SYLLABUS

Amazon Career Choice Cybersecurity Analytics

// FLATIRON SCHOOL

amazon | career choice

Last Updated 9/29/2023

Table of Contents

Overview

You are living at an unprecedented inflection point 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.

Amazon Career Choice: Cybersecurity Analytics

The Cybersecurity Analytics course is your path to an analytical cybersecurity career. This curriculum includes five foundational courses that deep-dive on concepts related to threat intelligence, data visualization, and log analysis. This program is highly analytical in nature. A natural interest in research and problem solving is recommended. The Amazon Cybersecurity Analytics program will help you be career-ready in 29 weeks, plus provide career coaching support to help you launch your new career outside of Amazon.

Career Services

As part of Amazon Career Choice, this course is designed to prepare students for careers in cybersecurity outside of Amazon. Graduates of this program will be equipped for a wide range of jobs across the cybersecurity industry. Sample alumni job titles include:

- Compliance Analyst
- Tier 1 SOC Analyst
- Network/Systems Analyst

During the job search, graduates will have access to a Career Coach. Coaches help with everything from résumé review to interview prep, and help you tell your story to land your first job. With Flatiron School's tried-and-true job search framework, graduates gain the skills and support they need to launch new careers.

Getting Started

Flatiron School is here to support you every step of the way, from application all the way through graduation (and beyond).

APPLICATION PROCESS

APPLY	Apply at flatironschool.com/amazoncareerchoice. Eligible applicants will have a high school diploma, GED, or equivalent; be located in the United States; be a full-time or part-time Blue Badge employee who will have completed at least 90 days of continuous employment prior to June 3, 2024; be interested in pursuing a new career in tech upon successful completion of the course.
ADMISSIONS ASSESSMENT	Complete an admissions assessment. This will only take you 15 minutes and is a measure of cognitive aptitude - don't worry, no studying or technical skills required!
BEGIN PREWORK	Prework is ~20-40 hours of basic curriculum that you must complete before enrolling in the course. You'll receive login credentials and further information on how to get started.
ADMISSIONS INTERVIEW	After you complete 70% of your Prework, you can schedule a 15-minute phone chat with our team. There's nothing you need to prepare – this is a chance for you to ask questions and for us to get to know you!
SUBMIT TUITION VOUCHER	Once you successfully pass the admissions interview, Flatiron School will send you a payment code. Log into your Career Choice portal to submit the code for the program.
ENROLLMENT AGREEMENT	Sign your enrollment agreement prior to starting the program.
START CLASS!	Your first day of class is February 5, 2024. Class will run through August 30, 2024. Classes include two-hour live virtual workshops, which will be hosted on Mondays, Wednesdays, and Fridays. Students will have access to all recordings.

The power of learning **Cybersecurity**

WHY DO WE TEACH DEFENSIVE AND OFFENSIVE SECURITY?

Defensive

Cybersecurity is about doing the fundamental tasks well to help protect critical data and services across the organization.

This course was designed to build fundamental IT and cybersecurity skills to help you protect your organization and help you grow your cybersecurity career.

The skills learned in this program can help lay the foundation for a variety of Cybersecurity job roles that you might explore throughout your career.

Offensive Security

New threats to your organization emerge daily. By learning how a threat actor thinks and the tactics, techniques, and procedures they use, you can build a better defensive security posture across your organization.

Career Flexibility

Learning Cybersecurity is a lifelong endeavor. Learning both the defensive side and offensive (hacker) sides of Cybersecurity prepares you for the essential task of helping organizations become more secure and develops your skills for self-learning throughout your career as new threats and technologies appear.

Curriculum Overview

GETTING STARTED

Before starting the Amazon Cybersecurity Analytics course, students must complete an initial assessment. Once enrolled in the course, students will begin their cybersecurity journey in the pre-work course and learn the foundational skills needed for rewarding careers in the tech industry.

MASTERY-BASED PROGRESS

Our program is broken into curriculum modules. Each module concludes with a comprehensive project meant to bring together students' competencies and demonstrate them in their portfolios. Students work in teams and directly with instructors to ensure they've mastered key concepts before progressing. If students need additional support, they receive additional direct mentorship. Our instructors' goal is to equip students to be successful at every stage of the course.

LIFELONG LEARNING

With guidance from their Career Coach, students will continue to build their technical skills after graduation as they embark upon their Cybersecurity job search.

