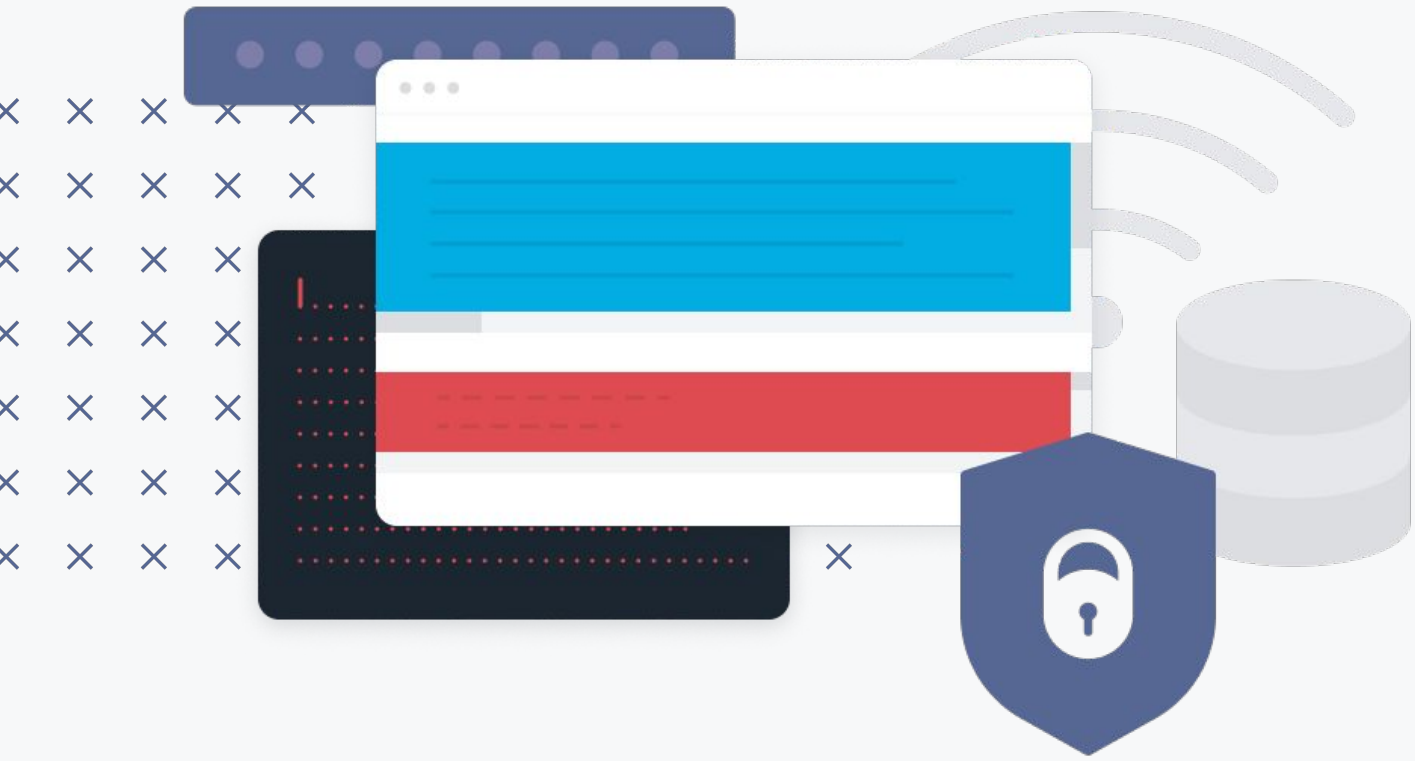


SYLLABUS | FULL-TIME

Cybersecurity Engineering

Become a Cybersecurity Engineer in as little as 15 weeks.

// FLATIRON SCHOOL

Table of Contents

Why Cybersecurity?

The demand for Cybersecurity professionals is growing rapidly. In fact, The Bureau of Labor & Statistics indicate a 35% national growth for Security Analysts, which is much faster than the average of all occupations.

Flatiron School's Cybersecurity Engineering course takes a holistic approach towards learning, teaching students fundamental principles and problem-solving techniques as well as the latest technologies. Our course features hands-on, collaborative experiences, whether that is leveraging AI (artificial intelligence), ML (machine learning), or the latest tools such as ChatGPT.

