tripleten

Visit our website

Cyber Security

Syllabus

7 Months

Contents

About the program

The Cyber Security Program is designed to prepare individuals to become a security specialist by providing hands-on training on the latest security technologies and methodologies.

What you'll learn

Our program provides hands-on training on the latest security technologies and methodologies. You will learn such hard skills as malware and virus threats, network security controls, cryptography, and vulnerability testing methodologies. You will also learn how to manage risk, develop security procedures, and plan for disaster recovery. Overall, the program prepares you to become a cyber security specialist, equipped to protect organizations from cyber threats.

Soft skills are a must-have

You will develop both technical and soft skills during the program, including risk management and critical thinking. Your ability to assess threats and prioritize tasks will help you focus your energy where it is needed the most. Communication is also important in cyber security, as you may need to explain technical concepts to non-technical individuals, such as executives or legal teams.

Career-focused lessons

Our ultimate goal is to help you become a successful Cyber Security. That's why this program also features externships for students to gain hands-on experience in various roles. The bootcamp also includes a Career Prep Course to help students prepare for life after graduation, including creating a resume, LinkedIn profile, and GitHub account, improving networking and interview skills, and providing career coaching to help find a job.

Course structure

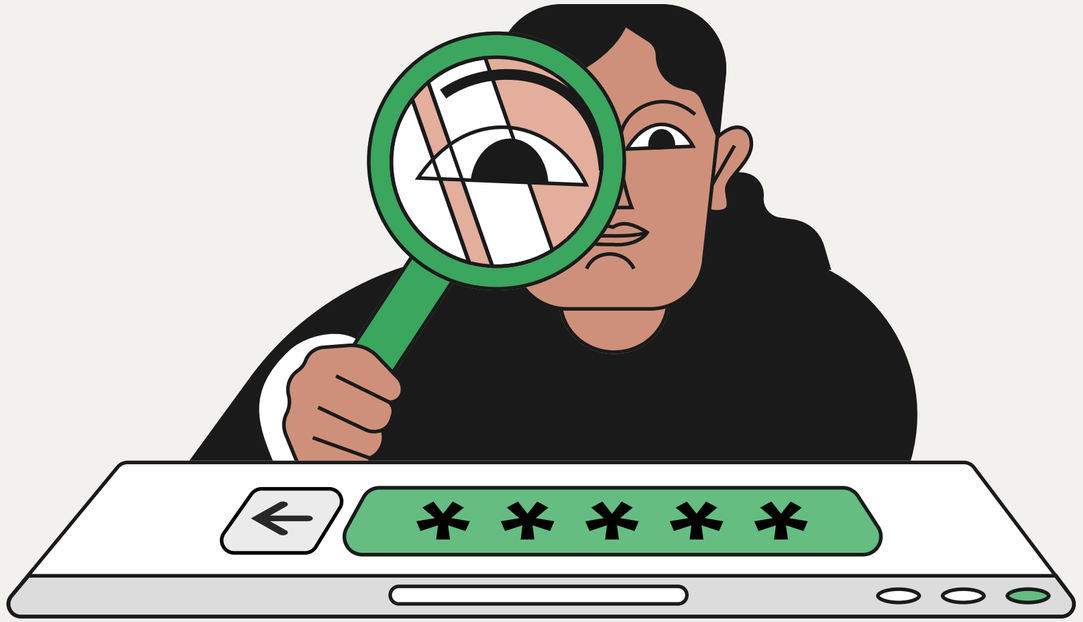
Your journey will be structured as a series of sprints, grouped into thematic modules. Each sprint will have a particular set of learning outcomes, reinforced through quizzes and tasks.

We provide rough time estimates but recommend spending around 25 hours per week studying. Everyone learns at different paces, so feel free to go at your own speed. Suggested breaks are scheduled in between modules.

After completing the program and obtaining the CompTIA Security+ certification, you'll spend 10-15 hours in Career Services and join Career Acceleration Program preparing you for a job search as a certified cyber security professional.

Module 1. Fundamentals

6 weeks



Sprint 1. Network Configuration

Recognize critical networking components. Evaluate network topologies. Read IP addresses. Identify protocols responsible for moving data. Analyze traffic using network monitoring tools. Distinguish between anomalies caused by misconfigurations or malicious attackers. Evaluate network design choices. Match problematic network design choices with the appropriate security-sensitive alternate implementation.

Project description

Analyze a network for security flaws. Generate a plan to update it according to best security practices.

