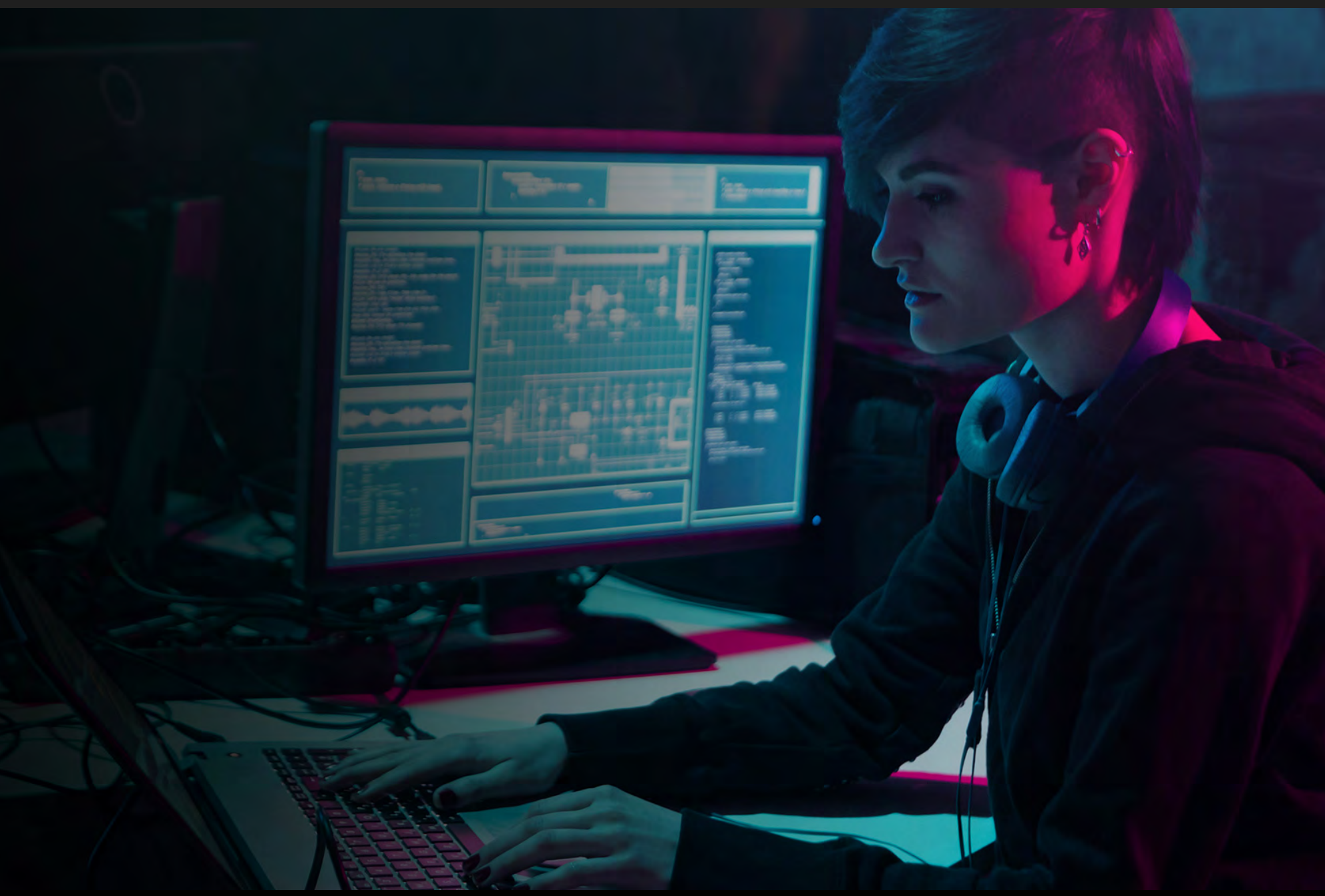
CODING DOJO | PART OF COLORADO TECHNICAL UNIVERSITY

Course Packet

Cybersecurity

Part-Time Online

24 weeks, 25 hours/week



Part-Time
class commitment

Career Services
Included

Learn by Doing
50-75% Lab Work

Join the 13,000+ global alumni who kickstarted their career paths in tech.

Program Overview

The importance of cybersecurity today cannot be overstated. As our reliance on technology grows, there's a corresponding need to secure and defend networks and data against leaks, theft, and attacks. That's good news for cybersecurity specialists— the U.S. Bureau of Labor Statistics projects cybersecurity jobs will grow 31% through 2029. In short, there's job security in cybersecurity.

