FLATIRON SCHOOL

Online
Cybersecurity Analytics

Table of Contents

// FLATIRON SCHOOL

Overview

Learn how to stop hackers!

You are living at an unprecedented inflection point 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 enable the future potential of technology itself.

Flatiron School's Online Cybersecurity Analytics program, Full-time or Part-time Options

The Cybersecurity Analytics program is your path to an analytical cybersecurity career. Whether you enroll in the online full-time or part-time paths, this curriculum includes **eight (8) foundational courses** that deep-dive on concepts related to threat intelligence, data visualization, and log analysis, as well as threat hunting. This program is highly analytical in nature. A natural interest in research and problem solving is recommended. The move from an IT to a technical cybersecurity position usually takes five to ten years. Our online Cybersecurity Analytics program will help you be career-ready in three months.

The **30 hours of optional online pre-work** will give you a foundation in Systems, Networking and Python that you need to be successful before starting in the Cybersecurity Analytics program.

// FLATIRON SCHOOL

Overview

Learn how to stop hackers!

You are living at an unprecedented inflection point 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 enable the future potential of technology itself.

Flatiron School's Online Cybersecurity Analytics program, Full-time or Part-time Options

The Cybersecurity Analytics program is your path to an analytical cybersecurity career. Whether you enroll in the online full-time or part-time paths, this curriculum includes **eight (8) foundational courses** that deep-dive on concepts related to threat intelligence, data visualization, and log analysis, as well as threat hunting. This program is highly analytical in nature. A natural interest in research and problem solving is recommended. The move from an IT to a technical cybersecurity position usually takes five to ten years. Our online Cybersecurity Analytics program will help you be career-ready in three months.

The **30 hours of optional online pre-work** will give you a foundation in Systems, Networking and Python that you need to be successful before starting in the Cybersecurity Analytics program.

Cybersecurity Analytics

At Flatiron School, our Cybersecurity Analytics curriculum will prepare you to handle rapidly-advancing threats. Learn to set traps and catch threat actors, through real-world lab environments paired with industry-grade curriculum. You will learn the analytical skills needed to stand out from the competition. The Cybersecurity Analytics program includes eight (8) foundational courses designed to prepare you for success in the cybersecurity industry.

Network Administration
You'll be exposed to network security, protocols, and attacks, which are foundational concepts to cyber careers.

System Administration
Foundational to a cyber career, you will learn basic skills in system security, desktop OSes, and service configuration.

Strategy and Analysis
You will learn to anticipate threat actors through the psychology of analysis, criminal psychology, and threat intelligence.

GRC (Governance, Risk and Compliance)
You will learn to engage the enterprise, gain a management level perspective of cybersecurity within the organization, and develop plans and policies.

Security Intelligence and Event Management Administration
This course spans the course and will teach security monitoring, threat ID & response, and crisis management.

Hunt Skills
Learn to effectively work with teams and tools while learning threat ID, surveillance, data, and tracking.

Threat Intelligence
We will teach you how to create and consume threat intelligence which is absolutely core to an analytics career.

Capstone
Through a culminating capstone project, you will demonstrate applied knowledge from all of the above Cybersecurity Analytics courses.

// FLATIRON SCHOOL

Cybersecurity Analytics: An In-Depth Look

Network Administration

This course will focus on core ideas in network security. The first portion will review basic network protocols: Ethernet, 802.11 (wifi), IP, UDP, TCP, ARP, DHCP, DNS, ICMP, BGP, SMTP, POP/IMAP, FTP, HTTP, IGMP, etc. Then, the course introduces 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. We then cover wireless protocols and their security. After completing this course, a student will have far more than is needed to pass the Communication and Network Security section of the industry-standard CISSP certification program.

At the end of this course, students will be able to:
- Explain network security protocols and their vulnerabilities
- Use attack tools to mount attacks against various types of networks.
- 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
- Understand how to combat all of these attacks

System Administration

This course will focus on core ideas in system security. The first portion will review the three central desktop OSes: Windows, OS X, and Linux, along with the two preeminent mobile OSes: Android and iOS. The course will cover basic configuration of standard services and what happens when this is not done correctly. Students will study Windows Security, then Linux Security.

At the end of this course, students will be able to:
- Explain the basics of Windows, OS X, and Linux as well as Android and iOS
- Correctly configure well-known services (eg, a Web Server) without leaving security holes
- 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 c ompromised machine
- Understand how to combat all of these attacks as well

// FLATIRON SCHOOL

Strategy & Analysis

Strategy is an art and a science that has developed over centuries and is particularly poignant to today's cybersecurity professional. This course will focus on developing the student into a cybersecurity analyst with a broader, and more effective understanding of activity in cyberspace. The modern strategist must build upon the tested theory of classic strategists, while applying that knowledge in an environment that is constantly changing using technology and tactics that are continually developing. The intended result is the ability to assess data, organize resources, and refine capabilities in order to execute the mission of cybersecurity with the greatest effectiveness and efficiency.

