tripleten

Visit our website

Cyber Security

Program

3 Months

full time

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 specialist.

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 and LinkedIn profile, 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. At the end of the sprint, you will take the skills you've learned and combine them with your existing skills to work on a project that will be assessed by industry experts.

We provide rough time estimates but recommend spending around 40 hours per week studying.

After completing the program and obtaining the CompTIA Security+ certification, you will be ready to begin the job search as a certified cyber security professional.

Module 1. Fundamentals

3 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.

1 week

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.

1 week

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.

1 week

Module 2. Incident Response

2 weeks

Sprint 4. Identifying Common Threats and Attack Vectors

Threat model an organization. Identify and prioritize mitigations to reduce attack surface.

Project description
Threat model a company based on a list of assets. Recommend an effective mitigation strategy to reduce attack surface.

1 week

Sprint 5. 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.

1 week

Begin your certification journey preparing for the CompTIA Security+ exam with flashcards to help you memorize key terms as well as access to unlimited practice exams.

Module 3. Vulnerability Management

4 weeks

Sprint 6. 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.

1 week

Sprint 7. Vulnerability Assessment

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

1 week

Sprint 8. 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?

1 week

Sprint 9. 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.

1 week

Module 4. Investigating Incidents

4 weeks

Sprint 10. Deploy a SIEM

Validate, aggregate, and maintain valuable sources of data for continuous monitoring. Test using Atomic Red Team.

Project description
Set up a continuous monitoring system for existing devices and ensure it is correctly ingesting security-critical logs from endpoints. Validate your setup using an adversary emulation platform. Document and share your process using an industry-standard blog format.

1 week

Sprint 11. Triage Alerts and Anomalies

Dive into using Splunk for detecting security incidents: 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. Triage security alerts using an industry-standard report format to document each investigation's findings.

1 week

Sprint 12. Your First Major Investigation

Investigate a major security incident 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 Splunk, leveraging the MITRE ATT&CK matrix to map the attacker's TTPs. Write a SIGMA detection. Document and share your investigation and present your findings using an industry-standard blog format.

1 week

Sprint 13. Investigate a Complex Attack

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

Project description
Investigate a more complex cloud-based security incident using Splunk, leveraging the MITRE ATT&CK matrix to map the attacker's TTPs. Write a YARA detection rule. Document your investigation and present your findings using an industry-standard blog format.

1 week

Finally, take the industry-recognized CompTIA Security+ exam and submit your certificate as the capstone achievement of your bootcamp experience.

Career Preparation

From day one

Access career-focused lessons that strengthen both:

- **Hard skills:** for job applications
- **Soft skills:** networking, communication, self-promotion and interview techniques
- Attend workshops with a career coach

Midway through

Partner with a career coach to:

- Develop a personalized job search strategy
- Perfect your resume, LinkedIn profile, and portfolio
- Practice interview & networking techniques in group and individual sessions

As you progress

- Participate in Code Jams—team competitions to apply your skills
- Complete an Externship—gain real-world business experience (you'll learn more as you advance!)

After graduation

Enter the job search phase with support from a Placement Coordinator:

- Regular check-ins to keep you on track
- Feedback to improve applications and networking
- Help connecting with recruiters and hiring managers
- AI-powered job search platform to manage applications and track progress

Learn { the job.
Get the job.