Top Industry Certifications. Learn skills applicable to certifications such as the Network+, Linux+, Server+, Cloud+, and certified Ethical Hacker (CEH)., and receive vouchers for CompTIA Security+ and CySA+.

Learn By Doing. Gain hands-on experience with a host of popular tools such as Wireshark, Kali Linux, Metasploit, and more through real-world hands-on lab assignments.

Cyber-Specific Career Services. Receive personalized career support from a dedicated cybersecurity career services manager, and keep your career service access for life.

End-to-End, Extensive Curriculum. Cover the latest real-world deployment of cybersecurity management practices, including defensive and offensive tactics, NIST Cybersecurity Framework, and event & incident management.

Up Next: The Curriculum Overview

The Curriculum Overview

Pre-Course

Before the program, set up your VM, organize your schedule, set your expectations, complete readings and assignments.

What You'll Focus On:

- Getting organized

Weeks One to Eight

Core Course

The first part of the program you'll get started on the basics.

What You'll Focus On:

-
- Command Line
- Kali Linux
- Vulnerabilities
- Powershell
- IOCs
- Frewalls

Weeks Nine to Sixteen

Intermediate Course

The second part of the program you'll progress to the intermediate course.

What You'll Focus On:

- SIFM
- Wireshark
- Nmap
- IAM
- Metasploit
- Cloud Security

Weeks Seventeen to Twenty-Four

Professional Course

The last part of the program you'll move to the professional course.

What You'll Focus On:

- Metasploitable 3
- Eternal Blue
- Ethical Hacking
- Pen Testing
- BurpSuite
- Malware

Up Next: The Whole Curriculum

The Whole Curriculum

Week One
Fundamentals
Dive right in with broad exposure to cybersecurity including: Controls, Frameworks, Benchmarks, Virtual Machines, Threats, Vulnerabilities, Defenses, Secure Software, Testing, and Cryptography.

Labs:
- Nessus Installation
- Network Scanning

Week Two
Attacks
Continuing the broad exposure adding more major cybersecurity elements.
Build out your Kali Linux machine while also learning about networking and data security.

Labs:
- Password Cracking

Week Three
Access Control & Security
Learn about network configurations and data security, including Network Design, Firewall Configuration, Access Control.

Labs:
- OpenSSL Certification
- Packet Sniffing
- Basic ACL

Week Four
Malware & Intrusion Detection
Viruses and Ransomware, intrusion detection, useful tools, introduction to embedded (control) systems, secure shell, mobile & endpoint security.

Labs:
- Firewall Configuration in Kali
- Secure Network Design

Week Five
Disaster Recovery
Learn more about Virtual Machines, malicious code, Disaster Recovery, and Powershell.

Labs:
- Snort Installation
- SSH

Week Six
Incident Response & Forensics
Identifying and responding to incidents, technical and legal elements of forensics

Labs:
- Endpoint Protection
- Malicious Code
- Powershell Security

Week Seven
Resiliency & Automation
Learn how resiliency, automation, and backups provide essential and fundamental protection

Labs:
- Tabletop Exercise
- Digital Forensics
- Backup Lab

Week Eight
Cyber Career Prep
Tabletop exercises are effective for learning, preparing, and solving problems before they happen.

Labs:
- Career Preparation
- Belt Exam Sec+

Week Nine
Threat Assessments
Understand roles and responsibilities, security controls, indicators of compromise, understanding threats, attack tools, monitoring networks.

Labs:
- IoC Investigation
- Network Group Assignment

Week Ten
Output Analysis
Protect networks, monitor and analyze various services for signs of compromise, run scripts, understand and use SIEM (Security Information and Event Management).

Labs:
- Wireshark Analysis
- Log Analysis
- Windows Security Logs

Week Eleven
Intermediate Forensics
Examining forensic tools and techniques, digging into indicators of compromise, understanding detection and containment, learning digital evidence collection, understanding frameworks, policies and procedures, exploring attacker lateral movement and pivoting.

Labs:
- Analyzing Email Headers
- SIEM Group Assignment

Week Twelve
Intermediate Incident Response
Review of the phases of IR for further in depth work, participate in extended lab exercise, as well as understand the critical importance of effective recovery.

Labs:
- Digital Evidence Collection
- IR Writing Assignment (2 day lab)

Week Thirteen
Risk Management
Understanding and managing risk is a key to security professional and program success; enumeration, credential security, and vulnerability assessment are key to effectiveness of security professionals and programs.