2 weeks

Sprint 2. Scanning and Enumeration

Conduct scans to enumerate clusters of devices belonging to a company. Interpret clues about what is contained on those devices—and use that information to assemble a list of the company's assets. Implement defense measures to mask devices' true identities from attackers.

Project description
Interpret results from standard scanning and enumeration tools to create an accurate CMDB listing the company's assets.

2 weeks

Sprint 3. Cyber Security Frameworks

Identify a company's cybersecurity risk profile. Protect business continuity by limiting the impact of cybersecurity events. Implement systems to continuously monitor assets and detect security incidents as they occur. Craft effective responses to cybersecurity incidents to contain impact. Recover from incidents efficiently—and ensure that lessons learned drive improvements to prevent future incidents.

Project description
Assess the cybersecurity posture of a medium-sized business. Develop an effective mitigation plan with improved security policies and procedures, using the NIST CSF to guide your risk assessment.

2 weeks

Module 2. Networks

4 weeks

Sprint 4. Network Hardening and Virtualization

Harden a network. Establish a SNOC. Automate repetitive tasks. Compare and test network architecture choices. Evaluate network changes without disrupting production services. Strengthen authentication practices. Identify defensive gaps according to threat model.

Project description
A neglected, outdated company network needs to be modernized...securely. The existing network architecture adheres to a conventional on-premises model reliant on physical hardware. Identify strategies to stabilize current technologies by implementing virtualization, providing the company with the time needed to develop a comprehensive action plan for broader cloud adoption. Finally, create a presentation outlining your proposal to the company's executives—and get the green light.

2 weeks

Sprint 5. Managing Networks Securely

Secure physical, virtual, and cloud networks. Safely extend a corporate network. Align network security with compliance goals. Validate, aggregate, and maintain valuable sources of data for continuous monitoring.

Project description
You got the green light! But until the infrastructure is fully modernized (and leadership has designated which systems will be rehosted, re-platformed, refactored, or retired), you must accommodate daily operations alongside activities supporting the transition—without incurring a loss or inducing an incident. You must successfully upgrade the network's legacy systems according to your previously-proposed plan.

2 weeks

Module 3. Risks

6 weeks

Sprint 6. Identifying Common Threats and Attack Vectors

Detect phishing, malware, DDoS, insider threat, and APT attacks. Leverage patch management, user awareness training, improved authentication, backups, audits, and other techniques to prevent these attacks from succeeding.

Project description

Simulate a phish, investigate the incident, and document your findings along with an appropriate response strategy.

2 weeks

Sprint 7. Alerts and Anomalies

Investigate anomalous file changes. Analyze unusual network traffic. Dig into suspicious login activity. Zero in on suspicious traffic leaving the network.

Project description
A company's cybersecurity monitoring system generated alerts indicating several possible malicious incidents. In the process of investigating these alerts, you must identify which are real (and which are false positives)—then develop appropriate response plans for the true security incidents.

2 weeks

Sprint 8. Incident Response

Develop playbooks for standard incident response scenarios: phishing, malware, data breach, and DDoS.

Project description
One of our client companies was just devastated by a ransomware incident. It's up to you to review their current, poorly-implemented incident response plan and revise it to satisfy industry-honed standards set forth by NIST—protecting them from repeating past mistakes.

2 weeks

Module 4. Vulnerability management

6 weeks

Sprint 9. Vulnerability assessment

Inventory the assets. Conduct scans—and interpret their results. Assess the severity of detected vulnerabilities. Remediate highest risk vulnerabilities.

Project description

A new client company has just been added to the MSSP's SOC...and they need you to conduct a vulnerability assessment, ASAP. Assess their assets and prepare a formal report of your findings.

2 weeks

Sprint 10. Vulnerability Exploitation

Perform penetration tests focusing on exploiting vulnerabilities on servers, verifying your initial findings.

Project description
The company is alarmed by your findings. They've authorized you to perform a penetration test confirming critical vulnerabilities discovered during your assessment—and determining the true severity of your findings. Are things really as bad as they look?

2 weeks

Sprint 11. Vulnerability Remediation

Present your findings using industry-standard report formats.
Plan remediations. Execute the fixes.

Project description
Vulnerabilities confirmed, it's time to choose then implement appropriate remediation strategies.

2 weeks

Module 5. Investigating Incidents

4 weeks

Sprint 12. Detecting Complex Attacks

Detect common attacks using standard sources of evidence available to security analysts. Craft the perfect search queries to cut through the data and zero in on evidence of attacks. Distinguish between normal and malicious activity.

Project description
Investigate a major security incident using a SIEM, leveraging the MITRE ATT&CK matrix to map the attacker's TTPs.