At the end of this course students will be able to:
- Apply concepts of strategy to both cybersecurity operations and analysis of adversaries in order to more effectively navigate and succeed in the cyber environment
- Be familiar with and practiced in the collection and analysis of data and the application of that information to organize and guide cybersecurity operations
- To understand and apply strategy and analysis in a deliberate planning environment

GRC (Governance, Risk 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 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 Program.

On engaging all functional levels within the enterprise to deliver information system security:
- Plans and policies
- Enterprise roles
- Security metrics
- Risk management
- Standards and regulations
- Physical security
- Business continuity

// FLATIRON SCHOOL

SIEM Administration

This course will teach security monitoring, threat ID & response, and crisis management. This course will instruct students on computer information systems security monitoring, intrusion detection, and crisis management. It includes topics such as, alarm management, signature configuration, sensor configuration, and troubleshooting components. It also emphasizes identifying, resolving, and documenting network crises and activating the response team.

At the end of this course students will be able to:
- Run reconnaissance on a network and discover what updates and patches might be exploitable
- Correct vulnerabilities on the network and run detection software to determine when intrusions have taken place.
- Mitigate damage once an intrusions has taken place, how to report it and how to use forensics to determine the scale and scope of the breach and possible attacker identity.

Hunt Skills

This course will focus on core ideas in hunt skills for analysts. The first portion will review basic analytical techniques and introductions to basic hunt skills. The second portion will focus on passive hunt techniques such as deception grids and lures. The final portion will focus on active hunting techniques using visualization and active network probing and management. After completing this course, a student will have far more than is needed to pass the CSA+ certification program.

A deeper look into hunt team methods and tools
- Threat identification and hunting
- Multivariate correlation
- Surveillance in use cases
- Introduction to Data Visualization
- Introduction to Machine Learning
- Big data analysis
- Tracking adversaries
- Active Defense
- Incident Response

// FLATIRON SCHOOL

Threat Intelligence

This 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. 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 course will culminate with students presenting their Mission Analysis Brief to the instructor as if they are the CISO.

At the end of this course you'll be able to:
- Understand the major threat actors operating in cyberspace to include their methods of operating, motivations, and capabilities, then apply these to determine how a threat could potentially attack.
- Utilize structured analytical techniques to develop situational understanding and conduct effective threat intelligence.
- Conduct Cyber Intelligence Preparation of the Environment to develop detailed understanding of the threat environment and determine threat courses of action.
- Conduct Cyber Mission Analysis to provide leadership with accurate information to drive effective decision-making.

Capstone

Through a culminating capstone project, you will demonstrate applied knowledge from all of the Cybersecurity Analytics courses.

// FLATIRON SCHOOL

What makes a Cybersecurity Analyst?

Flatiron School students get jobs — period. As a graduate of our Online Cybersecurity Analytics program, job-seek with the support of our Career Services team. From weekly 1:1 career coaching sessions, to mock interviews, to employer evangelism, our seasoned Career Services team is dedicated to helping our students launch lifelong careers within 6 months of their job-seeking start date, or we'll refund your tuition (see eligibility terms).

CAREERS IN CYBERSECURITY

SOC Analyst
Be responsible for defensive cyber counter infiltration operations against Advanced Persistent Threats (APT).

Compliance Analyst/Auditor
Track and analyze metrics to suggest steps for improving alignment with cybersecurity policies and regulations.

