cybersecurity Analysts, it is essential for bootcampers to understand offensive methodologies in cyber warfare. In Ethical Hacking, they will learn how to perform cyber-attacks, which will provide them with insights on 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

- Ethical Hacking Processes and Methodologies
- Network Hacking, Reconnaissance, Google Hacking and Locating Attack Vectors
- Web Application Hacking, OWASP Top 10 – XSS, SQL Injection, Manual and Automated Attacks
- Post Incident Activity

Tools: Metasploit, SQLMap, Nmap

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, Magent RAM Capture, Redline, HxD

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, they 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

FINAL SCENARIOS

The final module includes real-life scenarios of cybersecurity incidents, and a final exam covering all the content learned along with the Bootcamp. This ensures bootcampers have gained the necessary technical knowledge and practical skills to begin their new career in cybersecurity.