Our Cybersecurity Engineering graduates have raved about the structure, support, and camaraderie throughout the course. After graduation we provide all the ingredients for an effective job search, including 180 days of 1-on-1 career coaching. Ultimately, our grads have landed jobs at some amazing companies - Google, Meta, and Facebook, to name a few.*

POSSIBLE CYBERSECURITY CAREER PATHS

CYBER ENGINEER | Average salaries: $134,280

Cybersecurity Engineers, sometimes called Information Security Engineers, identify threats and vulnerabilities in systems and software, then apply their skills to developing and implementing high-tech solutions to defend against hacking, malware and ransomware, insider threats and all types of cybercrime.
(salary from ZipRecruiter, as of May 2023)

PENETRATION TESTER | Average salaries: $117,189

Penetration Testers help organizations identify and resolve security vulnerabilities affecting their digital assets and computer networks.
(salary from ZipRecruiter, as of May 2023)

SECURITY ANALYST | Average salaries: $102,379

Security Analysts are responsible for ensuring the company's digital assets are protected from unauthorized access. This includes securing both online and on-premise infrastructures, weeding through data to filter out suspicious activity, and mitigating risks before breaches occur.
(salary from ZipRecruiter, as of May 2023)

SECURITY CONSULTANT | Average salaries: $101,619

Security Consultants protect a company's assets. They prevent possible threats and create contingency protocols for when violations occur.
(salary from ZipRecruiter, as of May 2023)

Includes graduates from all disciplines at Flatiron School, Designation Labs, or SecureSet Academy who were hired from 2012 - 2023

Course Overview

Network Security
This course will focus on the core ideas in network security - Ethernet, WIFI, attacks on TCP hijacking, and more.

Systems Security
This course will focus on System Architecture, Operating System Architecture, System Exploits (hardware, operating system and memory). Learn to utilize tools such as Metasploit and command line tools in Linux.

Cyber Threat Intelligence
The course teaches techniques organized around military principles of intelligence analysis and introduces larger concepts of how cyberspace has become a new warfighting space

Governance, Risk Management, & Compliance
This course covers how to engage all functional levels within the enterprise to deliver information system security. The course addresses a range of topics on securing the modern enterprise.

Logs & Detection
This course will focus on engineering solutions to allow analyzing the logs in various network devices, including workstations, servers, routers, firewalls and other network security devices.

Python
This six-week course course provides the fundamental structure and language for creating Python scripts and automation. The focus will be on learning basic coding, code analysis and secure coding practices.

Application Security & Penetration Testing
This course focuses on applications and their vulnerabilities running on both workstations and servers. You'll learn penetration testing for vulnerabilities either in applications or network resources.

Applied Cryptography
This 9-week course teaches the components of cryptography, provides hands-on experience on configuring a web server with SSL/TLS, and interfacing with Certificate Authorities, issuing certificates, configuring SSH securely, and sending/receiving encrypted and signed email.

Capstone
The group project will present a scenario and allow the students to work within their individual expertise to work through the particulars. The project will culminate in a professional level oral and written report, which can be used as part of a portfolio.

COURSE OUTLINE BY PHASE

		HOURS	DAYS
PHASE 1	**Cybersecurity Foundational Skills** Network Security, Systems Security, Applied Cryptography, GRC, and Python	105	15 (3 weeks)
PHASE 2	**Cybersecurity Intermediate Skills** Systems Security, Network Security, Applied Cryptography, Cyber Threat Intelligence, and Python	105	15 (3 weeks)
PHASE 3	**Cybersecurity Skills Development** Systems Security, Network Security, Applied Cryptography, Cyber Threat Intelligence, and Logs & Detection	105	15 (3 weeks)
PHASE 4	**Gray Hat Hacking** Systems Security, Network Security, Logs & Detection, Application Security & Penetration Testing, and GRC	105	15 (3 weeks)
PHASE 5	**Cybersecurity Skills Application** Systems Security, Network Security, Logs and Detection, Application Security and Penetration Testing, & Capstone	105	15 (3 weeks)
PROGRAM TOTAL		525	

Curriculum

Cybersecurity Engineering Prep

All students are required to complete what we call “Cybersecurity Engineering Prep” at least one week before the start of class. During the prep course, students will get accustomed to the Canvas platform, set up their virtual machines, and obtain a basic understanding of Python, Systems, and Networks to prepare them for day 1 of class.

The prep course generally takes between 30-40 hours to complete, and is bookended by a pre-test and post-test to assess understanding of the concepts covered.

