



# Part-Time Online Cybersecurity Bootcamp

24 Weeks to a Cyber Career

**Part-Time**

class commitment

**Career Services**

Included

**Learn by Doing**

50-75% Lab Work

Over 6,000 alumni, hired by tech companies worldwide

Google

amazon



cisco



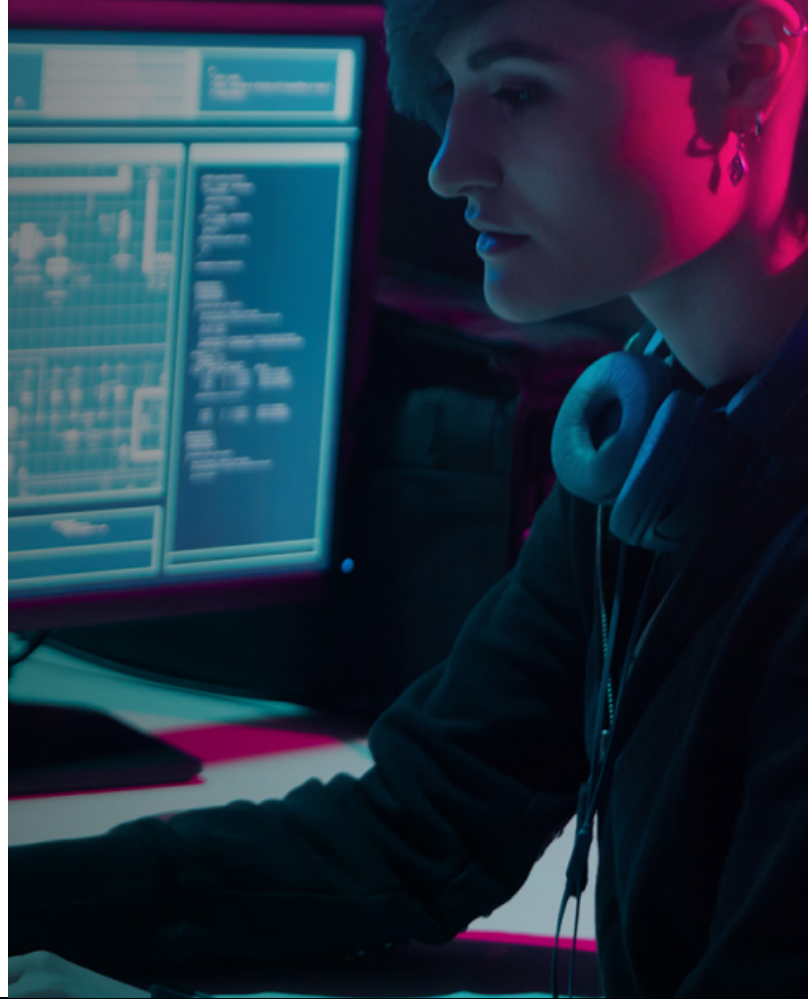
UBER

LinkedIn

\*As of 2020 alumni data

# Overview

The importance of cybersecurity today cannot be overstated. As our reliance on technology grows, there's a corresponding need to secure and defend networks and data against leaks, theft, and attacks. That's good news for cybersecurity specialists - the U.S. Bureau of Labor Statistics projects cybersecurity jobs will grow 31% through 2029. In short, there's job security in cybersecurity.



## What You'll Get



### Top Industry Certifications

Learn skills applicable to certifications such as the Network+, Linux+, Server+, Cloud+, and certified Ethical Hacker (CEH), and receive vouchers for CompTIA Security+ and CySA+.



### Cyber-Specific Career Services

Receive personalized career support from a dedicated cybersecurity career services manager, and keep your career service access for life.



### Learn By Doing

Gain hands-on experience with a host of popular tools such as Wireshark, Kali Linux, Metasploit, and more within a sandbox environment.



### End-to-End, Extensive Curriculum

Cover the latest real-world deployment of cybersecurity management practices, including defensive and offensive tactics, NIST Cybersecurity Framework, and event & incident management

# A Professional-Grade Curriculum

From CompTIA Security+ to CySA+ certifications and beyond, our Cybersecurity program teaches students critical skills to assist in the identification, assessment, reporting, and mitigation of technology and information security risks.