Threat Intel Analyst
Lead/perform the delivery of data protection engagements including discovery and classification.
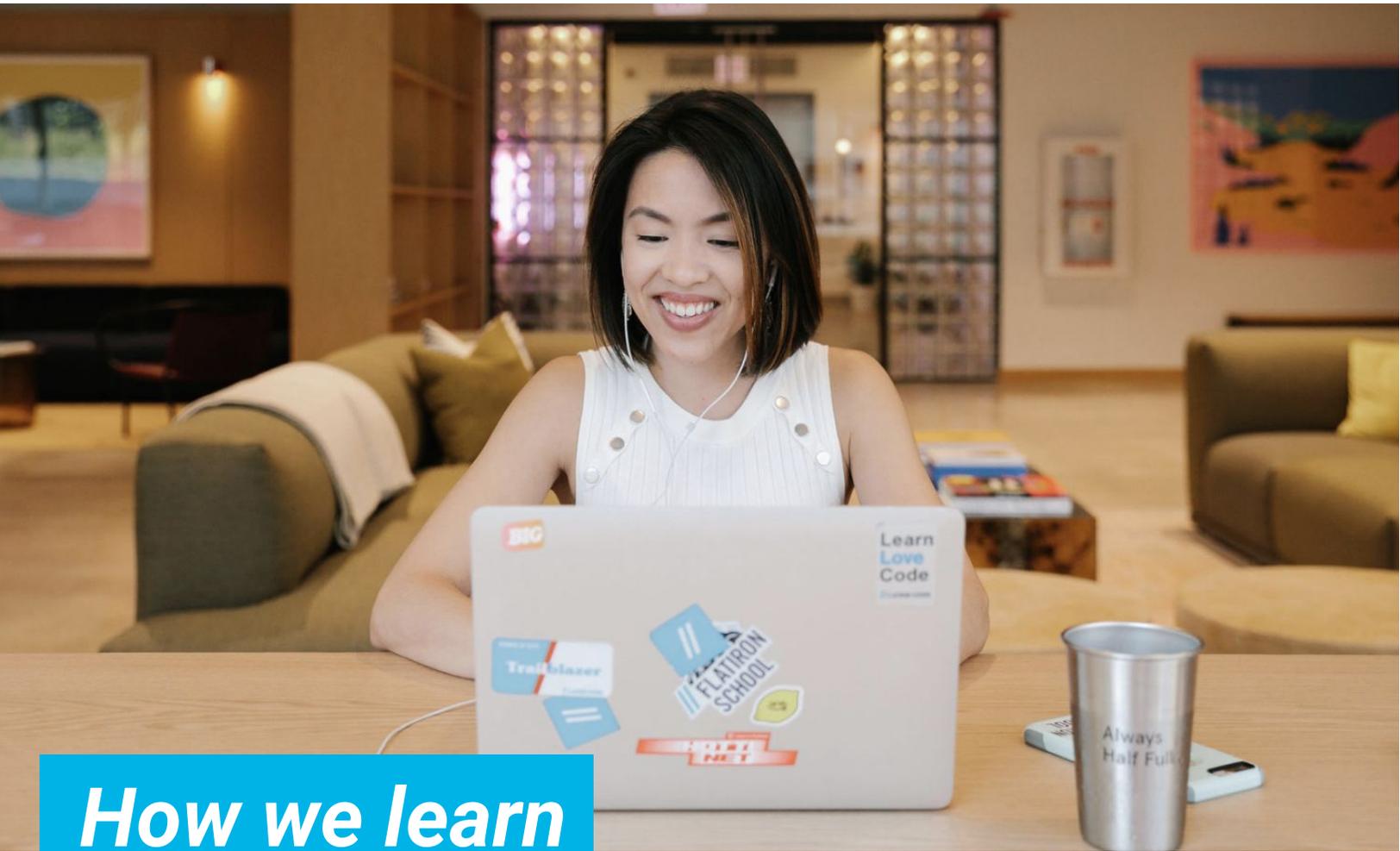
// FLATIRON SCHOOL

How we learn

50/50 Educational Approach
Flatiron School's Online Cybersecurity Analytics program is taught by industry veterans. Unlike traditional educational methods, 50% of these programs are reserved for hands-on lab time. This approach allows you to start your cyber-career in months instead of years.

Online, but Not Alone
You'll collaborate with fellow online students and teachers, join live study groups, pair and chat with your peers, and access a living course that features thousands of updates a year to reflect current industry trends.

Cyber Range
Learn to set traps and catch threat actors, through real-world lab environments using our state-of-the-art Cyber Range, a sandbox where you can safely explore, track, gather, break, and build things.

WeWork Membership
With Online Cybersecurity Analytics, connect in-person with other online learners in your city and work together in a collaborative, supportive workspace with a one-year WeWork hot desk membership included with your tuition.

/// FLATIRON SCHOOL

Online, full-time or part-time

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 and individualized support from our educational team, all students have access to a personalized learning experience. Choose from two different program options, each tailored to today's online learner.

	FULL-TIME	PART-TIME
Length	4 months *16 weeks*	8 months *32 weeks*
Time Commitment	30 - 40 hr/week	15 - 20 hr/week
Admissions	Admissions + Technical Interview	Admissions + Technical Interview
Career Services Support	YES	YES
480 Curriculum Hours	YES	YES
Slack & Community Support	YES	YES
Educational Coaching	YES	YES
Live Lectures	YES	YES
Assigned Cohort	YES	YES
Technical Mentorship	2:1 1 hr/week	4:1 1 hr/week
WeWork Hot Desk Membership	YES	YES
Money-back Guarantee	YES	YES

Both course pace options include career services support, a [Money-Back Guarantee](#), and provide the same level of rigorous curriculum designed to make you a well-rounded cybersecurity professional no matter when you graduate.

// FLATIRON SCHOOL

Contact Us

For more information, please check out our website at
www.flatironschool.com or contact us at
admissions@flatironschool.com

// FLATIRON SCHOOL