Cyber Bootcamp

Curriculum Package

LIGHTHOUSE LABS

Powered by Cybint

Cyber Bootcamp Overview: Your Cyber Career Starts Here

Cyber Bootcamp is an accelerated cybersecurity training program that prepares people with little or no IT background for cybersecurity careers. In just 12 weeks, this hands-on virtual training program gives you the practical skills you need to land your first role in the booming cybersecurity industry. Cyber Bootcamp provides a top-notch learning environment and industry-aligned curriculum as well as mentorship and job-search support for positions such as a Cybersecurity Specialist or Technician, a SOC Analyst Level 1, or a Cybersecurity Incident Analyst or Responder.

Why Cybersecurity?

Cybersecurity is the fastest growing market in technology, with 30x growth over the last decade. The industry's rapid growth and ongoing expansion have created considerable skills and job gaps, with virtually no unemployment for nearly a decade. With plentiful opportunities and competitive compensation, Cyber Bootcamp gives you the skills to launch a lucrative, future-proof career in cybersecurity.

Who Is Cyber Bootcamp For?

Cyber Bootcamp is an excellent fit for non-technical people as well as those with some security or digital experience, including recent graduates and those looking for a career pivot or to reskill. Successful applicants thrive on problem-solving, collaboration and attention to detail. If you're looking for a dynamic and rewarding career, you've come to the right place.

Education Approach: How We Do It

Intensive and immersive, Cyber Bootcamp takes a hybrid virtual approach, mixing live online classrooms and self-guided learning. We developed the bootcamp under the principle of "everything you need to know but only what you need to know." With an accelerated learning methodology based on military bootcamps, we focus on teaching students the specific skills they will need for success.

We accomplish this 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**, including teamwork and interview prep, embedded throughout the program

During Bootcamp

- Intense and immersive learning environment with mentor feedback
- Curriculum based on National Initiative for Cybersecurity Education (NICE)
- Access to cybersecurity experts for Q&A
- Guidance on resume-building and job-searching

Upon Graduation

- 12 months of continued access to Cybint's online learning platform
- Connection to our alumni and career network
- A new career as a Cybersecurity Specialist/Technician, Cybersecurity Incident Analyst/Responder and/or Cybersecurity Analyst

12-week Bootcamp

Industry-Driven Education

On-Demand Mentorship

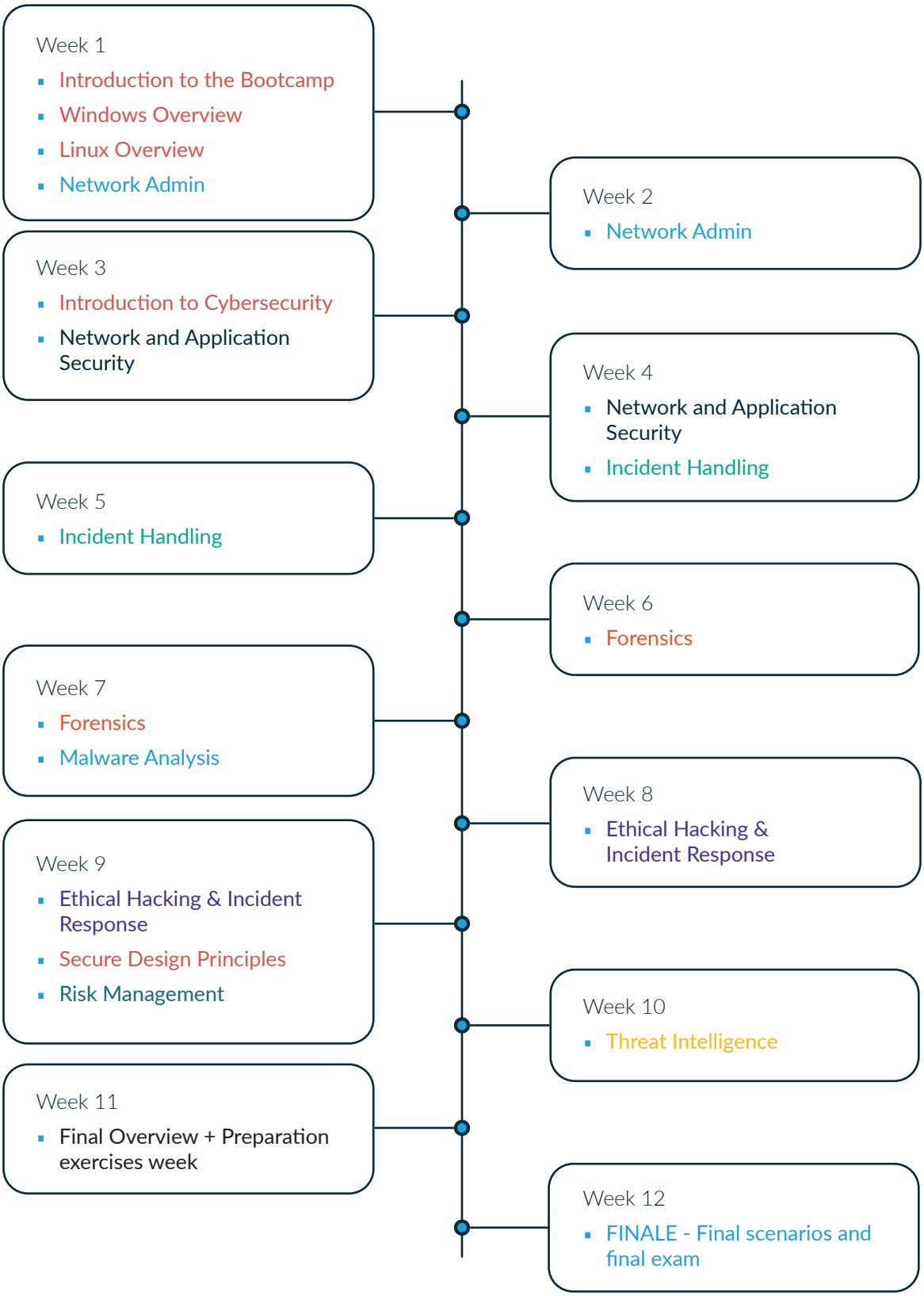
Personalized Learning through Small Class Sizes

