

Cybersecurity Bootcamp

ASU Arizona State
University

Bootcamp Brochure



Contents page

Overview	1
The process	2
Code review in partnership with HyperionDev	3
Why choose cybersecurity as a career?	4
How we help you get hired	5
Potential career paths	6
Structure of the bootcamp	8
What to expect from the cybersecurity syllabus	9



Overview

As cyber threats continue to rise, so does the demand for skilled professionals to protect businesses and critical IT infrastructure. If the idea of ethical hacking—identifying system and network vulnerabilities to design defense mechanisms against cyberattacks—excites you, then this could be the career for you.

Cybersecurity, also known as information technology security, involves protecting electronic information by addressing risks and vulnerabilities. These risks

can include unauthorized access, use, disclosure, interception or destruction of data, which may involve sensitive information from businesses, organizations or individuals.

No prior coding experience is required for this bootcamp, as it is designed to help you progress from beginner to job-ready. Enrolling in this bootcamp will accelerate your path toward a rewarding career in cybersecurity.

Beyond cybersecurity

This bootcamp will guide you in developing the skills needed to think beyond traditional information security. You'll learn to evaluate and mitigate risks related to issues like poor access policies and common cyberattack techniques, including cross-site scripting, SQL injection and man-in-the-middle attacks. You'll also explore a wide range of essential cybersecurity tools and concepts, including PKI, ciphers, Bash scripting, Kali Linux, penetration testing and digital forensics.



The process

- 1** Log onto your personalized dashboard
- 2** Complete coding exercises online
- 3** Your Mentor reviews your work
- 4** Perfect your coding over 3-6 months
- 5** Receive a certificate of completion
- 6** Begin your new career in tech with our post-bootcamp support



Code review in partnership with HyperionDev

Bootcamp code reviewers and mentors are expertly trained to integrate code review into the learning experience. This on-demand approach helps participants become fluent in their chosen area of study faster.

Our one-on-one code review approach works

Code review helps you learn to code the right way by mastering the deeper aspects of software development that are essential for a career in tech. We help you build a strong foundation for a successful career in coding.

Why learning through code review is smarter

Don't make the same mistakes as computers

Automated code checking is like spell check for computer programs. But you can't write a world-class essay with just good spelling – you need the right tone, facts, grammar, and style. Only human-led code review can help you learn aspects of coding that are analogous to tone and style that will make you truly fluent as a developer – automated graders just can't help you learn this!

Be exposed to industry standards from day one

In the tech industry, developers have their work assessed through code review by senior developers. We are the only bootcamp that introduces this technique from day one, giving you a competitive edge in the job market.

Get unstuck with on- demand technical help

Our code reviewers help you debug your programs, ensuring you maintain steady progress and stay on track.

A unique, proven and personalized approach to code review

A safe space to learn and grow

Human-led code review fosters trust with your mentors and allows you to learn at your own pace. It provides a supportive environment to discuss challenges without fear of failure.

Join a community of career changers

Learn alongside a cohort of bootcamp participants who are also pursuing career fulfillment. Engage in online group tutorials, community chats and peer coaching.

Industry experts with expertise tailored to your goals

You'll work with experienced code reviewers and mentors who provide guidance through one-on-one calls and email support.

Why choose cybersecurity as a career?

The global cybersecurity industry is projected to reach \$193 billion by 2026 as technology continues to evolve. This growing field needs experts who can address emerging threats and vulnerabilities. A career in cybersecurity is both challenging and rewarding, offering high salaries and six-figure earning potential for those with experience and expertise. Rapid growth in the industry also provides opportunities for advancement. If you're looking for a career that is both dynamic and lucrative, cybersecurity may be the right choice for you.



How we help you get hired

We're with you every step of the way, and our support doesn't end when you graduate. Our career services are designed to help you stand out from the competition and get noticed by top employers.

Technical résumé and portfolio

Receive technical assistance in getting your résumé and tech portfolio industry-ready by applying accepted best-practice formats.

Interview preparation

Know what to expect when getting ready for that big interview with expert interview preparation guidance from professionals who have been where you are.

Bootcamp certificate

Walk away with a newly minted certificate as evidence of your skills and expertise in cybersecurity.

Join our hiring network

We work with select hiring partners and aim to help you prepare for and land your first tech job opportunity after completing your bootcamp.



Potential career paths

Penetration Tester

Penetration testers, also known as ethical hackers, simulate real-world cyberattacks to identify and address vulnerabilities in an organization's systems and applications. They use a variety of tools and techniques to attempt unauthorized access to systems and networks, then report their findings and provide recommendations to improve security.

The responsibilities of a penetration tester include:

- Identifying vulnerabilities and security issues before malicious hackers can exploit them.
- Recommending security solutions or improvements.
- Conducting security assessments.
- Testing applications, network devices and cloud infrastructure.
- Writing reports and presenting findings to clients and technical teams.
- Attempting to exploit existing systems and software to detect and correct weaknesses.