Labs:
- Risk Management
- Nmap Formatting

Week Fourteen
Vulnerability Scanning
Wireshark, Regulations, IAM, Network segmentation and other protections, Linux auditing, hardware assurance, specialized technologies

Labs:
- Another Wireshark
- Linux Audit

Week Fifteen
Share Permissions
Learn technical and non-technical controls, various related regulations, the relationship of security and privacy, how to configure and analyze share permissions, and mitigate attacks.

Labs:
- Configuring and Analyzing Share Permissions
- OWASP Top 10
- Web Assessment

Week Sixteen
Cloud Access
Learn cloud technologies and how to protect your cloud-based solutions.

Labs:
- Belt Exam CySA+

Week Seventeen
Reporting, Metasploit and Exploitation
Discuss the ethics of hacking while learning penetration testing, Metasploitable2 and Eternal Blue.

Labs:
- Metasploitable3
- Eternal Blue

Week Eighteen
Footprinting & Active Reconnaissance
Understanding the underlying capabilities of search engines, WHOIS, DNS, nmap, dirbuster and gobuster, nikto, social engineering, specialized scanners, SNB enumeration.

Labs:
- Footprinting Assignment
- Specialized Scanners

Week Nineteen
Enumeration & Exploiting the Web
Become proactive in your approach to cybersecurity by seeking threats.

Labs:
- SMB Enumeration
- Vulnerability Scanning 1 & 2
- BurpSuite Setup

Week Twenty
Web Pen Testing & Android Hacking
Learning Local File Inclusion and Remote File Inclusion, SQL injection techniques and defenses, hacking and testing mobile devices.

Labs:
- Local File Inclusion
- SQL Injection
- Mobile Pentesting

Week Twenty-One
Buffer Overflow & Advanced Malware Analysis
Learn to counter and create a buffer overflow attack on Windows/Linux.

Labs:
- Windows Buffer Overflow
- Buffer Overflow
- Malware Analysis

Week Twenty-Two
Transferring Files & Privilege Escalation
Add to your malware knowledge with advanced techniques and tools.

Labs:
- Linux Privesc
- Windows Privesc

Week Twenty-Three
Locating Exploits
Learn to elevate privilege to fully exploit the platform, monitor the network, or access other systems during an attack.

Labs:
- How Many Shells

Week Twenty-Four
Exploits & Password Attacks
Learn various sources for exploits and how to use them, the use of Shells, password attacks. With great power comes great responsibility!

Labs:
- Password Attacks

Career Services

Lifetime career services support. Our experienced Career Services team provides guidance, strategy, and prep to help you land a job whether it's post-graduation or later down the road in your search for senior roles.

1

Professional Profile & Portfolio Building

From day one, gain access to your Career Services Manager who will begin to guide you into creating your digital footprint, learning skills companies seek, and building a profile that communicates those points to the right recruiters. Milestones include:

- LinkedIn Profile Creation & Optimization
- Github Portfolio Production
- Resume Development & Curation

2

Job Prospecting & Application Guidance

While learning the most in-demand programs in tech, you'll be working on your job search for when graduation approaches. Your Career Services Manager will work with you on potential job titles to seek, understand different role descriptions, and guide you toward your long-term career goals. Milestones include:

- Real Job Search
- Sample Applications
- Hiring Manager Communication
- Job Title Refinement

