QUICKSTART

Over 35 years in Technology Education

Cybersecurity
Bootcamp

CURRICULUM GUIDE - 2025

Why Study Cybersecurity?

Embark on a rewarding journey into the thriving field of cybersecurity, where the demand for skilled professionals continues to grow. Elevate your career through our accelerated and immersive Cybersecurity Bootcamp, built by subject matter experts for both seasoned IT professionals and those interested in pivoting into the field.
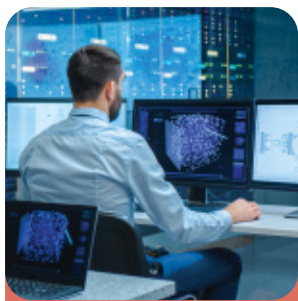

Who Is This Bootcamp For?

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

Our training prepares you for IT roles such as **Cybersecurity Analyst** and **Security Operations Center Analyst (SOC).**

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

Course Structure

Designed to empower working professionals with the skills to thrive in the dynamic cybersecurity field, our program offers the flexibility and interactive instruction online learners need. Our hybrid learning model combines independent learning modules and live, instructor-led class time.

The **part-time** option, spanning 18 weeks, offers a balanced approach to virtual learning. Part-time students learn through predominantly asynchronous course content, complemented by live class sessions.

The **full-time** option condenses the program into an intensive 10-week period and features more synchronous class sessions to enhance real-time interaction and engagement.
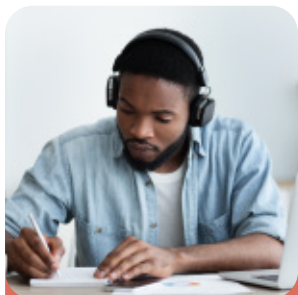
The cybersecurity bootcamp requires an average commitment of 20-25 hours per week for the **part-time** program option. Students enrolled in the full-time program can expect to spend at least 35-40 hours per week in class and 8-10 hours per week on assignments and independent study.
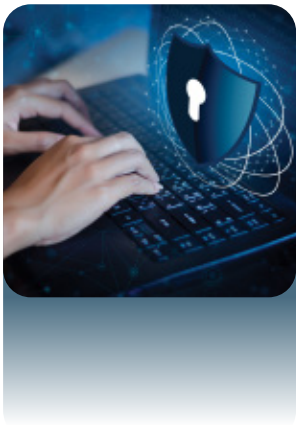
Projects and Assignments

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.
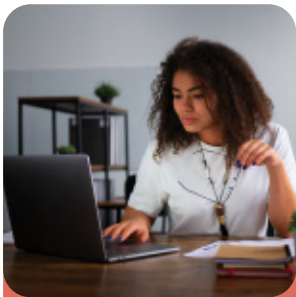
Capstone Project

As a bootcamp student, you will be paired with another student to encourage peer-to-peer collaboration. This capstone project will challenge students to collaborate, encouraging technical skill development and communication and teamwork skills. Students will also complete two career simulators, scenario-based projects that model on-the-job situations, at the conclusion of the program.

Virtual Hands-On Lab Experiences

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 hands-on "sandbox environment" that provides a controlled and secure space for students to experiment without the risk of causing damage or compromising actual systems. Sandbox assignments allow you to build confidence and proficiency in real-world scenarios.
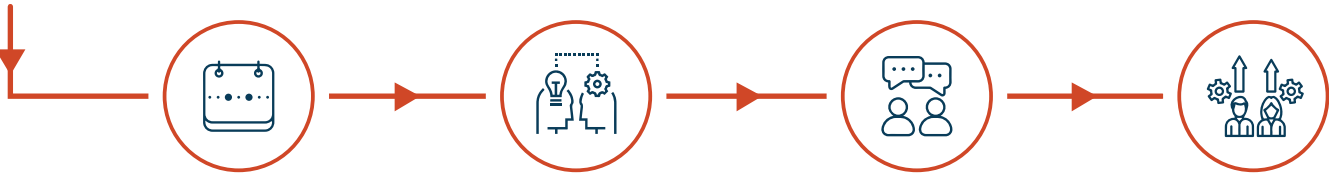
Dedicated Certificate Preparation

Our bootcamp includes dedicated certification preparation during the final weeks of the program, designed to help students review and solidify cybersecurity skills prior to taking the industry-aligned CompTIA Sec+ certification exam. This intensive phase includes mock exams and targeted review sessions, ensuring students are well-equipped and confident to pursue relevant certifications in cybersecurity upon completion of the bootcamp.

CompTIA Sec+ certification is compliant with ISO 17024 standards and approved by the United States Department of Defense (DoD). This accredited certification opens the door to professionals in both the government and private sectors. In 2023 alone, over 81,000 job openings requiring CompTIA Security+ certifications existed. By pursuing the QuickStart Cybersecurity Bootcamp, students not only prepare to ace the CompTIA Security+ certification exam but do so at an incredible value.
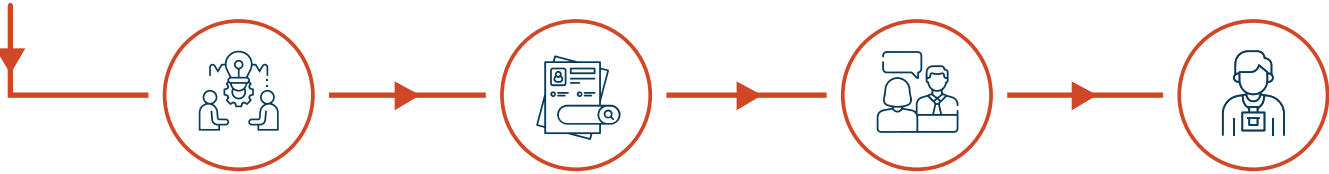
Certification	Preparation Provided	Course Cost Included	Exam Cost Included	Study Guide Value
CompTIA Security+	Exam preparation, targeted review sessions, mock exams	$2,300	$400	$170

