Cyber Security Program

Curriculum Package

LIGHTHOUSE LABS

The Lighthouse Labs Experience

LIGHTHOUSE LABS

Our digital world is increasingly more complex and interconnected. As cyber security rapidly becomes the fastest growing field in tech and the demand for cyber security professionals increases daily, we're doing our part to train the next generation of tech talent and make tech more accessible and inclusive. With the support of a diverse community of mentors, student success coordinators, and career services advisors, our outcomes-driven program is designed to give you the in-demand skills you need to become an effective and impactful cyber security professional.

Industry-Driven Education

Personalized and Immersive

Real-World Experience

Hands-On Learning

At Lighthouse Labs, we're committed to building a diverse and inclusive learning community. If you need help and support, we're here for you — no matter where you are in the process.

Build Real-World Experience

Personalized, outcomes-driven cyber security training that meets you where you're at. Even if you have zero tech or industry experience, there are many pathways to start and advance your career in cyber security. In fact, companies are looking to hire applicants with non-traditional backgrounds—like those graduating from short-term, intensive cyber training programs—to fill critical workforce needs. This gives you the unique opportunity to build on your existing strengths, education, unique insights, and transferable skills.

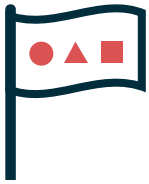
Your learning journey at Lighthouse Labs will give you the experience and practical skills you need to land your first entry-level job as a Cyber Security Analyst, Information Security Analyst, Incident Responder/Handler, Network Security Specialist, or Risk Analyst, among other cyber security roles.

Our annual **Student Outcomes Report** is a validation of our reputation for solid outcomes for our students - **an impressive 96% employment rate** for all graduates, with 89% of job-seeking graduates finding a job within 180 days of graduation.

Learn How to Learn

We've built a carefully crafted curriculum with cyber security and technology experts who know what you need to succeed as a cyber security professional. To ensure your success in an ever-changing landscape, our program sets you up with the tools you need to be a lifelong effective, adaptive, and curious learner throughout your career.

Cyber Security Pillars



Fundamentals

Networks

Operating Systems (OS)
Linux and Windows

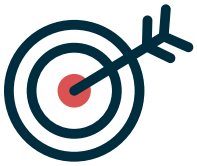
Shell Commands

Batch Files

Wireshark

Python

Firewalls



Industry Relevance

Industry Frameworks
NIST and ISO

Compliance Frameworks
GRC Management Framework

Vulnerability Frameworks
PCI Mapping, PCI Index, Nessus-Scanner Reporting, CWE, CVE, NVD

Incident Response
NIST Incident Handling Process
NIST vs. SANS Attack Vectors
NIST Containment
NIST Audit and Review

Defensive Security

Security Incident and Event Management (SIEM)

IDS (SNORT)

Wi-Fi Monitoring

Risk Assessment Tools

Cryptographic Tools

Syslog

Our Educational Approach

Hands-On Experience

Knowledge is gained through experimentation. Technical skills, frameworks, and tools taught through hands-on exercises and labs. You'll get the opportunity to become familiar with these tools and frameworks throughout the course. You'll also share findings with your peers, learning how to develop reports, recommendations, and presentations tailored to specific business audiences. Throughout the program, you'll benefit from feedback from our expert instructors to ensure your progression.

Virtual Labs

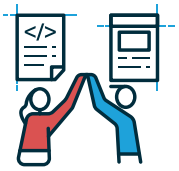
To ensure you get hands-on experience, we also use virtual labs. A virtual lab is a simulated environment that allows students to practice and apply the concepts and skills in safe and controlled setting thanks to virtualized hardware and software components. In these online labs, you'll learn how to configure and monitor a virtual network, analyze and respond to cyber threats, and leverage security tools and techniques to identify and mitigate vulnerabilities.

Effective Communication

Knowing how to communicate cyber security risks is just as important as knowing how to identify them. Strong communication skills can help you persuade stakeholders to take cyber threats seriously. To ensure the security and reliability of systems and networks, we'll teach you how to write reports that clearly communicate information about threats and vulnerabilities to stakeholders like management teams, business clients, and other cyber security professionals.