Digital Forensics Analyst

Digital forensics analysts collect, analyze and present digital evidence to support criminal investigations or legal proceedings. This may involve using programming skills to automate data collection and analysis or developing custom tools for specific tasks.

The responsibilities of a digital forensics analyst include:

- Investigating security incidents and reverse-engineering hacks and attacks.
- Conducting computer and mobile device forensics investigations.
- Analyzing evidence and preparing reports.
- Performing data analysis to ensure the relevance of retrieved content.
- Working independently on investigations while also collaborating on problem-solving.



Cybersecurity Analyst

Cybersecurity analysts protect an organization's networks and systems from cyber threats. This role may involve using programming skills to create custom tools and scripts for analyzing data from sources such as log files, network traffic and mobile devices.

The responsibilities of a cybersecurity analyst include:

- Monitoring security procedures and ensuring best practices are followed.
- Using various tools and techniques to defend networks and systems from attacks.
- Continuously testing company networks to identify weaknesses before they can be exploited.
- Responding to security incidents.
- Writing reports and recommending security enhancements.

Cybercrime Investigator

Cybercrime investigators conduct investigations into crimes such as cyberstalking, cyberbullying, identity theft, online fraud and cyber espionage. They may use programming skills to develop custom tools and scripts for data analysis to identify activity patterns and build cases against suspects.

The responsibilities of a cybercrime investigator include:

- Investigating intrusions, recovering data from encrypted or erased files and recovering emails and deleted passwords.
- Collecting electronic evidence for use in criminal prosecutions.
- Testing existing security systems by attempting to hack into networks.
- Optimizing computer system performance.
- Presenting computer evidence and recovering files and data.
- Drafting testimonies and affidavits.
- Preparing reports and consulting with clients.



Structure of the bootcamp

This bootcamp guides you from learning the basics of programming in Python to launching a career as a cybersecurity specialist. Progress from novice to coding expert and pursue the career you deserve.

Your learning journey will include:

- **Bootcamp Prep** – Learn about the tech sector and how HyperionDev supports you in achieving your development goals. Begin programming with Python to determine if a tech career is the right path for you.
- **Introduction to Programming and Cybersecurity** – Get acquainted with cybersecurity, including types of cyberattacks and the impact of cybercrime. Explore industry best practices in software development and build a solid coding foundation in Python, one of the most powerful and versatile programming languages.
- **HTML and Semantic HTML** – Learn how web pages are created to understand the internet infrastructure exploited by hackers. Study common cyberattacks such as cross-site scripting, how they work, and how to prevent them.
- **Databases and SQL** – Discover how to write code that interacts with databases and learn how hackers exploit this process through attacks like SQL injection. Master secure coding practices to safeguard against vulnerabilities.
- **Penetration Testing and Digital Forensics** – Learn to ethically compromise systems as part of security evaluations, identify vulnerabilities, and report or resolve them before malicious actors can exploit them.
- **A Toolbox for Ethical Hacking** – Master tools used for reconnaissance, scanning and enumeration, exploitation, and post-exploitation.
- **Career Readiness and Employability (Post-Bootcamp Completion)** – After completing your bootcamp, you'll receive career support and guidance, including interview preparation and résumé reviews. You'll be equipped with technical skills as well as the professional development tools needed to succeed in your job search. We introduce graduates to the tech industry through networking events, career expos, and job opportunities with our hiring partners. With our support and mentorship, most graduates find employment within six months of completing the program.



What to expect from the cybersecurity syllabus

During the bootcamp, you will complete a series of learning tasks, each with a lesson and one or more practical activities. Some tasks introduce new concepts, while others are capstone projects designed to challenge you to integrate the skills you've acquired. These projects allow you to build more complex programs and showcase your learning.

By the end of your bootcamp, you should be able to:

- Program confidently in Python.
- Learn how to set up local and cloud-based virtual machines (command line as well as GUI).
- Write bash scripts and understand scripting exploits.
- Install and navigate a Linux environment, using advanced cybersecurity tools provided by Kali Linux, a distribution designed for digital forensics and penetration testing.
- Use the command line and bash scripting to secure servers and networks, protecting them from attacks.
- Write and understand HTML, semantic HTML, and CSS, and relate these skills to secure web programming.
- Learn security fundamentals and how to think like an experienced cybersecurity professional by evaluating threats and mitigating risks.
- Explore offensive security techniques, including XSS vulnerabilities, SQL injection, and penetration testing.
- Utilize support from our career team to refine your job application and interview skills, helping you secure a role in tech.

With Arizona State University and HyperionDev, you're never alone. Reach out to a code reviewer or mentor whenever you need help. Every piece of code you submit is reviewed by an expert who provides feedback to enhance its efficiency and quality.

We look forward to supporting you on your journey to becoming a cybersecurity expert!

Arizona State University is partnering with online education provider HyperionDev to offer a portfolio of high-impact outcomes-oriented online learning programs. Please note that course contents shown here are subject to change without prior notice. These programs are provided by HyperionDev and quality assured by Arizona State University to leverage their thought leadership in technical practice developed over decades of expertise.