2 weeks

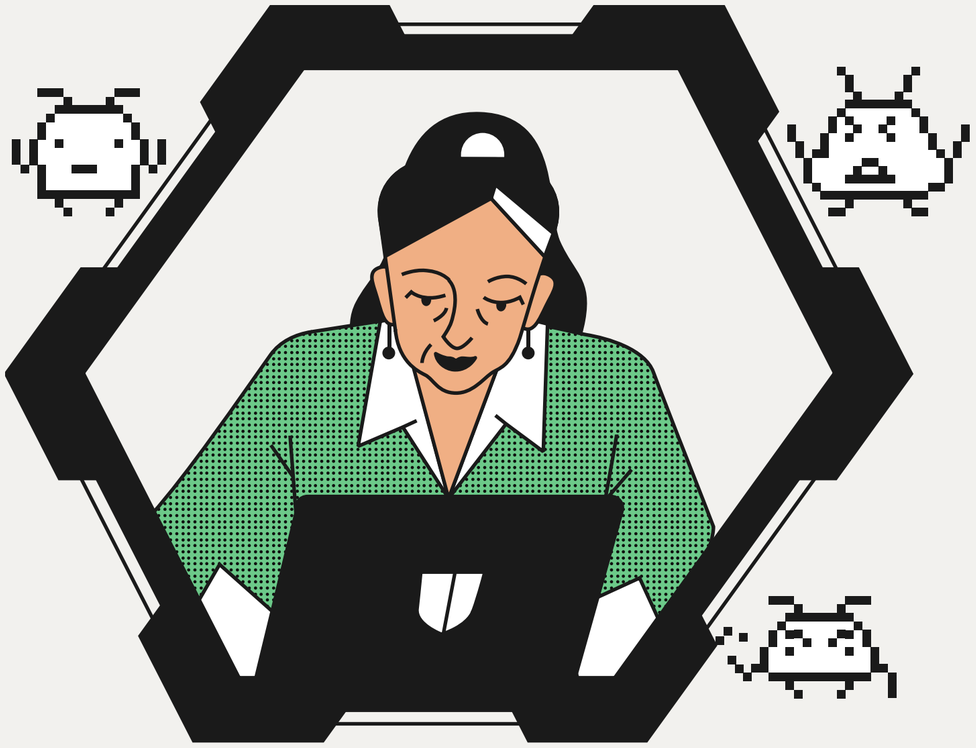
Sprint 13. Investigating Incidents

Practice the art of asking the right questions—and pivoting between evidence sources to answer those questions. Tailor mitigation and remediation recommendations to reduce attack vectors revealed by the incident.

Project description
Author a formal report effectively communicating your investigation's findings and recommended incident response actions to both technical and layperson audiences.

2 weeks

Module 6. CompTIA Security+



Sprint 14. CompTIA Security+ Exam Preparation

Undertake an intensive review covering all the domains of the CompTIA Security+ certification exam. Through practice questions, labs, and mock exams, you will reinforce the concepts learned throughout the program while preparing to take the Security+ certification exam.

Project description
Obtain the CompTIA Security+ certification.

2 weeks

Employment Preparation

At TripleTen, we know that learning the technical skills you need for a job is only one piece of the employment puzzle. That's why we offer a range of courses to help you land your dream job. These are included as part of the course, but you are free to opt out of Career Acceleration and the Externships if you don't need them (note: the Career Prep Course and Career Acceleration are necessary if you want to take advantage of the money-back guarantee).

Career Prep

10-15 hours in total

If you want some guidance on landing your dream job, Career Prep has all the information you need. First, you'll cover some of the necessary groundwork before you can start applying for jobs. This includes creating a portfolio, building an online presence via LinkedIn, working on your job search strategy, and growing your professional network. Once that's done, you'll focus on the different stages of the job application process, perfecting your resume and cover letters, acing interviews, and masterfully negotiating offers.

Career Acceleration* After graduation

Typically 3-6 months

Prepare for real-world interviews and gain experience through authentic practice. This program is designed to help you find a job and also provides extra work with technical skills. It can last anywhere from 3-6 months after graduation. You will attend mock interviews, get your career documents reviewed, and receive 1:1 career coaching that will take your job search to the next level.

*Only available to students eligible to work in the US.

Externships

4 to 5 weeks, 30+ hours

Boost your portfolio and gain confidence in solving work tasks by completing a project for a real company. Learn to communicate with clients, meet their expectations, exchange peer reviews with colleagues, and present results to a company. Externships become available for participants towards the end of the bootcamp.

tripleten

Visit our website

Learn  the job.

✨ Get the job. ✨