PennState Behrend   Continuing Education

Cybersecurity Impact Bootcamp

Accelerate Your Cyber Career in Just 24 Weeks

The **Penn State Behrend Cybersecurity Impact Bootcamp, offered in partnership with ThriveDX**, is a self-paced, accelerated training program designed to successfully prepare learners with little to no background in information technology (IT) for entry-level jobs in cybersecurity–one of the most in-demand technology fields.

Delivered remotely through self-paced classes, our non-credit, non-degree bootcamp enables learners to gain the job-ready skills they need to enter the growing cybersecurity industry.

Overview

Format

Online
Self-Paced

Schedule

12 Hours per Week
Self-Directed Learning

Duration

24 Weeks
480 Hours

Career

Aligned with the
National Initiative for
Cybersecurity Education

Opportunity

Nearly 500,000
Cybersecurity Positions
Unfilled in the U.S.*

Price

$9,995
Payment Plans &
Funding Available

*Source: Cyberseek.org

Methodology

The Penn State Behrend Cybersecurity Impact Bootcamp aims to train students to enter the cybersecurity industry using an accelerated, hands-on model. The learning methodology focuses on teaching the specific skills required for success. This is accomplished with:

- Practical and theoretical knowledge delivered through over 100 hands-on labs and real-world scenarios.
- Technical skills, frameworks, and tools taught through hands-on exercises in a safe virtual environment.
- Essential career-focused and soft-skills training–from teamwork to interview prep–embedded throughout the program.

Aligned with NICE Framework

The National Initiative for Cybersecurity Education (NICE) framework was developed by the National Institute of Standards and Technology (NIST) to define cybersecurity jobs, and the skills learners need to acquire to qualify for them.

The **Penn State Behrend Cybersecurity Impact Bootcamp** aligns with the NICE framework, so that the curriculum is designed to prepare you for the most in-demand and sought-after jobs in cybersecurity.

Upon completion, learners will be prepared for these cybersecurity roles:

- Network Operations
- Systems Administration
- Defensive Cybersecurity
- Systems Security Analysis
- Digital Forensics
- Incident Response

Program Structure

	Learner Outcome	Courses
Introduction	Learn the basics of cybersecurity and discover the different roles in the field. Review operating systems, networks, Artificial Intelligence, and the fundamentals of mitigating security risks.	Intro to Cyber
Foundational Courses	During the first part of the program, learners cover the most common vulnerabilities, risks, and threats in cybersecurity, as well as the fundamentals of networking and network security.	Bootcamp Introduction Network Administration Cybersecurity Fundamentals Network and Application Security Incident Handling
Midterm	After the first part of the bootcamp, learners take a midterm exam. They are expected to achieve a grade of 60% to pass.	
Advanced Courses	During the second part of the program, learners dive deeper into advanced cybersecurity topics and acquire skills pertaining to different areas of specialization.	Forensics Malware Analysis Ethical Hacking and Incident Response Secure Design Principles Risk Management Threat Intelligence
Final Assessment	Learners complete several final scenarios and a cumulative final exam during the last course. They are expected to achieve an overall grade of 60% in their final assessments to earn a certificate of completion and feel prepared to sit for the CertNexus' CFR certification.	

Bootcamp Syllabus

Intro to Cyber

Prior to the start of the bootcamp, participants familiarize themselves with the platform and learn the basics of cybersecurity, including Gen AI, malware, risk management, and career paths. This module also covers operating systems, networks, and fundamental cybersecurity concepts.

Topics Covered:

- Overview of the cybersecurity field, industry challenges, and why a career in this field is a wise choice.
- Computer fundamentals, operating systems (Windows, Linux), and command line utilities.
- Computer networks, the OSI model, and main network protocols.
- Attackers and APTS.
- Present-Day Cyber Threats.
- Artificial intelligence (AI) and Generative AI.

TOOLS: Windows CMD, Linux Terminal, VirusTotal

01 | Bootcamp Introduction

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

Topics Covered:

- Overview of the Bootcamp and Cybersecurity Industry
- Cybersecurity Career Paths

03 | Cybersecurity Fundamentals

This course covers what cybersecurity is and how organizations apply it. Learners acquire knowledge about vulnerabilities, exploits, and threats. They also explore different types of attackers, their motivations, capabilities, strategies, and the kinds of malware used 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 Cyberattacks
- Famous Cyber Incidents in the Industry

02 | Network Admin

This course dives even deeper and focuses on designing, configuring, and troubleshooting networks. Learners acquire 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
- System Administration

TOOLS: Cisco Packet Tracer, Nmap, Windows PowerShell

04 | Network and Application Security

In this course, learners acquire knowledge about network and application security defense methodologies and construction of secure network architectures. Learners will understand how to detect and eventually block malicious actors from carrying out cyberattacks 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

05 | Incident Handling

This course teaches learners about the most common cyberattacks, how they work, their impact, and how to detect them. Then, they practice detection and analysis of incidents in security applications and practice the role of a cybersecurity analyst in real life.

Topics Covered:

- Types of Attacks in the Web, Domain, & Malware Areas
- Practicing the Role of the SOC Analyst by Detecting Alerts, and Analyzing Alerts and Incidents
- Analyzing Malicious Indicators and Documenting the Findings
- Group and Individual Incident Report Writing

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

06 | Forensics

In this course, learners access 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

07 | Malware Analysis

Learners acquire different techniques for analyzing malicious software and understanding its behavior. This is 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

08 | Ethical Hacking and Incident Response

In this course, learners perform cyberattacks and practice relevant response methodologies. They 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

09 | Secure Design Principles

This course exposes learners to trend analysis and how to perform it. They become familiar with the newest cybersecurity trends and threats and 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

10 | Risk Management

In today's world, almost any action can become a potential risk. In this course, learners study risk management and related methodologies and processes that 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

11 | Threat Intelligence

One of the ways to protect your organization is to know your enemy. In this course, learners discover 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: ThriveDX Security Awareness Training (Formerly Lucy)

12 | Final Scenarios and Interview Prep

The final course includes real-life scenarios of cybersecurity incidents and a final exam covering all the content learned during the bootcamp. Learners present group projects which were worked on throughout the course. They also review technical and soft-skill preparation for job interviews.

Included in the Bootcamp

Hands-On Skills Training

Learn job-ready skills with 60+ unique labs and 100+ different exercises. Technical skills, frameworks, and tools are taught through hands-on exercises in a safe virtual environment.

Industry Leading Certifications

Curriculum is aligned with CertNexus for CyberSec First Responder® and CompTIA® Security+.

Flexible Learning

An online platform allows learners to study and practice at their own pace. The cohort-based concept provides a supportive community environment that maximizes engagement.

Accelerated Program

The accelerated learning methodology and streamlined curriculum focus on teaching the specific skills needed to hit the ground running in the cyber industry.

Career Services and Support

A dedicated team of career success professionals provides guidance and support throughout the job-seeking process. Upon completion, learners also connect to a global alumni network and community.

Seize this opportunity to learn the skills you need to start the career of your dreams.

The next cohort is starting soon. Contact our ThriveDX partners today at 814-626-9251 to learn more about getting started.

This Cybersecurity Bootcamp is offered through the Continuing Education services of Penn State Beaver, Penn State Behrend, Penn State Greater Allegheny, and Penn State New Kensington.