Network Security

This course will focus on the core ideas in network security. The first portion of the class will continue review of basic network protocols: Ethernet, 802.11 (WiFi), IP, UDP, TCP, ARP, DHCP, DNS, ICMP, BGP, SMTP, POP/IMAP, FTP, HTTP, IGMP, and the attacks on these basic technologies: TCP hijacking, ARP cache poisoning and domain spoofing, as well as countermeasures. We then explain sniffing and port scanning, firewalls, IDSes and NIDSes and cover wireless protocols and their security. Then we segue into AppSec with a focus on web security. Finally, we look at denial of service and attack payloads.

TOOLS LEARNED

WIRESHARK
LAMP STACK
WEB SPIDERS
HONEYPOTS
MARAI BOTNET
IOT
TCP HIJACKING
ETHERNET SNIFFING
DNSSEC
SQL/INJECTION
IP FUNDAMENTALS
FIREWALLS, WAFS
NETCAT
PORT SCANNING
WPA/AIRCRACK-NG
ARP CACHE/POISONING
FILTERING AND REGEX
IDS/IPS
SOAP/REST
XSS

At the completion of this course, a student will be able to:

- Utilize the layers of the TCP/IP and OSI models in analyzing network protocols.
- Analyze packet captures and draw conclusions about network activity.
- Create a web application and evaluate its security.
- Explain network security protocols as well as their vulnerabilities.
- Utilize attack tools to mount attacks against various types of networks and use countermeasures to forestall these same attacks.
- Map ports on a given IP, fingerprint services, catalog vulnerabilities, bypass firewalls, and mount a large array of web-based exploits.
- Deliver a wide variety of payloads to attain and maintain backdoor access to a compromised machine.
- Analyze AI/ML/ChatGPT traffic and use AI for deep packet inspection.

TOOLS LEARNED

WINDOWS
LINUX SYSTEM
BASH SHELLS
LINUX SEC MODEL
AUTHENTICATION
ACTIVE DIRECTORY
OWASP
BASIC C CODING
LINUX COMMAND
ASSEMBLY BASICS
BUFFER OVERFLOW
SHELLCODE INJECTION
METASPLOIT PAYLOADS
METERPRETER
ROOT KITS
CLOUD SECURITY
HYPERVISOR EXPLOITS
IOS SECURITY

Systems Security

This course will focus on System Architecture, Operating System Architecture, System Exploits (hardware, operating system and memory). We will also utilize tools, including Metasploit and command line tools in Linux (xxd, gdb, etc) for further analysis of exploits.

We will explore exploits and their countermeasures, including buffer overflows, TOCTOU, shellcode injections, integer overflows and off-by-one errors. We will also cover basic Cloud security and migration considerations, Hypervisor Exploits and Android and iOS security.

At the completion of this course, a student will be able to:

- Utilize AI/ML/ChatGPT for host hardening and secure coding.

Cyber Threat Intelligence

TOOLS LEARNED

OPERATIONAL DESIGN
OPEN SOURCE INTELLIGENCE (OSINT)
MALTEGO
SOCIAL ENGINEERING
CYBER THREAT INTELLIGENCE CYCLE
INTELLIGENCE PREPARATION OF THE ENVIRONMENT
CYBER KILL CHAIN
ACTIVE CYBER DEFENSE MODEL
CENTER OF GRAVITY ANALYSIS
CARVER MATRIX

Cyber Threat Intelligence 100 provides students with the foundational skills of a Threat Intelligence Analyst. The course teaches techniques organized around military principles of intelligence analysis and introduces larger concepts of how cyberspace has become a new warfighting space that targets private and public critical infrastructure, economic and national security targets across all sectors globally. Students must understand the overall threat environment, how to discern the "so what" of information, and critically think and analyze complex human influenced cyber problems and threats to public and private information enterprises. Threat Intelligence 200 introduces students to the various methodologies of intelligence analysis and planning. Students will learn about the Cyber Kill Chain, Center of Gravity (COG) Analysis and CTI Diamond Model and then learn how to apply them using Cyber Intelligence Preparation of the Environment (IPE). The class, Cyber Mission Analysis, will culminate with students presenting their Mission Analysis Brief to the instructor as if they are the CISO.