A Support Ecosystem Adapted to Your Needs

On-Demand Mentorship



Mentorship is the backbone of our programs. If you're stuck on a tricky assignment, you can count on our outstanding mentors to be there for you at the click of a button. As working industry professionals, our mentors are also key in building industry connections to support your future career success.

Proactive Student Support

Support from the day you apply to the day you graduate.
We pride ourselves on our hands-on, proactive education approach, so you can expect daily and weekly check-ins from Student Success Coordinators to track your progress and support your student experience.

Accessible Education

We're committed to building a diverse and inclusive learning community. If you need help and support as a student, we're here for you. Accessibility is not one-size-fits-all, so neither is your accommodation plan. We work with each student to develop personalized plans that support their individual needs.

Learn more about accommodations and accessibility at Lighthouse Labs on our website.

Curriculum Breakdown

Prep Work

There's a bit of homework you need to complete before the first day of class. The prep work sets you up for success — it equips every student with the same technical skills and foundation before the program begins.

In this module, you'll gain an understanding of cyber security principles and roles, computers and operating systems, and networks.

IT Essentials

- **Single-Site Network Management**
- **Networking Issues Troubleshooting**
- **TCP/IP Concepts and Network Usage**
- **Basic Network Segmentation Planning**
  VLANs
  Firewalls
  VPNs

Security Essentials

- **Risks, Vulnerabilities, Exploits and Threats**
- **Mitigation Strategies and Assessment Tools**
- **Confidentiality, Integrity and Availability (CIA)**
- **Attack Pattern Identification**
- **Log, System, and Network Traffic Analysis**
- **Cryptographic Processes and Confidentiality and Integrity Enhancements**
  - Encrypt and Decrypt
  - Key Exchange
  - Signed Certificates
- **Industry Standard Frameworks**
  - NIST Risk Management Framework
  - NIST National Vulnerability Database
  - Common Vulnerability Scoring System

Programming for Cyber Security

- **Scripting Batch and Bash Files**
  - Regular Expressions (Regex)
  - Variables, Conditions and Loops
  - Shell Scripts
- **Introduction to Python**
  - Scripts, Procedures and Automation
  - Filtering and Sorting Algorithms
  - Debugging

Blue Team Fundamentals

- **Blue Team Roles, Responsibilities, and Development**
- **Organization Chart and Functional Report Optimization**
- **Red, Blue and Purple Team Functions and Relationships**
- **Security Operations Centres (SOC)**
  - Chain of Command
  - Shift Change Reports

Governance, Risk and Compliance (GRC)

- **GRC, Blue Teams and Business**
- **Security Decision Making Processes**
- **Compliance Frameworks (ISO/NIST)**
- **Compliance Report Development**
- **Communicating with Executive Audiences**

Curriculum Breakdown

Vulnerability Assessment

- Vulnerability Assessments and Reviews
- Reporting and Risk Identification Tools
- Communicating High-Risk Items and Remediations to Technical and Non-Technical Stakeholders in Reports

Incident Response

- Incident Categorization and Prioritization
- Rules of Escalation
- NIST Incident Response Lifecycle Phases
- Incident Triage Criteria
- Incident Response Playbooks
- Incident Response Documentation
  - Source
  - Target
  - Suspected Goals
  - Remedial Actions Taken
  - Future Incident Mitigation

Encryption

- Cryptographic Methods for Network Components and Websites (SSL/TLS)
- Asymmetric and Symmetric Key Encryption Cryptanalysis
- Encryption Standards, Protocols and Tools
  - Open SSH
  - Lets' Encrypt
  - Apache Web Server
  - IIS
  - OpenPGP
  - NIST SP 800-52, NIST SP 800-57 and NIST
  - SP 800-175B
  - SSL/TLS Certificates
  - WinSCP
  - PuTTY SSH
  - SmartTTY
  - HTTP and HTTPS
  - Wireshark PCAP

Threat Defence Operations

- Threat Hunting and Network Monitoring
- SNORT Rules
- SIEM
- Intrusion Detection and Prevention Systems
- MITRE ATT&CK, Lockheed Martin Cyber Kill Chain and Diamond Framework Models
- Dwell Times
- Compromised System Assessment
- Intrusion and Intelligence Analysis
- Threat Intelligence Gathering
- Threat Detection Engineering

