



Over 35 years in Technology Education

Cybersecurity Bootcamp



CURRICULUM GUIDE

Why Study Cybersecurity?

With employer demand for cybersecurity professionals at an all-time high, there's never been a better time to enter or advance your career within a lucrative field. Prepare for a dynamic career with an accelerated and immersive cybersecurity bootcamp from QuickStart.

Our 100% online Cybersecurity Bootcamp offers experienced and aspiring IT professionals hands-on technical training to advance in the field. Through interactive class sessions, projects, and mentoring sessions, you'll gain industry-aligned skills to earn valuable certifications.

Over the course of 24 weeks, you will dedicate an average of 15-25 hours per week to master new cybersecurity skills. You'll have access to career services from the start of the program to help you land your next role.

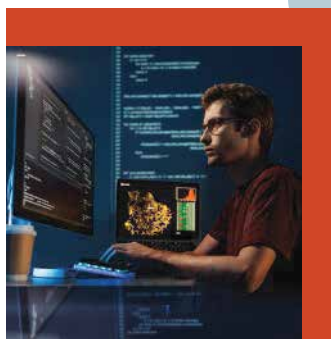
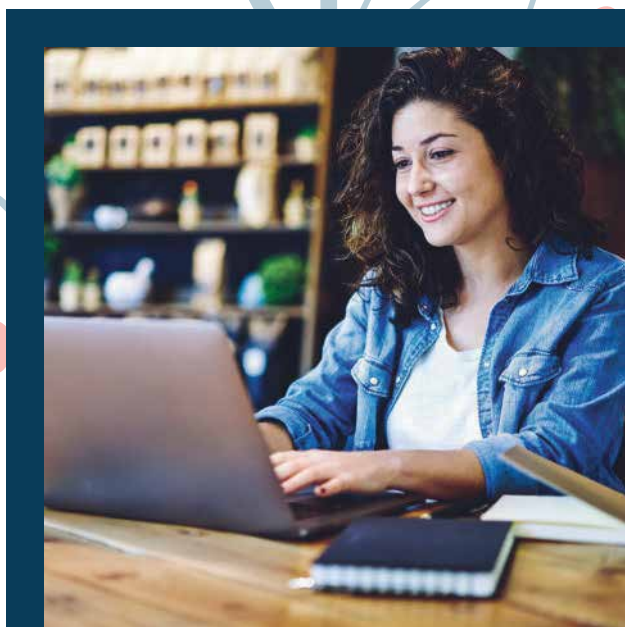
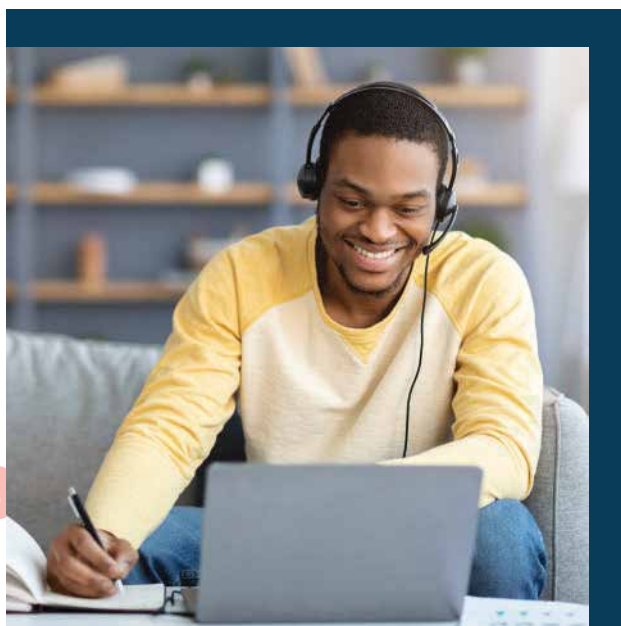


Who Is This Bootcamp For?

Designed for entry-level and experienced IT professionals alike, the Cybersecurity Bootcamp offers hands-on training in the latest technical skills.

Entry and junior-level IT professionals will benefit from coursework focused on foundational cybersecurity skills and concepts, including CompTIA Security+ and Network+ certification preparation.

Advanced cybersecurity professionals who aim to reach the next level of career success will benefit from training in emerging and industry-aligned skills, including Certified Ethical hacker (CEH) coursework.





Course Structure

By combining the best of online learning with collaborative modules, our program offers the flexibility and rigor you need to accelerate your cybersecurity career. Throughout the program, you will attend live online lectures and apply class concepts through virtual hands-on labs and project assignments. With the support of instructors, you will develop the framework to solve problems cybersecurity professionals face daily.



Virtual Office Hours

While most of your bootcamp can be completed on demand and at your own pace, your instructors will reinforce asynchronous lessons with virtual office hours. These live, instructor-led sessions offer you the opportunity to ask questions, receive immediate support, and advance your understanding of the course concepts.



Course Learning Tracks

As an online bootcamp student, you will have the option to choose between three modes of virtual instruction:

- Immersive: This learning format features two, 2-hour live mentoring (virtual office hour) sessions per week.
- Flex: Students attend one, 2-hour live mentoring (virtual office hour) session per week.
- On-demand: Students complete five, 30-minute mentoring (virtual office hour) sessions on their own schedule.