A high-level perspective of threat intelligence (its creation and consumption):

- Adversary monetization methods
- Intelligence gathering
- Intel sources
- Intelligence analysis
- Planning with intelligence
- Leveraging AI/ML/ChatGPT for threat intelligence feeds

Governance, Risk Management & Compliance

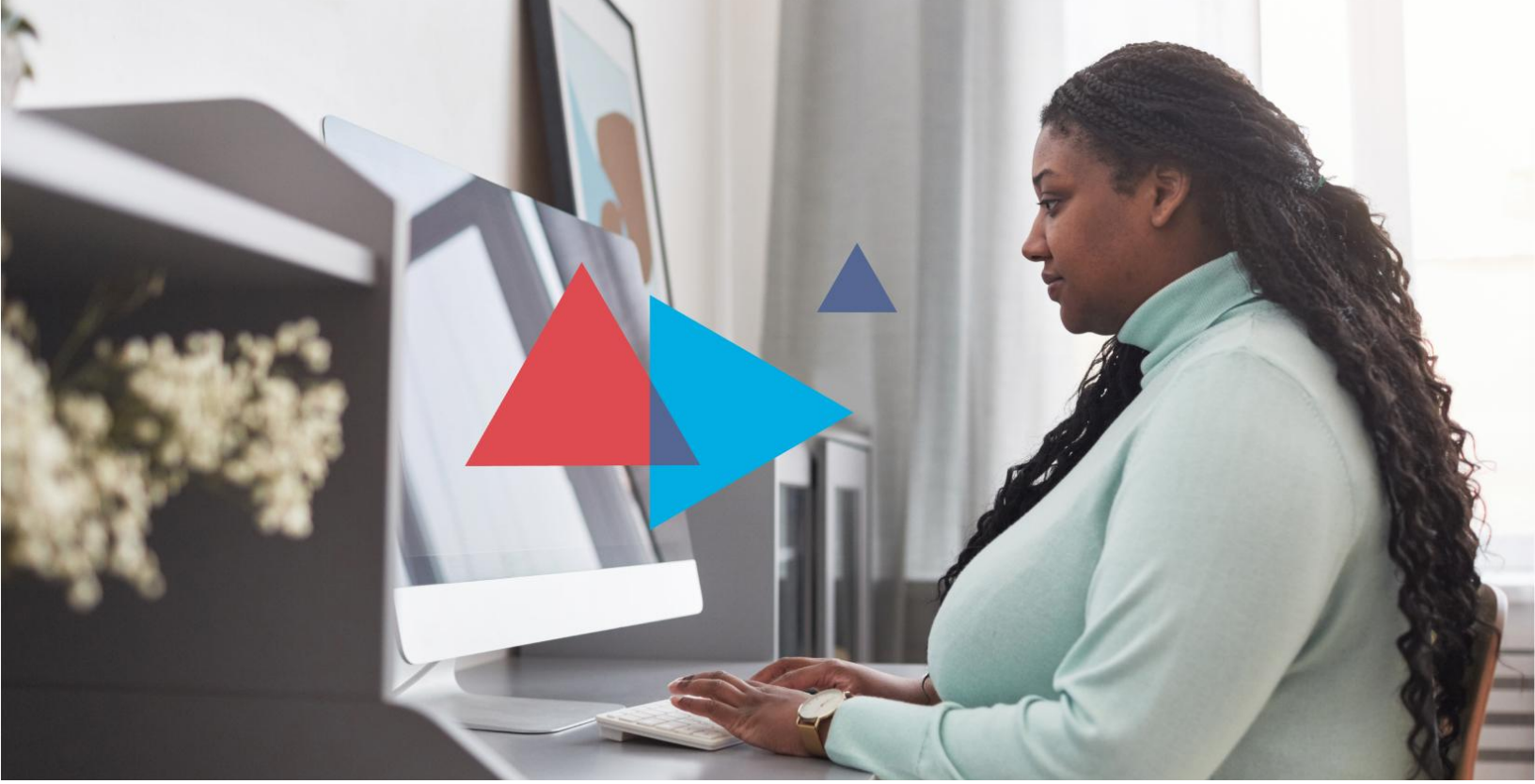
TOOLS LEARNED

ISO/IEC 38500
COBIT 5
ISO/IEC 27001
OCTAVE
NIST
ITIL
RISK MANAGEMENT FRAMEWORK
CIA MODEL
BUSINESS IMPACT ANALYSIS
IDENTITY AND ACCESS MANAGEMENT

This course will focus on Governance, Risk, and Compliance (GRC). Students will learn how to engage all functional levels within the enterprise to deliver information system security. To this end, the course addresses a range of topics, each of which is vital to securing the modern enterprise. These topics include inter alia plans and policies, enterprise roles, security metrics, risk management, standards and regulations, physical security, and business continuity. Each piece of the puzzle must be in place for the enterprise to achieve its security goals; adversaries will invariably find and exploit weak links. By the end of the course, students will be able to implement GRC programs at the maturity level that many organizations are not at currently and to establish efficient, effective, and elegant Information Security Programs.

