IMPACT BOOTCAMP SYLLABUS

Intro to Cyber
Intro to Cyber is an online, self-paced, 30-hour introductory course that's ideal for learners who are curious about the world of cyber and want to get familiar with this exciting industry. The course is the best way for students to gain the fundamentals of cybersecurity, discover the different roles in the field and learn how each makes an impact, and become the next generation of cyber professionals.

Topics Covered:
- The Cybersecurity World and Crime
- Attackers and APTs
- Mitigating the Risk and Taking Control

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 is structured and get more information on the basics of computers.

Topics Covered:
- Overview of Bootcamp and Cybersecurity Industry
- Cybersecurity Career Paths
- Prework Content Review

II. NETWORK ADMIN
The Network Administration module dives even deeper and focuses on designing, configuring, and troubleshooting networks. Learners will obtain 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. Bootcamp participants 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 types of attacks they use to target their victims.

Topics Covered:

- Most Common Vulnerabilities, Risks, And Threats
- Main Concepts In Cybersecurity
- Types Of Malware And Attackers
- NIST & International Cybersecurity Framework
- Most Common Cyber Attacks
- Famous Cyber Incidents

IV. NETWORK AND APPLICATION SECURITY

In this module, bootcamp participants 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 also covers construction of secure network architectures. For each method, learners will understand 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 students 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 & Application Security 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 Injection)
- Types Of Attacks in The Domain Area (Typosquatting, 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 Documenting the Findings
- Group and Individual Incident Report Writing

TOOLS:

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

VI. FORENSICS

In this module, bootcamp students 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

Bootcamp students 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, it is essential for learners 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, bootcamp participants 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

- Exploitation Techniques
- Web Application Hacking, OWASP Top 10 – XSS, SQL Injection, Manual and Automated Attacks
- Post Incident Activity

TOOLS:

- Metasploit, SQLMap, Nmap

IX. SECURE DESIGN PRINCIPLES

In this module, students will learn about trend analysis and how to perform it. They will become familiar with the newest cybersecurity trends, threats and more. Furthermore, participants 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, bootcamp students will learn about risk management, and dive into the cybersecurity aspects involved. In today's world, almost any action can become a potential risk. Therefore, learners will dive into risk management methodologies and processes that assist in effectively managing such risks – while understanding that not all risks can be eliminated entirely.

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

XI. THREAT INTELLIGENCE

In this module, students learn about the need of security governance in any type of organization. Participants will learn how to train employees to avoid threats and how to minimize vulnerability to these types of attacks.

Topics Covered:

- Security Governance
- Employees Education

TOOLS

- ThriveDX Security Awareness Training (Formerly Lucy)

XII. FINAL SCENARIOS AND INTERVIEW PREP

The final module includes real-life scenarios of cybersecurity incidents, and a final exam covering all the content learned during the bootcamp. Learners will be equipped to demonstrate their technical, transferable, and soft skills in job interviews.


FOUNDED 1855
EUREKA
COLLEGE


ThriveDX