Amazon Cybersecurity Analytics

Our Cybersecurity Analytics curriculum will prepare you to handle rapidly-advancing threats. This program is designed to help you develop the skills you need for a career as a tier 1+ SOC analyst, threat intel analyst, and compliance analyst. Passionate people with strong critical thinking, research, and analytical skills, are a good fit for this program. Students will complete 5 different courses in the areas shown below:

System Administration

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

Network Administration

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

Security Intelligence and Event Management Administration

This module spans the course and will teach security monitoring, threat ID & response, and crisis management.

Cyber Threat Intelligence

Learn strategy, sources of threat intelligence and leverage Maltego for gathering intel.

GRC (Governance, Risk, and Compliance)

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

Course Schedule: An In-Depth Look

Instructional Calendar | Cybersecurity Analytics			
	Date of Instructional Week	**Courses**	**Objectives**
Week 1	June 10 - June 14	**Network Administration** **System Administration**	- Overview of computer networking - Build knowledge of networking models - Build knowledge of encoding and binary to hexadecimal conversion - Build knowledge of the OSI and TCP/IP models - Build knowledge of virtualization
Week 2	June 17 - June 21	**Network Administration** **System Administration**	- Build knowledge of Wireshark - Build deeper knowledge of OSI layers 1 and 2 - Build a network diagram - Build knowledge of the Linux OS
Week 3	June 24 - June 28	**Network Administration** **System Administration**	- Build knowledge of IP addressing (IPv6 and IPv6) and subnetting - Build deeper knowledge of OSI layers 3 and 4 - Build knowledge of NAT - Build knowledge of identity and access management in Linux - Build knowledge of file systems and volumes
Week 4	July 1 - July 5	**Network Administration** **System Administration**	- Leverage Wireshark to analyze network traffic - Build knowledge of bash scripting - Build knowledge of Extended Attributes
Week 5	July 8 - July 12	**Network Administration** **System Administration**	- Build knowledge of routing and routing devices - Build knowledge of firewalls - Build knowledge of Windows OS
Week 6	July 15 - July 19	**Network Administration** **System Administration**	- Build knowledge of Windows Registry - Build knowledge of PowerShell - Configure a pfSense firewall - Configure a VyOS router
Week 7	July 22 - July 26	**Network Administration** **System Administration**	- Build knowledge of VPNs - Build knowledge of DNS - Build knowledge of Windows system administration - Build knowledge of LDAP
Week 8	July 29 - August 2	**Network Administration** **System Administration**	- Build knowledge of IDS and IPS - Set up and configure intrusion detection with Snort - Build knowledge of port mirroring, sniffing, and forwarding - Build knowledge of Windows Active Directory

Course Schedule: An In-Depth Look

Instructional Calendar | Cybersecurity Analytics			
	Date of Instructional Week	**Courses**	**Objectives**
Week 9	August 5 - August 9	**Network Administration** **System Administration** **Governance, Risk, Compliance**	- Build knowledge of Web servers and applications - Build knowledge of LAMP - Build knowledge of directory traversal - Overview of GRC
Week 10	August 12 - August 16	**Network Administration** **System Administration** **Governance, Risk, Compliance**	- Build knowledge of HTML - Build knowledge of bash scripting and Cron jobs - Build knowledge of GRC standards and best practices
Week 11	August 19 - August 23	**Network Administration** **System Administration** **Governance, Risk, Compliance**	- Build knowledge of server hardening - Build knowledge of databases (SQL, MySQL) - Build knowledge of Race conditions - Build knowledge of privacy and GDPR
Week 12	August 26 - August 30	**Network Administration** **System Administration** **Governance, Risk, Compliance**	- Configure an Apache Web server - Compile software code - Build knowledge of asset management - Build knowledge of enterprise architecture and change management
Week 13	Sept 2 - Sept 6	**Network Administration** **System Administration** **Governance, Risk, Compliance**	- Build knowledge of APIs - Build knowledge of secure coding - Build knowledge of business continuity planning (BCP)
Week 14	Sept 9 - Sept 13	**Security Information and Event Management Administration** **Cyber Threat Intelligence**	- Overview of SIEM tools - Build knowledge of SIEM logs - Build knowledge of SIEM architecture - Overview of security strategy
Week 15	Sept 16 - Sept 20	**Security Information and Event Management Administration** **Cyber Threat Intelligence**	- Install and configure ELK - Build knowledge of data normalization - Analyze SIEM logs - Introduction to threat intelligence
Week 16	Sept 23 - Sept 27	**Security Information and Event Management Administration** **Cyber Threat Intelligence**	- Build knowledge of regular expressions (RegEx) - Build regular expressions for data analysis - Install and configure Splunk - Introduction to the threat intelligence lifecycle