A high-level perspective of threat intelligence (its creation and consumption):

- Plans and policies
- Enterprise roles
- Security metrics
- Risk management
- Standards and regulations
- Physical security
- Business continuity
- Identify AI/ML/ChatGPT compliance, privacy, and risk considerations



TOOLS LEARNED

CYBER KILL CHAIN AND LOGGING
REGEX
LOGSTASH AND FILEBEAT CONFIGURATION
NETWORK MAPPING
NORMALIZATION
SIEM ARCHITECTURE & AUTOMATION
DATA VISUALIZATIONS
KIBANA
SPLUNK

Logs & Detection

This course will focus on engineering solutions to allow analyzing the logs in various network devices, including workstations, servers, routers, firewalls and other network security devices. We will explore the information stored in logs and how to capture this data for analyzing these logs with a Security Information and Event Manager (SIEM). We will learn the steps involved in Incident Response and Crisis Management.

At the completion of this course, a student will be able to:

- Identify log sources and the configurations necessary to achieve appropriate logging levels.
- Describe the different types of data contained in log files.
- Configure data sources and SIEMs to allow the analysis of log data, including the automation of those tasks.
- Identify steps in Incident Response and Crisis Management.
- Use AI/ML/ChatGPT to detect anomalous and behavioral events.

TOOLS LEARNED

PYTHON 2.X
PYTHON 3.X
PYTHON IDES
CONDITIONALS
LOOPS
DATA STRUCTURES

Python

Python programming is a fundamental skill used by Cybersecurity Engineers. This six week course course provides the fundamental structure and language for creating Python scripts and automation. The focus will be on learning basic coding, code analysis and secure coding practices.

Python 100 will cover the differences between interpreted and compiled coding languages. The focus for the interpreted languages will be the basic code structure for Python, conditionals, loops and algorithm diagramming tools. Students will work on analyzing basic code, modify that code to add additional functionality and writing simple algorithms.

Python 200 will dive deeper into topics such as more advanced algorithms and Object Oriented Programming. Secure coding techniques and methodologies will also be covered, including standard frameworks.

Python code will be utilized in other courses, such as Networking, Systems and Cryptography.

At the completion of this course, a student will be able to:

- Analyze Python scripts to determine what functionality they provide.
- Write simple Python scripts using conditionals, loops, variables and other data structures.
- Import modules to increase the functionality of the Python script.
- Use coding frameworks to ensure secure coding techniques are utilized.
- Address considerations for AI/ML/ChatGPT for secure coding.

TOOLS LEARNED

PENETRATION TESTING EXECUTION STANDARD (PTES) FRAMEWORK

METASPLOIT
OPENVAS
NMAP
SHELLCODE GENERATION
FUZZING
ROOTKITS
BURP SUITE

Application Security & Penetration Testing

Application Security focuses on the applications and their vulnerabilities running on both workstations and servers. Penetration testing is using vulnerabilities either in applications or network resources that allows for exploitation. This can lead to server downtime, service interruptions or in the worst case, root level access for the malicious actor. This six-week course focuses on methodologies utilized by penetration testers to analyze and assess risk to systems, networks, applications and other vulnerable areas of concern to a company. These are the same techniques used by malicious actors to compromise a company. The role of the penetration tester is critical in finding the vulnerabilities and risks before they can be exploited.

APP100 will focus on the basic techniques and tools employed by a penetration tester or hacker. The focus will be on the Penetration Testing Execution Standard (PTES) framework for determining where a company has exposure, testings the vulnerabilities, and basic approaches to exploiting the vulnerabilities. Additionally, network mapping will be revisited and specific techniques for reconnaissance will be discussed.

APP200 will look at specific exploits and how they can be utilized to more efficiently target and exploit systems and networks. The focus will be on crafting specific exploits based on the results of the reconnaissance techniques. Finally, post exploitation activities and reporting will be discussed.

At the completion of this course, a student will be able to:

- Describe the usage of Metasploit and other Kali Linux pentesting tools.
- Describe the Penetration Testing Execution Standard (PTES).
- Utilize attack tools to mount attacks against various types of networks and applications and use countermeasures to forestall these same attacks.
- Deliver a wide variety of payloads to attain and maintain backdoor access to a compromised machine and actions to combat these attacks, as well.
- Leveraging AI/ML/ChatGPT for vulnerability and pen testing.

