SYLLABUS | FLEX

Cybersecurity Engineering

Flexible pacing option. You pick the pace—20, 40, or 60 weeks.

// FLATIRON SCHOOL

Table of Contents

Why Cybersecurity?

You are living in unprecedented times in the course of technological development. The world has fully adopted the most transformational technology in its history before figuring how to deal with its inherent—and very real—risks. The Internet is revolutionizing the world. We are totally dependent on it. But, it wasn't designed with security in mind. We have traded our personal security for convenience.

That's where cybersecurity comes in. This relatively new, exploding industry is on a mission to secure a world that suddenly finds itself running on the Internet, and thereby enabling the future potential of technology itself. The world needs more cybersecurity professionals.

Our Cybersecurity Engineering program will prepare you for entry-level jobs in the cybersecurity industry.

Security Engineer
Design computer security architecture and develop detailed cybersecurity designs. You are a security builder and guard.

Security Analyst
Perform information assurance certification, accreditation analysis, and security assessments. You are a security detector and protector.

Security Consultant
Lead/perform the delivery of data protection engagements including discovery and classification (structured and unstructured). You are an advisor and guide.

Security Pen Tester
Perform external, internal, and wireless network penetration tests. You are an ethical hacker.

The U.S. Bureau of Labor Statistics predicts cybersecurity jobs will grow 31% through 2029, over seven times faster than the national average job growth of 4%.

According to the U.S. BUREAU OF LABOR STATISTICS Occupational Outlook Handbook

Program 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). Part of the course will focus on learning to utilize tools such as Metasploit and command line tools in Linux.

Cyber Threat Intelligence
This course teaches techniques organized around military principles of intelligence analysis and introduces larger concepts related to how cyberspace has become a new warfighting arena.

Governance, Risk Management, and 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 and 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 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 and Penetration Testing
This course focuses on applications, and their vulnerabilities, running on both workstations and servers. The focus will involve learning penetration testing for vulnerabilities in applications and network resources.

Applied Cryptography
This course teaches the components of cryptography, provides hands-on experience 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
This course will present a scenario-based capstone project and will culminate in a professional level oral and written report, which can be used as part of a portfolio.

Program Outline by Phase

Phase	Hours
Phase 1: Cybersecurity Foundational Skills Systems Security, Network Security, Applied Cryptography, GRC, & Python	105
Phase 2: Cybersecurity Intermediate Skills Systems Security, Network Security, Applied Cryptography, Cyber Threat Intelligence, & Python	105
Phase 3: Cybersecurity Skills Development Systems Security, Network Security, Applied Cryptography, Cyber Threat Intelligence, & Logs and Detection	105
Phase 4: Gray Hat Hacking Systems Security, Network Security, Logs and Detection, Application Security and Penetration Testing, & GRC	105
Phase 5: Cybersecurity Skills Application Systems Security, Network Security, Logs and Detection, Application Security and Penetration Testing, & Capstone	105
Program Total:	**525***

*In addition to the program hours set forth above, most students will need to spend additional to complete the work and fully understand the material.

Curriculum

PRE–WORK

Cybersecurity Engineering

All students are required to complete what we call “pre-work” at least one week before the start of class. During pre-work, 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. Pre-work 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 review 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.

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

- Categorize network security protocols and their vulnerabilities
- Employ common network tools to analyze and view network traffic and use attack tools to mount attacks against various types of network, then select countermeasures to forestall these same attacks.
- Analyze network assets by mapping ports on a given IP, fingerprinting services, cataloging vulnerabilities, bypassing firewalls, and mounting a large array of web-based exploits.
- Install web services and analyze common web vulnerabilities against those services, including appropriate countermeasures.