CURRICULUM OVERVIEW

Course Schedule: An In-Depth Look

Instructional Calendar | Cybersecurity Analytics			
	Date of Instructional Week	**Courses**	**Objectives**
Week 17	Sept 30 - Oct 4	**Security Information and Event Management Administration** **Cyber Threat Intelligence**	- SIEM + CTI Assessments
Week 18	Oct 7 - Oct 11	**Security Information and Event Management Administration** **Cyber Threat Intelligence**	- Build deeper knowledge of SIEM architecture - Analyze data with Splunk - Build knowledge of data indexing, storage, and processing - Introduction to targeting
Week 19	Oct 14 - Oct 18	**Security Information and Event Management Administration** **Cyber Threat Intelligence**	- Build knowledge of data visualization - Configure a SIEM dashboard - Build knowledge of SIEM reporting
Week 20	Oct 21 - Oct 25	**Security Information and Event Management Administration** **Cyber Threat Intelligence**	- Build knowledge of SIEM alerts and compliance - Configure alerting with Splunk - Overview of Diamond Model
Week 21	Oct 28 - Nov 1	**Security Information and Event Management Administration** **Cyber Threat Intelligence**	- Build knowledge of notifications, including severity, automation, and remediation - Build knowledge of user and process monitoring - Build knowledge of best practices for processing logs
Week 22	Nov 4 - Nov 8	**Security Information and Event Management Administration**	- Build knowledge of event correlation - Build knowledge of AI and machine learning for log analysis
Break	**Nov 11 - Jan 17, 2025**	**Break for Amazon Peak Season**	**Break for Amazon Peak Season**
Week 23	Jan 20 - Jan 24, 2025	**Security Information and Event Management Administration**	- Build knowledge of automation using SIEM tools - Build deeper knowledge of fine tuning a SIEM tool
Week 24	Jan 27 - Jan 31, 2025	**Security Information and Event Management Administration**	- Build knowledge of using a SIEM to detect indicators of compromise (IOCs)
Week 25	Feb 3 - Feb 7, 2025	**Security Information and Event Management Administration**	- Build knowledge of advanced SIEM configurations

CURRICULUM OVERVIEW

Course Schedule: An In-Depth Look

Instructional Calendar | Cybersecurity Analytics			
	Date of Instructional Week	**Courses**	**Objectives**
Week 26	Feb 10 - Feb 14, 2025	**Governance, Risk, Compliance**	- Build knowledge of risk assessments - Build knowledge of risk management
Week 27	Feb 17 - Feb 21, 2025	**Governance, Risk, Compliance**	- Build knowledge of risk management frameworks
Week 28	Feb 24 - Feb 28, 2025	**Governance, Risk, Compliance**	- Build knowledge of risk treatment methods and security controls
Week 29	March 3 - March 7, 2025	**Governance, Risk, Compliance**	- GRC Final Assessment
Week 30	**March 14, 2025**	**Graduation**	

Career Services			
	Date of Instructional Week	**Courses**	**Objectives**
	March 17 - Sept 13, 2025	**180 Days of dedicated 1:1 Career Services**	- Job Search Strategy, Networking Tips, Resume Reviews, Interview Prep Support, Negotiating Job Offers

What makes a Cybersecurity Analyst?

Everything you learn in the Amazon Cybersecurity Analytics course is designed to prepare you for a new career in cybersecurity outside of Amazon. During your job search, you'll meet regularly with a Career Coach. Coaches help with everything from résumé review to interview prep, and help you tell your story to land your first job.

Through 1-on-1 guidance from our Career Coaching team and our tried-and-true job-search framework, you'll gain the skills and support you need to launch your career.

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.

How We Learn

Test-Driven Learning

We believe the best way to learn how to defend an organization is to put your hands on the keyboard during training. That's why our course blends instruction with hands-on labs that help you deliver to an organization on day one.

Open Curriculum

Our industry-tested curriculum has given over 1,500 Flatiron School graduates the skills to become Cybersecurity Analysts and thrive in their careers. We continually improve our coursework in reaction to feedback and real-world changes, and our edits are supplemented by hundreds of student submissions each month.

Use Real Tools

You can't learn real skills without real tools. We leverage industry tools, like Splunk to help you learn how to defend an organization from attackers.

Contact Us

For more information, please check out our website at **flatironschool.com/amazoncareerchoice** or contact us here.

t