COURSE SYLLABUS

Cybersecurity Bootcamp

Start your cybersecurity career and prepare for a new job in a growing field. Learn the skills for cybersecurity roles like Engineer and Analyst, and gain in-demand technical skills including Python programming, computer networking, Linux, and cloud computing in AWS.

For more information, visit
https://www.creativelive.com/learning-path/cybersecurity

support@creativelive.com • 302-217-6585

Course Outline

This package includes these courses

- Intro to Cybersecurity & Networks (24 Hours)
- Linux Operating System & Bash Scripting (18 Hours)
- Python Programming Bootcamp (30 Hours)
- Python for Network Security (30 Hours)
- Cybersecurity with Python (30 Hours)
- Offensive Security with Python (24 Hours)
- Digital Forensics (24 Hours)
- Cloud Computing with AWS (18 Hours)
- Cybersecurity Industry & Job Prep (12 Hours)

Intro to Cybersecurity & Networks

Get a comprehensive understanding of computer communication and security systems, including network models, authentication, authorization, admin roles, foundational cybersecurity concepts, Linux, Python, and networking protocols.

- Learn how computer communication and security systems work
- Get to know network models and the layers within them
- Gain an understanding of authentication, authorization, and admin roles

Linux Operating System & Bash Scripting

Learn how to work with Linux operating systems, navigate directories, and utilize major Linux distributions for cybersecurity, including Kali, NodeZero, and BlackArch. This course is open to beginners and requires no prior experience with Linux, Bash scripting, or coding.

- Use fundamental Linux commands and Bash scripts
- Navigate directories, files, and distributions for cybersecurity

- Learn Linux permissions and file security

Python Programming Bootcamp

Learn Python programming from the ground up, covering essential concepts, real-world applications, and coding best practices. This course prepares you to tackle technical challenges and build a portfolio of Python projects.

- Master Python fundamentals, including variables, data types, loops, and functions.
- Develop logical programming skills using conditionals, indexing, and slicing techniques.
- Work with file handling operations such as reading, writing, and appending to text files.
- Explore computer science fundamentals, including Big-O notation and sorting algorithms.
- Gain hands-on experience with object-oriented programming (OOP) to build scalable applications.
- Use Git and GitHub to manage projects and create a professional coding portfolio.

Python for Network Security

This course provides a comprehensive introduction to Python programming for networking and network security, covering topics such as foundational protocols, network monitoring, and scripting tools for network security. Learn how to secure and monitor networks for suspicious activities using Python scripting tools.

- Understand foundational network transfer protocols and security fundamentals
- Use Python to monitor networks and detect suspicious activities
- Build and implement scripting tools for basic network security tasks
- Apply Python programming techniques to automate network monitoring workflows
- Design and implement scripting solutions for basic network security protocols

Cybersecurity with Python

Learn how to use Python to automate security processes, execute system administration tasks, and solve common IT problems while also gaining an understanding of fundamental security protocols and methodologies associated with cybersecurity.

- Automate security processes and system administration tasks using Python scripting
- Apply fundamental security protocols and cybersecurity methodologies to real-world IT problems
- Use Python to identify, analyze, and resolve common network and system vulnerabilities
- Build practical tools for monitoring systems and streamlining security workflows

Offensive Security with Python

Learn the essential tools and techniques for preventing, detecting, and responding to cyber attacks, including penetration testing, threat modeling, and vulnerability analysis. Enhance your security measures by testing network protocols using Python programming and the Linux operating system.

- Learn the major tools and strategies for preventing, detecting, and responding to cyber attacks
- Learn how to plan and execute penetration tests
- Perform threat modeling and vulnerability analysis

Digital Forensics

Discover the inner workings of a Security Operations Center (SOC) and learn how to protect an organization's critical assets from various threats in this comprehensive course. Gain insights into security monitoring and logging, incident response, and the role of a SOC Analyst in preventing data loss.

- Learn the structure and daily operations of a modern Security Operations Center (SOC)
- Understand security monitoring, logging, and the incident response lifecycle
- Develop strategies for implementing security protocols

Cloud Computing with AWS

Learn how to build and secure an enterprise-level cloud environment with AWS. Gain practical experience and expert knowledge on AWS security, including SOC operations and the benefits of a well-architected framework in the cloud.

- Learn the fundamentals of AWS and cloud computing
- Build and secure and enterprise-level cloud environment
- Navigate cloud infrastructure, networking, and databases

Cybersecurity Industry & Job Prep

Learn how to break into the cybersecurity industry and succeed with job search strategies, mock interviews, and explorations of different job roles. Get tips on networking, resume prep, and continuous learning for a successful career.

- Learn job search strategies
- Prepare your resume
- Participate in mock interviews
- Review different job opportunities