Applied Cryptography

TOOLS LEARNED

BASIC SYMMETRIC CIPHERS
DES/3DES
AES
MODES OF OPERATION
HASH FUNCTIONS
AUTHENTICATION (HMAC)
RSA
OPENSSL
BITCOIN
SSLSTRIP

This 9-week course in Applied Cryptography teaches students the components of cryptography, provides hands-on experience on configuring a web server with SSL/TLS, and educates students in interfacing with Certificate Authorities, issuing certificates, configuring SSH securely, and sending/receiving encrypted and signed email.

In the 100 module students will be introduced to basic principles of encryption and authentication; additionally, students will understand and analyze historical approaches to cryptography. Students will practice symmetric cryptography, namely block ciphers, hash functions, and message authentication Codes.

The 200 module focuses on asymmetric cryptography (i.e. RSA and Diffie-Hellman Key Exchange). Combined with symmetric encryption, this makes a powerful combination for securing communications. Applications of these technologies will be explored by deploying SSL and SSH solutions. The 300 module covers anonymity and exploits using cryptography. Students explore weaknesses in WEP and SSL that lead vulnerabilities and discover how to counter them.

At the completion of this course, a student will be able to:

- Explain the fundamental goals of cryptography.
- Apply knowledge to use common crypto software.
- Analyze vulnerable applications with respect to cryptographic best practices.
- Create tools to attack and fix applications in a virtual lab environment.
- By the course's conclusion, students will have covered all relevant parts of the cryptography section of the industry-standard CISSP certification program.
- Identify how bad actors could leverage AI/ML/ChatGPT to crack encryption.

TOOLS LEARNED

All tools from any course may be taught and/or utilized.

Capstone

The scenario-based capstone activity allows the student to demonstrate their knowledge and proficiency. The group project will present a scenario and allow the students to work within their individual expertise to work through the particulars. Very little guidance will be given, allowing the students to work along multiple paths to completion. The project will culminate in a professional level oral and written report, which can be used as part of a portfolio.

At the completion of this course, a student will be able to:

- Apply the knowledge from all previous courses to analyze a scenario, for example by performing risk assessments or other security analysis.
- Utilize the knowledge from all previous courses to recommend best practice approaches to improve security posture in the scenario.
- Utilize the knowledge and skills from all previous courses to implement appropriate security controls and countermeasures in the scenario.
- Demonstrate decision-making, compliance, strategy development and professional communications through oral and written reports designed to support and make recommendations to senior management.

Pace & Schedule

At Flatiron School, we know that how you choose to study is as integral to your success as what you're learning. Paired with our online learning platform, Canvas, and individualized support, all students have access to a personalized learning experience.

Learn online. But not alone.

The community at Flatiron School is unmatched - from study groups to peer projects and Slack check-ins, our students often say their cohort supported them through the program.

You'll start the program with a cohort of students, all learning together in a live lecture format.

FULL-TIME LIVE

Length	15 weeks
Time Commitment	60 hrs/week
Career Services Support	Yes
1:1 with Instructors	Yes
Live Lectures	Yes
Assigned Cohort	Yes

Why Flatiron School?

Here at Flatiron School our ultimate goal is to prepare students to be successful in any job market. That's why our curriculum is regularly reviewed by hiring managers and incorporates the latest emerging technologies, such as how to leverage ChatGPT as well as other AI and ML tools.

During class, we have a hands-on, community approach to learning, one that includes lab work, creating a real-world portfolio, and 1-on-1 instructor access.

After graduation we provide all the ingredients for an effective job search, including 180 days of 1-on-1 career coaching.

WHERE OUR GRADS HAVE BEEN HIRED

Includes graduates from all disciplines at Flatiron School, Designation Labs, or SecureSet Academy who were hired from 2012 - 2023

// FLATIRON SCHOOL

Let’s stay in touch.

Education should be the best investment you make — and at Flatiron School, we’re committed to helping you learn the skills change your future. Online and on our New York or Denver campuses, we provide the skills, community, and immersive, outcomes-driven curriculum you need to launch a career in Cybersecurity, Software Engineering, Data Science, or UX / UI Product Design.

Apply Today

Start your application for one of our immersive bootcamps and change your life today.

Apply Now

Attend an Event

Join us for a seminar or info session to see what student life is like at Flatiron School.

See Events

Chat with Admissions

Have a question about our program that we haven’t answered? Our admissions team is here to help.

Schedule a Chat