Bootcamp Outcomes: The Skills You Need

At the end of Cyber Bootcamp, you will be able to:

- ✓ Understand how threat actors operate, their objectives and skills
- ✓ Assist organizations with their cybersecurity defence strategy to ensure business continuity
- ✓ Analyze, dissect and respond to cybersecurity incidents to protect organizational assets
- ✓ Analyze the various security attack vectors and their mitigations to strengthen an organization's cybersecurity position
- ✓ Use digital forensic processes for analyzing threats in digital devices
- ✓ Identification, recovery, investigation, and validation of digital evidence in computers and other media devices
- ✓ Apply malware analysis techniques, such as reverse engineering, binary analysis and evasion detection to dissect malware and understand its malicious objectives
- ✓ Apply offensive methodologies to your security operation role by learning the attack life cycle in cyber warfare
- ✓ Detect and respond to insider and outsider security threats by learning the incident response life cycle
- ✓ Perform trend analysis
- ✓ Assess security designs and uncover flaws
- ✓ Apply threat intelligence collection processes to improve detections and proactively prevent threats

Bootcamp Roadmap



Bootcamp Structure

Prework

The self-paced Prework Module gets all students to the same level of technical expertise before the Bootcamp begins.

Foundational Modules

The first part of the Bootcamp covers the foundations of cybersecurity in five modules:

- Bootcamp Introduction
- Network Admin
- Introduction to Cybersecurity
- Network and Application Security
- Incident Handling

Midterm

At the halfway mark, a Midterm Exam tests your learning so far. You must get a grade of at least 60% to pass.

Advanced Modules

The second part of the Bootcamp dives deep into advanced topics, introducing students to different areas of specialization, including:

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

Final Assessment

In the last module, students complete three scenarios and take the final exam. The passing grade is 60%. This final phase also focuses on job interview preparation.

Module-by-Module Breakdown

PREWORK

Prior to the start of the Bootcamp, students are required to complete the self-paced Prework module, whose objective is to bring everyone to the same level of technical expertise. This module will familiarize students with the Cybint platform and acknowledge key details of the Bootcamp. The Prework can take anywhere from 10–40 hours depending on their technical background.