Regardless of the mode of instruction you choose, you will have access to a dedicated bootcamp discussion forum to collaborate and seek help from industry experts and other students.

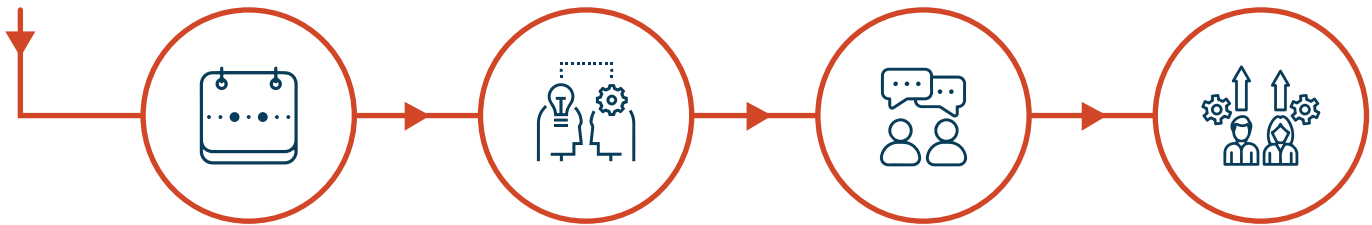


Virtual Hands-On Labs

When it comes to mastering new technical skills, the best way to learn is by doing. Your cybersecurity courses will feature several lab assignments that allow you to apply concepts in a virtual environment.

Your portfolio signals to employers that you possess the technical skills to hit the ground running in a new role. Throughout your bootcamp, you will build a substantial portfolio of projects that demonstrate your proficiency in the leading cybersecurity programs and tools.

As a bootcamp student, you will work independently on a series of applied capstone projects. Students are encouraged to pursue capstone project topics that interest them, and work alongside a mentor to complete the portfolio-ready assignment.



Career Services

You will have access to a suite of resources, including a career services platform featuring job opportunities and a talent portal where hiring organizations can contact you, resume review and feedback, assistance updating your LinkedIn profile, mock interviews, and guidance on how to market your new cybersecurity skills. Our team will also help you develop a portfolio for prospective employers and identify job opportunities. You will also have the opportunity to schedule individual sessions with a career coach, when needed.



Week 1-2 IT Fundamentals

Designed for beginners and students without any IT experience, the IT Fundamentals course covers the essentials for a career in information technology. This course is ideal for non-technical professionals and empowers students to use features and functions of common operating systems, establish network connectivity, identify common software applications, and more.

Week 3-4 Networking Fundamentals

Designed to prepare students for the CompTIA Network+ certification exam (N10-008), this course will focus on the security skills necessary for an entry-level role in cybersecurity.

Week 5-7 Security Fundamentals

This course will teach students how to identify security fundamentals and threats; analyze risk; conduct security assessments; implement network, operational, host, and software security; manage identity and access; implement cryptography; address security threats; and ensure business continuity. After completing this course, students will be able to complete CompTIA Sec+ certification.

Week 8-9 Project A

In this project, students will develop hands-on experience installing and configuring different types of operating systems, networks, networking tools, and security baselines. They will also learn to prepare a project report.

*Depending on your personal computer hardware settings, participants may need to run scans or updates overnight.

Week 10-11 Python Programming

In this course, students will learn the fundamentals of programming in Python, and develop applications to demonstrate proficiency.

Week 12 Project B

This project is designed to test learnings from previous courses. This project will test students' hands-on skills using various tools and best practices that are necessary for an information security professional.

Week 13-16 Ethical Hacking

This course enables students to identify, counter, and defend against hackers, who can maliciously penetrate networks and gain access to vital information. This course is designed to prepare students for the Certified Ethical Hacker certification exam.

Week 17-19 Project C

This project is designed to test learnings from previous courses. This project will test students' hands-on skills using various tools and best practices that are necessary for an information security professional.

Week 20-22 Cybersecurity Analyst

The course prepares students to proactively capture, monitor, and respond to network traffic findings. This course also emphasizes software and application security, automation, threat hunting, and IT regulatory compliance.

Capstone Project

Your coursework will culminate in two capstone projects, the first of which will challenge you to upgrade a CentOS Linux Firewall with a PFSense Firewall. This simulation will test your comprehension of opensource firewall tools, and the skills required of a cyber security analyst.

Week 23-24 CompTIA Pentest+

In this course, students will learn the art of implementing high-level penetration testing practices. This intermediate-level course presents a great learning opportunity for professionals who want to understand the art of scoping and planning a security assessment. This course is meant to follow the CompTIA Security+ Course and emphasizes mainly the niche of penetration testing.

Capstone Project

The second and final capstone project for this course will feature a simulation designed to test your awareness and response to cyber threats. As part of this project, you will demonstrate how to identify network vulnerabilities, and how a vulnerability could be exploited and used against an organization. This project will build on the first capstone assignment and will feature the same network.