This professional-grade program provides information, strategies, and tactics to identify and manage information system vulnerabilities, create effective defenses and preventative measures, and deploy countermeasures against attackers.

After completing Coding Dojo's Cybersecurity program, students are mission-ready to identify, assess, report, and mitigate technology and information security risks.

Vouchers Included!



## Your Progression Plan



# Week-By-Week Curriculum

Curriculum is subject to change

## WEEK 1

### Fundamentals of Hardware

Learn about hardware and operating system fundamentals to build your baseline.

#### Labs:

- Exploring the Lab Environment
- Scanning and Identifying Network Nodes
- Intercepting and Interpreting Network Traffic with Packet Sniffing
- Analyzing the Results of a Credentialed Vulnerability Scan

## WEEK 2

### Kali Linux Introduction

Build out your Kali Linux machine while also learning about networking and data security.

#### Labs:

- Managing the Life Cycle of a Certificate
- Managing Certificates with OpenSSL
- Auditing Passwords with a Password Cracking Utility
- Managing Centralized Authentication

## WEEK 3

### Networking & Security

Learn about network configurations and data security.

#### Labs:

- Installing, Using, and Blocking a Malware-based Backdoor
- Performing Network Reconnaissance and Vulnerability Scanning

## WEEK 4

### Cybersecurity Concepts

Enter into the cybersecurity realm by thinking about vulnerabilities and risks.

#### Labs:

- Managing Access Controls in Windows Server
- Configuring a System for Auditing Policies
- Managing Access Controls in Linux

## WEEK 5

### Virtual Machines

Get into more Windows administration tools.

#### Labs:

- Configuring Identity and Access Management Controls
- Implementing a Secure Network Design
- Configuring a Firewall

## WEEK 6

### Exploitation

Use Metasploit to run exploit code.

#### Labs:

- Configuring an Intrusion Detection System
- Implementing Secure Network Addressing Services
- Implementing a Virtual Private Network
- Implementing a Secure SSH Server

## WEEK 7

### Building a Defensible Network

Learn the basics of different network architecture and design principles.

#### Labs:

- Implementing Endpoint Protection
- Securing the Network Infrastructure
- Identifying Application Attack Indicators

## WEEK 8

### Identifying Risks to your Network

Take the necessary steps to identify the risks to your network.

#### Labs:

- Identifying a Browser Attack
- Implementing PowerShell Security
- Identifying Malicious Code

# Week-By-Week Curriculum

Curriculum is subject to change

WEEK 9

## Scanning the Network

Begin scanning a network periphery to find vulnerabilities.

### Labs:

- Identifying Application Attacks
- Managing Data Sources for Incident Response
- Configuring Mitigation Controls

WEEK 10

## Cloud Computing

Learn about the Cloud and its implications for risks and vulnerabilities, install Kali Linux with Cloud Computing.

### Labs:

- Acquiring Digital Forensics Evidence
- Backing Up and Restoring Data in Windows and Linux
- Managing Incident Response, Mitigation and Recovery

WEEK 11

## Certification Review

Tie off remaining concepts as you prepare for the CompTIA Security+ exam. Take the belt exam as your practice exam.

WEEK 12

## CompTIA Security+ Certification

A crucial point in your learning timeline: schedule, review, and complete your Security+ exam.



WEEK 13

## Threat Intelligence

Utilize threat intelligence and classification to support organizational security.

### Labs:

- Investigating Threat Data and Intelligence Sources
- Developing a Network Threat Model
- Analyzing Output from Network Security Monitoring Tools
- Discovering the Lab Environment

WEEK 14

## Intelligence & Indicator Management

Implement controls to mitigate attacks and software vulnerabilities.

### Labs:

- Analyzing Output from Security Appliance Logs
- Analyzing Output from Endpoint Security Monitoring Tools

WEEK 15

## Security Best Practices

Learn best practices of software, hardware, and infrastructure assurance.

### Labs:

- Analyzing Email Headers
- Configuring SIEM Agents and Collectors
- Analyzing, Filtering, and Searching Event Log and syslog Output

WEEK 16

## Cloud Access & Techniques

Revisit cloud technologies and how to protect your cloud-based solutions.