Topics Covered:

- Basics of Computer and Device Hardware, Software, Operating Systems and Processes in Windows and Linux
- Networking Basics and the OSI Model

TOOLS: Wireshark, Putty

I. BOOTCAMP INTRODUCTION

The Bootcamp Introduction will provide students with the tools required to make the Bootcamp an enjoyable and efficient learning experience. During this module, students 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 ADMIN

In the Prework module, we covered the fundamental principles and concepts of networking. This module will dive even deeper and focus on designing, configuring, and troubleshooting networks. Students will be taught 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. INTRODUCTION TO CYBERSECURITY

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

Topics Covered:

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

IV. NETWORK AND APPLICATION SECURITY

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

Topics Covered:

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

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

V. INCIDENT HANDLING

In this module, students will 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. Students will analyze different attack vectors and 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

VI. FORENSICS

In this module, students will 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

Students will learn different techniques for analyzing malicious software and understanding its behaviour. 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
- Android APK Analysis

TOOLS: HashCalc, Exeinfo PE, PDF Stream Dumper, FileAlyzer, HxD, Yaazhini Vulnerability Scanner, APKTool, Ghidra, HashCompare, UPX Easy GUI, Wireshark

VIII. ETHICAL HACKING AND INCIDENT RESPONSE

As future Cybersecurity Analysts, it is essential for students to understand offensive methodologies in cyber warfare. In Ethical Hacking, students will learn how to perform cyber-attacks, which will provide them insights on cyber defense best practices, vulnerabilities assessments, forensics, and incident response processes. In Incident Response, students will learn the relevant response methodologies used once an attack has occurred. Students 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 PRINCIPALS

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, students will learn cybersecurity design best practices, as well as hot 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, students 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, students 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

XI. THREAT INTELLIGENCE

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

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 along the Bootcamp. In the Full-Time Bootcamp, students will present group projects which were worked on throughout the course. We will also review technical and soft-skill preparation for job interviews.

Career Pathway: The Fast-Track to Your First Job

Cyber Bootcamp gives you the entry-level skills needed for your first year as a Cybersecurity Specialist/ Technician, Cybersecurity Incident Analyst/Responder or Cybersecurity Analyst. The program doesn't teach everything you need to know to become an expert–that takes years of practice. It's designed to teach you a way of thinking and problem-solving, providing the tools to **successfully start in the profession** and continue your learning on the job.

Career Services

We will give you the skills, tools and expertise to succeed on your job hunt now and in the future, including:

- Resume-writing workshop, resume review
- Job interview workshop
- Advice for situations such as networking, relocation and salary negotiation
- Listings of tech-specific job boards
- Listings for industry networking opportunities
- One-on-one guidance for concerns or situations you encounter along the way
- Industry networks you can leverage to connect with employers
- Connections to potential employers at our private events and industry gatherings, such as job fairs, networking events
- Post-bootcamp follow-up to ensure your job hunt is on track

Life After Bootcamp

To facilitate the jump from the classroom to the workplace as quickly as possible, we set the expectation with both students and employers that you are open to starting your career in a paid internship, apprenticeship or training capacity for the first three to four months. This model shortens the time it takes students to find positions post-bootcamp, with most being offered full-time jobs at the end of the internship.

Alumni who don't continue past the internship period have the full support of our Career Services team to help secure their next full-time position. We are constantly connecting our graduates and hiring partners. Employers are not obligated to hire from the Cyber Bootcamp, but we have an excellent reputation in the community and hiring partners see us as a trusted place to find talent. As a result, we cannot predict or guarantee that a specific employer (or type of employer) will be in the market for these roles at the time of your graduation.

Many students come to bootcamp with a "dream job" in mind, and we are happy to work with you to help you reach that goal immediately upon graduation. However, our Career Services process focuses on prioritizing your continued learning.

APPLY TO CYBER BOOTCAMP NOW

LIGHTHOUSE LABS

About Lighthouse Labs

Lighthouse Labs was launched in 2013 with the goal of finding innovative ways to train the next generation of tech talent. In an age of technological disruption across every industry, our mission is to give Canadians the skills they need to find long-lasting careers in a digital workforce. Eight years later, we've delivered hands-on technology and data education to over 30,000 Canadians, equipping them with the relevant tools to thrive in the future of work.

With the support of a brilliant team of instructors and mentors, we continue to empower students, launch careers, and contribute to the incredible growth of Canada's tech industry.

CYBER BOOTCAMP

Curriculum Package

LIGHTHOUSE LABS

Powered by Cybint