



Cybersecurity

CAREER TRACK SYLLABUS

2023

In partnership with

CompTIA
Authorized Partner

DELIVERY
PARTNER

INFOSEC
LEARNING
LLC

Content



Overview	3
Syllabus - AI for Cybersecurity	5
Syllabus – Core Units	6
Practical Skills For Your Portfolio	11
Career Support	13
Achieving Your Goals with the Springboard Learning Experience	14



Overview

With data migrating to the cloud and growing geopolitical concerns around security and privacy, many companies are investing in their cybersecurity expertise. They are looking to protect and defend their data through the identification, analysis, and mitigation of threats.

The **Springboard Cybersecurity Career Track** will teach you job-ready cybersecurity analysis skills, including the core mindset, tools, and best practices in the field. The learning resources and projects contained in the program are geared toward the CompTIA Security+ certification, the cost of which is included in this bootcamp. By the end of the program, you'll have the complete cybersecurity skillset to succeed on a network and information security team.

Overview

What You'll Learn

Over the course of six months, you'll:

- Gain proficiency in foundational cybersecurity skills and practices.
- Safeguard information systems, ensuring the integrity, availability, and confidentiality of data.
- Get hands-on experience aligning cybersecurity strategies with business goals.
- Develop the technical and professional skills to launch a career as a cybersecurity analyst, specialist, incident responder, or SOC analyst.
- Prepare for the CompTIA Security+ exam and CompTIA CySA+ certification.

How You'll Learn


- **An online curated curriculum** helps you absorb cybersecurity skills and best practices.
- **Project-based learning** through hands-on labs, mini-projects, and a capstone project helps you attain proficiency in end-to-end analyses and industry processes.


What You'll Gain


- **Graduate with a CompTIA Security+ Certification:** Chosen by more corporations and defense organizations to validate security skills than any other.
- **1-on-1 mentor support:** You'll be matched with a mentor who will help you tackle the curriculum, provide regular feedback, and answer your questions. Your mentor will keep you accountable and give you an insider's perspective.
- **Career coaching:** You'll work through career-specific units with a career coach guiding you — from defining your strategy, and developing your resume and LinkedIn profile to networking, mock interviews, and salary negotiation.
- **A certificate of completion and our Job Guarantee:** You'll graduate with a certificate from Springboard backed by our Job Guarantee — if you don't land a job after graduating, we'll give you a full refund. **Terms apply.**

Key Program Details

 **6 months**
Program length

 **10-20**
Hours per week

 **85 total projects**
55 labs
30 mini-projects
1 guided capstone

 **Prerequisites**

- No previous experience required
- Be prepared to pass an evaluation of baseline soft skills

Tools & skills learned



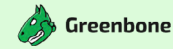
WIRESHARK



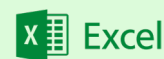
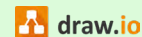
KALI
BY OFFENSIVE SECURITY



splunk>



LOIC
Low Orbit Ion Cannon





Syllabus

AI for Cybersecurity Units

1. AI for Cybersecurity Units

Learn to leverage the power of AI with new learning units throughout your cybersecurity curriculum. You'll explore AI's practical applications and how to leverage them to solve cybersecurity challenges. Learn how to identify and respond to security threats in real time, to predict cyber threats and future attack trends. With AI by your side, you can become a powerful guardian of cyberspace, and a valuable asset to your employer.

Topics Covered:

- Introduction to AI and its applications in cybersecurity
- AI for threat detection and incident response
- AI in malware analysis and NLP
- AI in network security and threat hunting
- AI for predictive security analytics

Syllabus

Core Units

1. Cybersecurity Basics

In this unit, you'll learn the basics of cybersecurity, gaining a comprehensive understanding of what cybersecurity is, its core definition, and discover the diverse career roles tied to this rapidly growing industry. Furthermore, we will focus on building essential Operating System skills, laying the groundwork for a strong technical foundation.

Topics Covered:

- Cybersecurity roles and careers
- Cybersecurity specializations
- Cybersecurity best practices
- Vocabulary and acronyms
- Introduction to operating system concepts

2. Cybersecurity Fundamentals

In this unit, you'll study the behavior, motivations, and game plan of your adversary — the cybercriminal. Learn about threat actors, the most common types of attacks, plus the frameworks and models used to build a robust defensive playbook.

You'll then learn how professionals set the defense standards through the CIA Triad, and the cyber kill chain model as you analyze real-life data breaches.