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

Systems Security

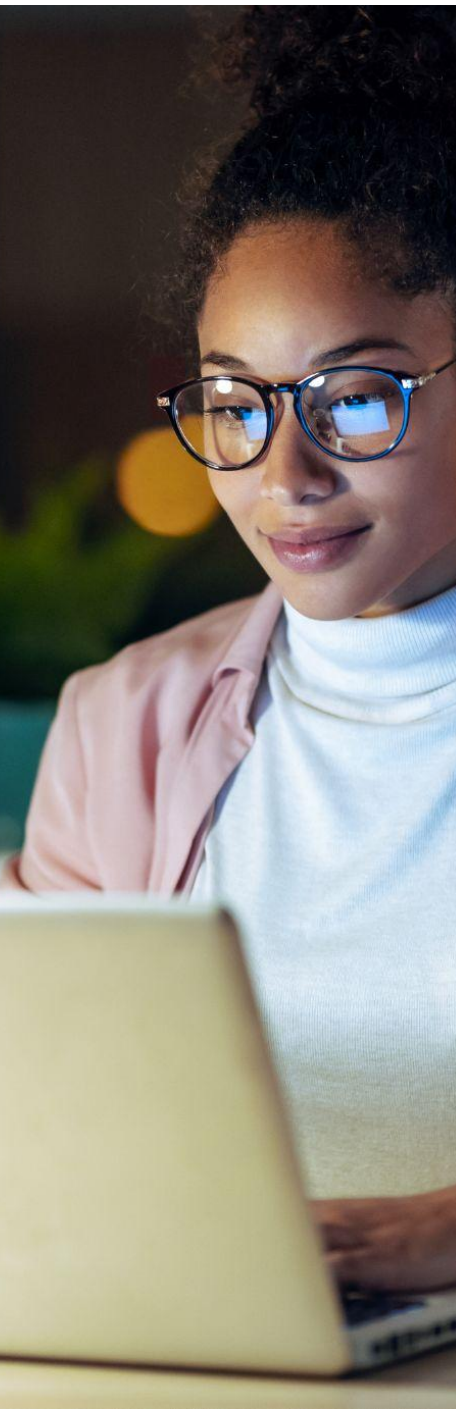
This course will focus on System Architecture, Operating System Architecture, System Exploits (hardware, operating system, and memory). We will also utilize tools, including Metasploit and command line tools in Linux (xxd, gdb, etc) for further analysis of exploits. We will explore exploits and their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

- Describe the System Architectures for Windows, Linux, Mac, and the mobile OSes (Android, IOS).
- Utilize Open Source tools to understand how modern exploits against those operating systems work and the countermeasures to prevent the exploits.
- Demonstrate basic coding and code analysis in PYTand C, and how basic exploits can be written.
- Describe advanced exploits and their countermeasures.

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



Cyber Threat Intelligence

This course helps students gain an appreciation of how to conduct strategic and operational planning, threat intelligence, and analysis in support of cybersecurity. This course will focus on the analytical and planning skills required to conduct effective Cyber Threat Intelligence. The course introduces larger concepts related to how cyberspace has become a new warfighting arena that targets private and public critical infrastructure, economic, and national security targets across all sectors globally.

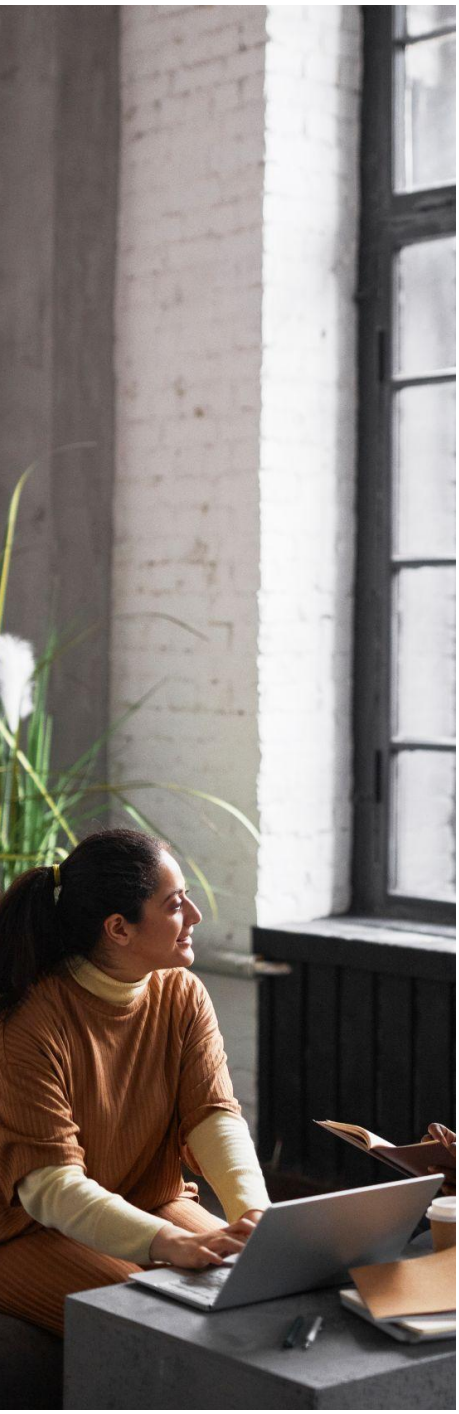
Students must understand the overall threat environment, how to discern the "so what" of information, and analyze complex human-influenced cyber problems and threats to public and private information enterprises. Students will develop performance-based skills to effectively understand, analyze, and communicate with a wide variety of audiences in public and private organizations. Students will study and practice analytical methodologies such as 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).