Forensics

- Computer and Network Forensics Processes
- Malware Analysis
- Organizational Policy Assessment
- Logging System Installation and Configuration
- Digital Investigation and Evidence Acquisition

Secure Architecture

- Security Vulnerability Testing
- Network Architecture Mitigation Planning
- Secure Design Principles
- Software Development Security
- Security Loophole Review and Remediation

Capstone Project

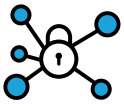
As your final project, you'll assess the security needs of a fictitious company and present your findings while applying everything you've learned throughout the program.

You'll analyze the company's tolerance for risk, vulnerabilities and threats; create an appropriate security policy; monitor for indicators of compromise (IOCs); conduct an incident response; and make recommendations to improve their security posture.

This project will include a complete report, set of policies, and playbook.

Our Tech Stack

LIGHTHOUSE LABS



Network Security

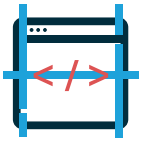
The fundamentals of network and application security are some of the most important tools in your cyber security skillset. You'll learn to recognize, intercept, and block malicious actors from infiltrating an organization's secure networks.

Encryption

Defend against brute-force and cyber attacks, like malware and ransomeware, with encryption. You'll learn how to research, compare, assess, and choose encryption tools and protocols.

Incident Response

Detect and analyze incidents as they happen by looking at modern exploitation techniques. You'll practice incident reporting, study response methodologies, and combine these skills to develop protection plans.



Coding

Learn the basics of programming. You'll create and maintain batch and BASH files, and learn how to write basic Python scripts for cyber security-specific scenarios.

Forensics

Discover the what, where, and when of a cyber attack. Complete a post-attack autopsy as you identify, investigate, and recover digital evidence to defend against future attacks.

Threat Detection Engineering

Learn about the important role of critical security controls and the technologies required to build effective cyber defences and a mature security posture.

Threat Defence Operations

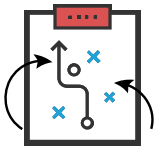
Explore and learn how to communicate the relevance of MITRE ATT&CK Framework, Lockheed Martin Cyber Kill Chain and dwell times to a business audience.

Blue Team

Build an effective blue team, an optimized organizational chart, and a functional security operations centre (SOC) to organize and monitor the security of an organization.

Launch Your Career

Our dedicated Career Services team is here to help you transition from the classroom to your first cyber security job as smoothly as possible.

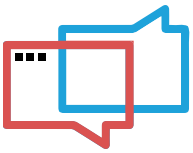


Personalized Coaching

Our team will work with you to map out a rigorous career plan and help you achieve it.

Resume and Interview Help

Detailed feedback and tips will help you perfect your points of contact with potential employers.



Connect with Employers

Tap into our vast network of leading tech employers through events, networking, and more.

Finding a job is no easy task, whether you're pivoting from a different role or looking for your first ever position as a cyber security professional. We're here to help you connect with fulfilling employment that'll keep you developing your abilities and building your skillset on the job. With an excellent reputation within the industry, hiring partners see us as a trusted source for finding talent. We also maintain relationships with an ever-growing network of industry contacts, keeping our finger on the pulse of what employers are looking for in this fast-paced industry. Our expert Career Services team will support you throughout your professional development journey, guiding you through growth even after you leave Lighthouse Labs.

Our support doesn't end at graduation — it's yours for life.

Staying Connected

Community

As an alum, you remain an active part of our community. We host Demo Days, guest speakers, and exclusive alumni events on the regular.

You also gain access to our Alumni Discord channel, where you can keep in touch with your peers, organize educational and social events, and hear about recurring alum events.

Lifelong Learning

As a Lighthouse Labs alum, you will always have access to our curriculum and its future iterations — yes, until the end of time.

Your access to our learning platform never expires. You'll benefit from ongoing lecture notes and learning resources as we continue to iterate our world-class curriculum.

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. We've since delivered hands-on technology and data education to over 40,000 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.

Ready to protect and defend?

Apply Now

LIGHTHOUSE LABS

www.lighthouselabs.ca