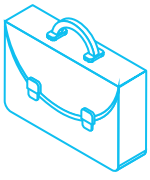
Cybersecurity Bootcamp

Launch Your Career in Cybersecurity

The Cybersecurity Bootcamp at Grand View University powered by Cybint is an accelerated training program designed to successfully prepare people with little or no background in IT for entry-level jobs in cybersecurity, a highly in-demand and lucrative career path.

Developed around military training methodologies and hands-on learning, the program focuses on the key skills sought by employers. The Bootcamp will prepare you not only with technical knowledge, but also with the essential skills necessary for a successful career in cybersecurity.

Accelerated, zero to hero training program



Career-ready skills aligned with NIST-NICE

+100 hands-on real-world exercises

www.grandview.edu/cybersecurity

GRAND VIEW UNIVERSITY

Cybint

Why Cybersecurity?

With the rate of cyber-attacks reaching record highs, there is an urgent need for workers in cybersecurity.

The field has 0% unemployment and forecasts 350% job growth through 2021. With plentiful opportunities and competitive compensation, an accelerated Cybersecurity Bootcamp is the best way to gain the necessary skills to fill these positions.

What Cybersecurity Jobs Can I Get Post-Bootcamp?

This Bootcamp will prepare you to start your career in cybersecurity with entry-level jobs such as:

- Cyber Defense Analyst
- Cyber Incident Responder
- Cyber Forensics Analyst
- Network Operations Specialist
- Cyber Infrastructure Support Specialist

Future-proof job sector

Competitive entry-level salary

Over 4M unfilled cybersecurity positions

www.grandview.edu/cybersecurity

GRAND VIEW UNIVERSITY

Cybint

Our Bootcamp Includes

ACCELERATED PROGRAM

The Bootcamp was developed under the principle of "everything you need to know, and only what you need to know." Our accelerated learning methodology and streamlined curriculum focus on teaching you the specific skills you will need for the job market.

PLUS - Ongoing access to Cybint's online learning platform after graduation, including content updates covering emerging cyber threats and tools.

HANDS-ON SKILLS TRAINING

To ensure you get to practice what you learn, we have developed over 60 unique labs and over 100 different exercises. Technical skills, frameworks, and tools are taught through hands-on exercises in a safe virtual environment.

BLENDED MODEL

Our unique blended model combines the best of both in person and self-paced learning. Our Bootcamp is led by a facilitator, whose role is to support your learning experience, while our online platform allows you to learn and practice during the day at your own pace. Lastly, the cohort-based concept provides a supportive community environment that maximizes engagement.

CAREER SERVICES AND SUPPORT

Essential soft-skills training, from teamwork to interview prep, is embedded throughout the program. Upon graduation, you will also connect to a global alumni network and community.

Bootcamp Tracks

Our Bootcamp is comprised of 480 hours of best-in-class content delivered in two accelerated tracks:

1. **Full time, 3 months:** 4 hours daily with the Bootcamp facilitator and 4 hours individual online work.
2. **Part time, 6 months:** This will cover the same content over a longer period of time, with classes occurring only twice a week, 4 hours each day.

Bootcamp Syllabus

PREWORK

- Preparatory work learners must complete prior to the start of the Bootcamp (~20 hrs)
- Basics of Computer and Device Hardware, Software, Operating Systems and Processes in Windows and Linux
- Networking Basics and the OSI Model

I. BOOTCAMP INTRODUCTION

- Introduction to the Bootcamp and Cybersecurity Landscape
- Cybersecurity Career Paths
- Prework Content Review

II. NETWORK ADMINISTRATION

- Network Configuration – LAN, WAN
- Segmentations, VLANs and Subnetting
- Network Mapping Tools
- Troubleshooting and Monitoring Networks
- Network Devices – Switches, Routers
- Telecommunication
- System Administration

III. INTRODUCTION TO CYBERSECURITY

- NIST Framework and the Cybersecurity Workforce
- Malware Types
- Social Engineering
- Vulnerabilities, Risks, and Exploits
- History of Cybersecurity and Famous Cyber-Attacks

IV. NETWORK APPLICATION SECURITY

- 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
- Honeypots and Cyber Traps

V. INCIDENT HANDLING

- 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

VI. FORENSICS

- 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

VII. MALWARE ANALYSIS

- Dynamic Malware Analysis, Reverse Engineering and Malware Obfuscation
- Fileless Malware Analysis
- Containment, Eradication and Recovery Malware Stages
- Android APK Analysis

VIII. ETHICAL HACKING AND INCIDENT RESPONSE

- 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

IX. SECURE DESIGN PRINCIPLES

- Trend Analysis
- Artificial Intelligence in Cybersecurity
- Zero-Trust Policy
- Best Detection Methodologies
- Incident Impact Mitigation

X. RISK MANAGEMENT

- 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

- 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

XII. FINAL SCENARIOS AND INTERVIEW PREP

- Final Hands-on Scenarios and Final Exam
- Course Summary and Bootcamper Presentations
- Technical and Soft-Skill Preparation for Job Interviews

Cybint is a global cyber education company with a commitment to reskilling and upskilling in cybersecurity. We tackle the industry's two greatest threats: the workforce shortage and the skills gap. Our solutions were developed by a team of military cyber experts, industry professionals, and educators under the vision of creating a safer digital world through education, training, and collaboration.

www.grandview.edu/cybersecurity

GRAND VIEW UNIVERSITY

Cybint