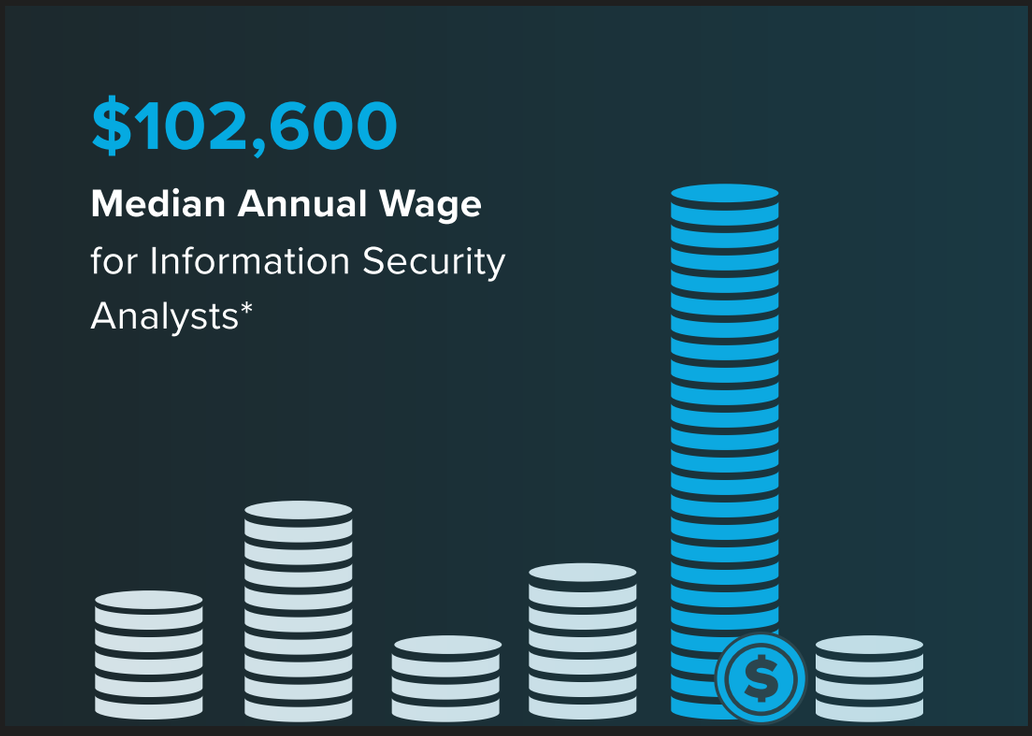
3

Interview Prep & Negotiation

One of the largest complaints by tech recruiters is it's easy to find people who can code, perform data analysis, and set up a Cybersecurity framework, but most of these people can't communicate or work in teams. Whether you're an introvert or a natural leader, our Career Services team will make sure you're equipped to show up as your best self in essential interviews and your day-to-day work. Milestones include:

- Mock Job Interviews
- Technical Job Skills Tests
- Target Compensation Management
- Contract Negotiation

Industry Trends

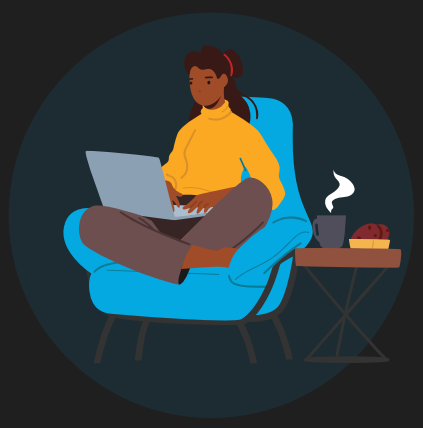


SOURCE: *Bureau of Labor Statistics, U.S. Department of Labor, Occupational Outlook Handbook, Information Security Analysts, at https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm (visited January 24, 2023). This data represents national figures and is not based on school-specific information. Conditions in your area may vary.

How to Enroll

Do Your Research

- Explore our programs on our website and view other program overviews.
- Schedule a call with one of our Admissions Advisors who will walk through your future career goals and what program would best suit you.
- Attend an Open House to meet directly with our Instruction and Career Service Managers.

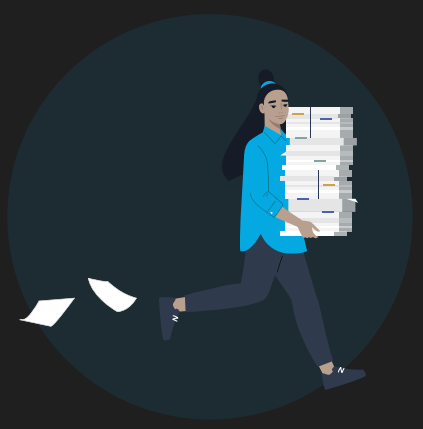


Submit Application

- Submit your application! The application process takes less than 5 minutes and has no technical assessment.
- Complete a quick 30-minute interview with our Admissions team.
- Receive your decision within 2-3 business days.

Get Financing

- Our Admissions Advisors will help you find the best financing dependent on your financial situation and your goals.
- Coding Dojo offers a variety of payment options, financing partners, and partial-scholarships.



Finalize Your Enrollment

- Submit your deposit, confirm your financing, and sign your Enrollment Agreement to reserve your seat in class!
- Your Admissions Advisor will introduce you to your Student Experience Manager who will help you get everything organized to start bootcamp.

Up Next: Financing Options

Financing Options

Installments

Spread tuition payments out over your program with customizable installment plans.

Third Party Financing

Finance your bootcamp with a third party loan from a variety of vendors or source your own.

Pay in Full

Pay your tuition in full and get started immediately.

Schedule a call with an Admissions Advisor to discuss which payment or financing option is right for you.

Chat with Admissions