Topics Covered:

- The CIA triad: Three-legged stool
- Threat actor types and attributes
- Cyber kill chain
- Ethical hacking
- Using Linux and Unix
- Intro to comptia security+ certification

3. Cybersecurity Attacks

Attacks, threats, and vulnerabilities are key concepts in the field of cybersecurity and information security. Vulnerabilities are weaknesses in a system or network, threats are potential risks or dangers that can exploit these vulnerabilities, and attacks are the actual actions taken by threat actors to exploit vulnerabilities and compromise security.

Topics Covered:

- Social engineering
- Attack types

Core Units

4. Host-Based Security

This unit will focus on host security, namely workstation and servers. It includes patching, hardening, and secure configuration. These activities are critical to defending and securing servers and workstations from threat actors and are often the first line of defense against attacks.

Topics Covered:

- Operating System Hardening
- Microsoft Windows Hardening
- Advanced Hardening Concepts
- System Patching
- Virtualization Technology

5. Network Security

Network security protects the integrity, confidentiality, and accessibility of computer networks and data using software and hardware technologies. You'll explore firewalls, the Internet of Things (IoT), and embedded systems. Next, you'll dive into network devices and technologies such as load balancers, routers, switches, virtual private networks, network access control, proxy servers, and intrusion prevention. Finally, you will learn the latest in wireless security and deployment options with cloud computing as you get hands-on practice with firewalls and RADIUS.

Topics Covered:

- Network technologies and models
- Securing tcp/ip networks
- Network attacks
- Network devices
- Firewalls, IoT, and embedded systems
- Wireless and cloud

6. Identity and Access Management

Identity and Access Management (IAM) is one of the most important disciplines within cybersecurity. It aims to manage user identities and their access to enterprise resources and data. In this unit, you'll learn IAM governance and how to manage user identities and access through authentication, authorization, and accounting.

At the end of the unit, you'll have the option to prepare for and take the Microsoft Security, Compliance, and Identity Fundamentals exam (Exam SC-900), which is 50% off for students taking this bootcamp.

Topics Covered:

- Controlling access
- Zero trust
- Microsoft security, compliance, and identity fundamentals

Core Units

7. Cryptography

Cryptography is the science and practice of securing communication and information by converting it into an unreadable format (ciphertext) and then back into its original, readable form (plaintext) using mathematical algorithms and encryption techniques. It plays a crucial role in ensuring the confidentiality, integrity, authenticity, and non-repudiation of data in various applications. In this unit, you'll take a deep dive into cryptographic technologies and concepts, all of which are covered in the Security+ exam.

Topics Covered:

- Cryptography technologies and methods



8. Security Architecture

Security architecture, also known as information security architecture, is a structured framework for designing and implementing security measures within an organization to protect its information, assets, and technology infrastructure. It encompasses the policies, processes, technologies, and practices that are employed to ensure that an organization's information and resources are secure from a wide range of threats and risks. Effective security architecture is essential to safeguard sensitive data, maintain compliance with regulations, and mitigate security vulnerabilities.

Topics Covered:

- Enterprise Security
- Authentication and Authorization
- Resilience

Core Units

9. Security Operations (SecOps)

In the Security Operations unit, you'll learn blue-team security operations, including security toolsets, encryption, and incident response workflows and procedures. Industry-relevant, leading tools you'll use in this unit include Splunk and Wireshark. In addition, foundational scripting skills that will make you a successful cybersecurity analyst, using Python, will also be covered.

Topics Covered:

- Using Tools to Monitor Systems and Networks
- Forensics
- Asset Security
- Physical Security
- Incident Response and Investigation

10. Application Security

Software is usually developed with a strong focus on functionality, not security. In many cases, security controls are bolted on as an afterthought (if at all). To get the best of both worlds, security and functionality have to be designed and integrated at each phase of the development life cycle to provide protection at the necessary layers.

This unit will cover the complex world of secure software development and the vulnerabilities and risks that are left open when security is not properly interwoven into applications.

Topics Covered:

- Intro to application security
- Secure development
- Application attacks
- Application security implementation



Core Units

11. Security Assessment and Testing

In this unit, you'll learn how to conduct security assessments and recommend remediation activities as well as how to create Information Security (IS) audit test plans, gaining insight into how IS auditors approach their engagements. You'll also get exposure to advanced concepts around web security testing and the use of Kali Linux.

Mini-projects will allow you to explore another side of penetration testing, real-world vulnerability management challenges, and software testing plans. The Labs in this unit will give you another slice of the red-team world, taking you through attacking web servers, exploring a vulnerable web application, and cracking passwords.