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

- Describe the role of strategic and operational planning in support of the cybersecurity missions and information security. Identify the role of cyber threat intelligence in supporting those processes.
- Explain the sources and methods for cyber threat intelligence collection and analysis.
- Demonstrate the process and uses of analytical tools such as Cyber Kill Chain and the Diamond Model.
- Perform the phases of Cyber Mission Analysis (CMA) and Intelligence Preparation of the Environment (IPE).

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



Governance, Risk Management, and Compliance

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 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 have not yet achieved and to establish efficient, effective, and elegant Information Security Programs.

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

- Apply the relevant GRC theoretical and practical knowledge behind various frameworks.
- Practice critical thinking to construct and evaluate information and cyber security claims and arguments with positive outcomes.
- Apply the relevant GRC theoretical and practical knowledge to technology used in business organizations.

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

Logs and Detection

This course will focus on engineering solutions to allow analyzing the logs in various network devices, including workstations, servers, routers, and firewalls. We will explore the information stored in logs and how to capture this data for analysis with a Security Information and Event Manager (SIEM). We will also 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.

Tools Learned:

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

Python

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

The first part of this course 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, modifying that code to add additional functionality, and writing simple algorithms.

In the second half of this course, we will dive deeper into topics including more advanced algorithms and Object Oriented Programming. Secure coding techniques and methodologies, including standard frameworks, will also be covered.

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:

- Research the history of Python and why it is used in cybersecurity.
- Compare and contrast interpreted and compiled languages.
- Create basic flowcharts and pseudocode for common algorithms.
- Script simple python code, including loops and data flows.
- Utilize packages and modules to increase the functionality of Python code.

Tools Learned:

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

Application Security and Penetration Testing

This 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.

Application Security focuses on the applications, and their vulnerabilities, running on both workstations and servers. Penetration testing uses vulnerabilities in applications or network resources that allow for exploitation. Exploitation can lead to server downtime, service interruptions, or, in the worst case, root level access for the malicious actor.

The first part of this course 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, testing the vulnerabilities, and basic approaches to exploiting these vulnerabilities. Additionally, network mapping will be revisited and specific techniques for reconnaissance will be discussed.

In the second half of this course, we will look at specific exploits and how they can be utilized to more efficiently target and manipulate 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**:**

- Explain and exhibit the usage of Metasploit and other Kali Linux pentesting tools.
- Become familiar with and rehearse using 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.

Tools Learned:

- PENETRATION TESTING EXECUTION STANDARD (PTES) FRAMEWORK
- METASPLOIT
- OPENVAS
- NMAP
- SHELLCODE GENERATION
- FUZZING
- ROOTKITS
- BURP SUITE

Applied Cryptography

This course teaches students the components of cryptography, provides hands-on experience 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 the first part of this course, students will be introduced to basic principles of encryption and authentication. Additionally, students will review and analyze historical approaches to cryptography. Students will practice symmetric cryptography, namely block ciphers, hash functions, and message authentication Codes.

The second half of this course 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. Finally, we will cover anonymity and exploits using cryptography. Students will explore weaknesses in WEP and SSL that lead to vulnerabilities and will discover how to counter them.

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

- Explain the fundamental goals of cryptography and its essentialness to cybersecurity best practices.
- Implement common crypto software to ensure secure communication and storage of data.
- Apply cryptographic best practices and analyze to assess the vulnerability of applications.
- Create tools to attack and fix applications in a virtual lab environment.
- By the course conclusion, students will have covered all relevant parts of the cryptography section of the industry-standard CISSP certification program.

Tools Learned:

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

Capstone

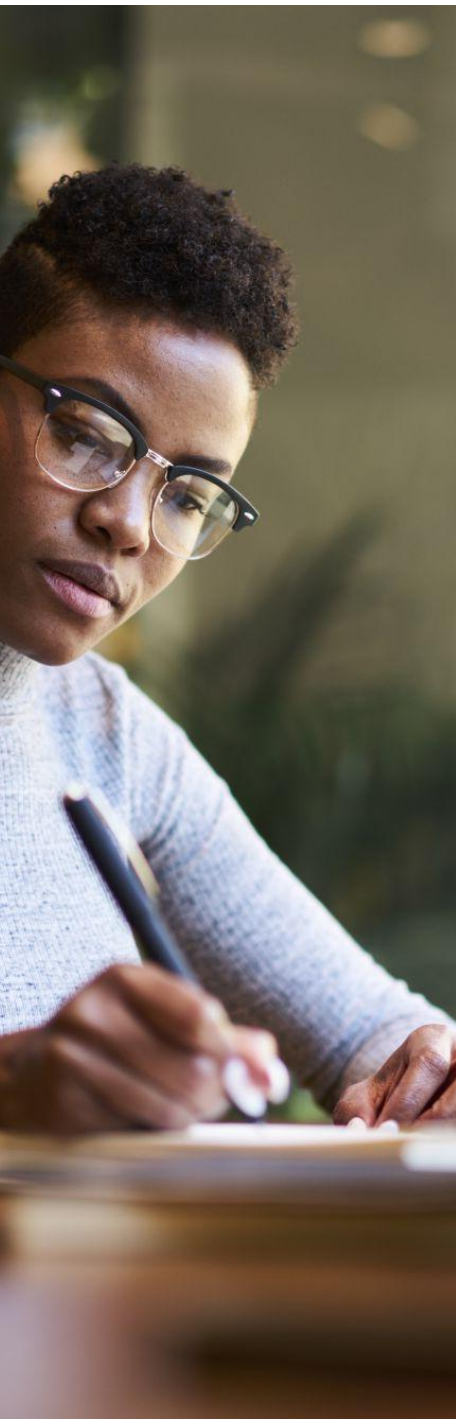
This course will focus on a final scenario-based capstone project summarizing learning from all parts of the Cybersecurity Engineering curriculum. Specifically, this will require detailed analysis of data, simulated and live action scenarios, installation, and configuration of components or applications and other activities. 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 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.

Tools Learned:

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



Program Pace & Schedule

At Flatiron School, we know that how you choose to study is as integral to your success as what you're learning. With our online learning platform, Canvas, and individualized support, all students have access to a personalized learning experience. Choose from 3 different pace options to fit your unique schedule.

Pace Options	20, 40, or 60 weeks
Time Commitment	Flexible depending on chosen pace
	Change the pace at any point to fit the unique needs of your schedule.
Career Services Support	Yes
Technical Coach	Yes
Educational Coaching	Yes
Lectures	Recorded lectures at your pace. Live lectures if/when available.
Assigned Cohort	No

Why Flatiron School?

Named One of the Best Coding Bootcamps for Q1 2020 by Career Karma

Ranked One of the Top Coding Bootcamps by Course Report

Practical hands-on learning

Get job-ready with practical, hands-on learning. You'll learn in-demand market languages and skills, labs, and real-world portfolio development.

Technical mentorship

Schedule 1:1s with your instructor to work on technical concepts, plan out your pacing or check in about your program milestones.

Learn in community

You may be learning online, but you're not alone. You'll be included in a number of specialized Slack channels that will build your online community and guide you to any instructional help you may need.

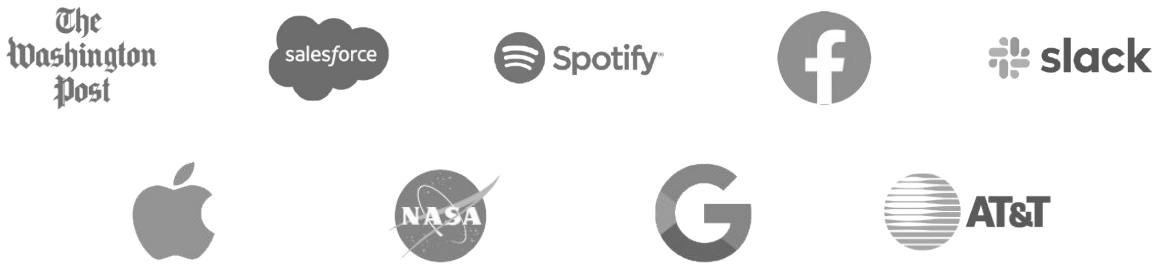
Campus Experience

If you're near one of our campuses, pop in to meet up for a study group with other students. Learn more about our campus experience and upcoming events you can join.

1:1 Career Coaching Support

You'll be paired with an individual career coach for 180 days after program completion.

Where our grads get hired



Let’s stay in touch.

Education should be the best investment you make in your future—and at Flatiron School, we’re committed to helping you learn the skills to change your future. Online and on our campuses across the country, we provide the skills, community, and immersive, outcomes-driven curriculum you need to launch a career in software engineering, data science, cybersecurity, or 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 workshop 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

This Syllabus includes summary descriptions and other information related to this Flatiron School program. For a detailed description, please consult the current Flatiron School student catalog, available at https://www.flatironschool.com/regulatory-information, and the enrollment agreement you sign in connection with your program.