

Cybersecurity

7 months

Online

Part-time

Table of contents

What is Cybersecurity?	2
Program Structure	3
Module 1. Fundamentals	4
Module 2. Incident Response	6
Module 3. Vulnerability Management	7
Module 4. Investigating Incidents	9
Module 5. Emerging Threats	11
CompTIA Security+ exam	12
Career Preparation	13
Active Job Search	14

What is Cybersecurity?

The Cybersecurity Program is designed to prepare individuals to become security specialists by providing hands-on training on the latest security technologies and methodologies.

🔗 What you'll learn

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 cybersecurity 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 cybersecurity, as you may need to explain technical concepts to non-technical individuals, such as executives or legal teams.

Program 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 15–20 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 will be ready to begin the job search as a certified cybersecurity professional.

Module 1. Fundamentals

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

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

Sprint 3

Cybersecurity 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: 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.

Module 2. Incident Response

Sprint 4

Identifying Common Threats and Attack Vectors

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

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

Sprint 5

Scanning and Enumeration

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

Project: 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.

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

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: 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.

Sprint 7

Vulnerability Assessment

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

Project: 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.

Sprint 8

Vulnerability Exploitation

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

Project: 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?

Sprint 9

Vulnerability Remediation

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

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

Module 4. Investigating Incidents

Sprint 10

Deploy a SIEM

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

Project: 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.

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: 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.

Sprint 12

Your First Major Investigation

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

Project: Investigate a major security incident using Splunk, leveraging the MITRE ATT&CK matrix to map the attacker's TTPs. Document and share your investigation, presenting your findings using an industry-standard incident investigation report format.

Sprint 13

Investigate a Complex Attack

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

Project: Investigate a major security incident using Splunk, leveraging the MITRE ATT&CK matrix to map the attacker's TTPs. Document and share your investigation, presenting your findings using an industry-standard incident investigation report format.

Module 5. Emerging Threats

Sprint 14

AI Security

In this capstone sprint, learners bring together everything they've gained throughout the program to take on one of the most urgent challenges facing the field today: securing AI systems. We begin with an overview of the rapidly evolving AI landscape—tracing the history of AI and security, examining how GenAI is reshaping technology and workplaces, and introducing the emerging risk frameworks that help us make sense of it all. From there, we get hands-on with the protocols defining this new age of autonomous agents, including MCP and A2A. We then dive deep into the vulnerabilities unique to AI-integrated systems, such as prompt injection and other LLM-based attack vectors. Finally, we turn to defense: designing robust, resilient AI systems, evaluating real-world AI deployments within an organization, and implementing best practices for mitigating AI-driven risks.

CompTIA Security+ exam

Sprint 15
Obtain
Your CompTIA
Security+
Credential

Take the industry-recognized CompTIA Security+ exam and submit your certificate as the capstone achievement of your program experience.

Career Preparation

During the program

Stay connected to your career goals while focusing on technical learning.

Career-focused lessons throughout the program

Job market insights and career awareness

Professional and soft skills development

Career Sprint

Spend 6 weeks preparing for your job search after graduation.

Build your resume, LinkedIn profile, and job search strategy

Join live group sessions and AMA sessions with career coaches and industry experts

Get started with our AI-powered job search platform for interview practice, career resources, and application management

Active Job Search

Throughout your job search period (up to 10 months), you'll receive ongoing guidance from the Career Team, strengthen your professional network, and have opportunities to keep building your portfolio.

Get guidance from your assigned career coach

Use our AI-powered job search platform to manage applications, networking, and interviews

Attend live career workshops and other learning opportunities

Access TripleTen's job board with roles from our employer network

Get opportunities to work on projects with partner employers

Receive unlimited AI-powered HR and technical interview practice

Practice live mock interviews with your coach when you land an interview

Learn the job by doing the job

7 months

Online

Part-time