Topics Covered:

- Logical and physical security testing
- Mobile device security
- Governance risk and compliance
- Security policies

12. CompTIA Security+ Exam Prep

In this final unit, you will run through practice Security+ Exams and will receive study tips to obtain the Security+ credential. Security+ is an industry-wide recognized certificate for cybersecurity professionals demonstrating they have obtained fundamental cybersecurity skills. Certificate achievement will help you more easily secure a job and is also a requirement to qualify for the Springboard Job Guarantee. A voucher to cover the exam cost is included in the program cost.

Topics Covered:

- Exam topics refresh and review
- Exam state of readiness
- Mock exams



Practical Skills for Your Portfolio

The bootcamp will guide you to complete **30 labs, 35 mini-projects, and 1 capstone project** to help you build strong, practical skills and prepare you for a career in cybersecurity.

Practical Skills for Your Portfolio

Labs

To provide you with practical experience using your newly acquired cybersecurity knowledge, this bootcamp features 30 labs. Labs range from practicing on real-world scenarios to building and sharing a custom cybersecurity range. You will practice what you've learned in each unit by completing labs involving host and network security hardening, malware crafting and analysis, and application security practices.

Mini-Projects

The 35 mini-projects included in this bootcamp range from researching and analyzing real-world events to reviewing industry-leading materials, such as podcasts, videos, and writing reflections on the topic, helping you to develop analytical and communication skills for a successful career. Your mini-projects will also allow you to put together a few high-level project plans, giving you a taste of the project-management aspect of cybersecurity roles.

Capstone Project

The guided capstone project will consist of several stages of solution design for a given problem statement. During this capstone, you will be required to work on a hypothetical “structured walkthrough” penetration test. The guided capstone is designed to help you understand how various components that you learn throughout the bootcamp come together to form an experience that familiarizes you with a day-in-the-life of a security analyst.

The five phases include:

- Phase 1: Perform reconnaissance
- Phase 2: Identify targets and run scans
- Phase 3: Identify vulnerabilities
- Phase 4: Threat assessment
- Phase 5: Reporting



Career Support

Career units throughout the bootcamp will help you create a tailored job search strategy based on your background and goals. Learn to craft a resume that stands out from the pack, evaluate companies and roles, ace interviews, and negotiate the best possible salary.

Your career coach will be with you every step of the way, offering feedback and providing personalized tips based on your goals.

Topics Covered

- Types of industry roles
- Job search strategies
- Building a network and using it to land interviews
- Creating a high-quality resume, linkedin profile, and cover letter
- Preparing for technical and non-technical interviews
- Successful negotiation

Build the Skills and Confidence to Transform Your Career

Learn through projects. Work 1-on-1 with a mentor and career coach.
Land a job or your money back.

HANDS-ON LEARNING

A high quality, project-based curriculum designed by industry experts helps students master their area of study so they're career ready.

REAL HUMAN SUPPORT

Students receive the dedicated support of a personal mentor, career coach, and student advisor, plus 24/7 access to a peer community.

MORE FREEDOM

100% online classrooms give students the flexibility they need to continue working while attending Springboard.

JOB GUARANTEE

You'll graduate with a certificate from Springboard backed by our Job Guarantee — if you don't land a job after graduating, we'll give you a full refund. [Terms apply](#).

Springboard Students Achieve Life-Changing Outcomes

NUMBER OF ENROLLED STUDENTS

810

Enrolled students in the Cybersecurity Career Track since March 2021.¹

September 2022

12 MONTH JOB PLACEMENT RATE

100%

Of job-qualified individuals who reported an offer, received it within 12 months of graduation.²

September 2022

AVERAGE SALARY INCREASE

\$12,228

Average salary increase of Cybersecurity students who provided pre- and post-course salaries.³

September 2022

¹ Number of students refers to all students who enrolled in the career track excluding any that were refunded due to cancellation in the first 7 days following course start.

² Job-qualified individuals defined as all graduates who maintained Job Guarantee eligibility (terms are from the Cybersecurity Career Track Job Guarantee) throughout their job search ("Job-Qualified Graduates"), or Job Guarantee-eligible students who receive a job regardless of completion status ("Early Offerees").

³ Data on compensation was not self-reported by 19 students who reported receiving offers.

Ready for the next step?

Learn more and apply [here](#)



Questions? We're here to help

Email us at hello@springboard.com
or call [+1.415.966.2533](tel:+14159662533)