Student Support Services

Our bootcamp offers comprehensive student support services to enhance the learning experience. Students benefit from weekly live sessions, serving as virtual office hours or dedicated class time, facilitating real-time interaction with instructors. Additionally, the program offers personalized 1:1 coaching sessions, allowing students to seek guidance and clarification up to 10 times throughout the program. To ensure continuous support, a 24/7 AI tutor is available, offering around-the-clock assistance through an AI bot. These robust support mechanisms aim to foster a supportive learning environment and help students succeed in mastering cybersecurity skills.

Career Services

You will have access 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 mentoring sessions when needed.

Career Outcomes

Completing an industry-aligned bootcamp and earning in-demand certifications opens the door to your IT career in cybersecurity, a field projected to grow 32% by 2032 (U.S. Bureau of Labor Statistics, 2023). Explore the top IT roles our program can help you prepare for in 10-18 weeks.

Role	Experience	Average Salary
Cybersecurity Analyst	Entry-level role	$88,779
Security Operations Center (SOC) Analyst	Entry-level role	$69,396

QuickStart Bootcamp students who have completed the program are employed by notable organizations across the country, including:
Source: Talent.com, 2023

American Airlines	Apple	AT&T	Berkshire Hathaway
Capgemini	Charles Schwab	Cognizant	Cisco
Fidelity	Fiserv	General Electric	General Motors
Home Depot	Meta	Norton Lifelock	Oracle
Revature	Shake Shack	Skillstorm	Tesla

Curriculum Overview

Course	Week		Learning Outcomes
	Full-Time option	Part-Time option	
Cybersecurity Essentials	1	1	This course introduces essential computing concepts, emphasizing troubleshooting skills and covering applications software, operating systems, and peripheral device setup. Students will also explore basic wireless networking, cybersecurity principles, and foundational knowledge in databases, coding, and emerging technologies.
System and Network Security	2	2-4	This course delves into the mechanics of data transmission among network- connected devices, teaching participants to monitor and optimize networks for seamless business continuity. It covers routing technologies, networking devices, and explores security concepts, enabling learners to comprehend and defend against network attacks to enhance network resilience.
Linux Essential	3	5-6	Explore the essential tools and techniques employed by Linux system administrators in this course. Delve into the intricacies of major Linux distributions, mastering system configurations, navigating graphical interfaces, and honing skills in bash scripting. Additionally, participants will learn robust user security controls to ensure a comprehensive understanding of Linux system administration.

Course	Week		Learning Outcomes
	Full-Time option	Part-Time option	
Career Simulation 1	4 - 5	7-8	Learners will immerse themselves in a career simulation where they assume the role of an IT subject matter expert hired by a company for a comprehensive IT system upgrade. Participants will take on tasks such as installing a virtual machine, configuring a firewall, setting up a PC for the CEO, deploying an internal web server, establishing an internal DNS server, and managing Linux machines for monitoring and cybersecurity-related activities. This simulation offers hands-on experience in a practical environment mirroring real-world IT challenges and responsibilities.
Security Operations and Architecture	6	9-12	This course prepares learners with a solid foundation in cybersecurity by introducing key terminology and concepts, laying the groundwork for understanding security controls. Participants will explore the security implications associated with diverse architecture models, grasp the principles of securing enterprise infrastructure, and develop skills in responding to common threats, cyberattacks, vulnerabilities, and security incidents.
Career Simulation 2	7	13	Embark on a dynamic career simulation where you take on the role of a cybersecurity professional tasked with assessing vulnerabilities in a new production server and the network's webserver. Through hands-on experience, participants will install and configure the production server, implement IDS/IPS on pfSense, an open-source firewall, and actively engage in simulated attacks to identify and address vulnerabilities. This immersive simulation provides a comprehensive learning experience in securing networks and responding proactively to potential cyber threats.

Course	Week		Learning Outcomes
	Full-Time option	Part-Time option	
Cyber Security Analyst Essentials	8	14-15	In this course, participants will learn to gather cybersecurity intelligence from diverse sources, developing the skills to analyze data extracted from security and event logs to identify potential threats. The focus extends to responding to and investigating cybersecurity incidents, allowing participants to address security issues within the organization's technology architecture effectively. Students will gain practical insights into threat detection, analysis, and incident response to bolster organizational cybersecurity resilience.
Final Career Simulation	9	16	Embark on an engaging career simulation centered around the Capture the Flag (CTF) activity, a widely embraced and dynamic approach in the cybersecurity realm. As participants navigate challenges and capture flags, they acquire valuable skills and real-world experience, equipping them for success in the dynamic and evolving field of cybersecurity.
Exam Preparation for CompTIA Sec+	10	17-18	In this final exam preparation course for the CompTIA Security+ exam, participants will go through practice exams and receive study tips to attain the Security+ credential. Under an instructor's guidance, they will have the opportunity to review and refresh their knowledge on exam topics, with access to multiple mock exams for repeated practice. Successful completion of the certificate not only validates their expertise but also enhances job prospects, providing a solid foundation for securing a position in the field.