### Labs:

- Collecting and Validating Digital Evidence
- Analyzing Network-related IoCs

# Week-By-Week Curriculum

Curriculum is subject to change

WEEK 17

## Attacking & Protecting

Learn about DoS attacks and mitigation as well as deploying honeypot solutions to intercept hackers.

### Labs:

- Analyzing Host and Application IoCs
- Following an Incident Response Process

WEEK 18

## Impact Analysis & SIEM

Implement configuration changes to existing controls to improve security based on data analysis you make part of everyday security monitoring activities.

### Labs:

- Following an Incident Response Process
- Observing IoCs during a Security Incident

WEEK 19

## Proactive Threat Hunting

Become proactive in your approach to cybersecurity by seeking threats.

### Labs:

- Reviewing Risk Management Processes
- Analyzing Output from Topology and Host Enumeration Tools
- Testing Credential Security
- Configuring Vulnerability Scanning and Analyzing Outputs

WEEK 20

## Security Monitoring

Deploy Security Content Automation Protocol (SCAP)

### Labs:

- Assessing Vulnerability Scan Outputs
- Assessing the Impact of Regulation on Vulnerability Management
- Performing Account and Permissions Audits
- Configuring Network Segmentation and Security

WEEK 21

## Incident Response

Apply incident response procedures

### Labs:

- Configuring and Analyzing Share Permissions
- Assessing the Impact of Web Application Vulnerabilities
- Analyzing Output from Web Application Assessment Tools

WEEK 22

## Digital Forensics

Collect and analyze indicators of compromise.

### Labs:

- Analyzing Output from Cloud Infrastructure Assessment Tools
- Assessing the Impact of Threats to Cloud Infrastructure

WEEK 23

## Certification Review

Tie off remaining concepts as you prepare for the CompTIA CySA+ exam. Take your second belt exam as prep.

WEEK 24

## CompTIA CySA+ Certification

The final step in your bootcamp journey - your CySA+ certification!



# Career Services Overview

## OBJECTIVE 1

### Professional Profile & Portfolio

- ✓ LinkedIn Profile Creation
- ✓ HackerRank and Hack.Me Intro
- ✓ Resume Development & Curation

## OBJECTIVE 2

### Job Prospecting & Application Guidance

- ✓ Real Job Search
- ✓ Sample Applications
- ✓ Hiring Manager Communication
- ✓ Job Title Refinement

## OBJECTIVE 3

### Interview Prep & Salary Negotiation

- ✓ Mock Interviews
- ✓ Technical Skills Test Prep
- ✓ Target Compensation Guidance
- ✓ Contract Negotiation

Our Outcomes are third-party verified by the independent firm, Delivery Associates, for accuracy and transparency.

# 89.1%

within 6 months of graduating

# 95.3%

within one year of graduating

Student Employment Status	# of Students	% of Students
Student employed in a relevant position within six months of graduation	229	89.1%
Student was not employed until more than six months after graduation, but was then employed in a relevant position	16	6.2%
Student employed within six months of graduation, but not in a relevant position	11	4.3%
Student was not employed until more than six months after graduation, and was not then employed in a relevant position	1	0.4%
<b>Totals</b>	<b>257</b>	<b>100%</b>

[View Our Outcomes](#)

# How to Enroll

1

## Explore (optional)

Schedule a Q&A call with Admissions to get quick answers about the bootcamp or join the next Open House.

2

## Apply

Ready to join? Submit your application and pick your start date to join.

3

## Take the Exam

The entrance exam is a timed exam consisting of 32 logic problems. You have one opportunity to take the exam per class start date.

4

## Deposit to Enroll

If accepted, submit your deposit to officially save your seat and gain access to bootcamp-prep materials for your start date.

Apply Now

## Financing Options

Not sure what is right for you? Visit our [Financing 101](#) page or schedule a call with an Admissions Advisor.

TALK TO US



### Standard

2 Payments  
50% of tuition due week 1  
50% of tuition due midway



### Monthly Plan

As low as \$262/month  
30/60 month terms available

Financing provided by:



### Income Share Agreement

Pay when you're hired!  
Max 60 payments  
Income: 9.80%