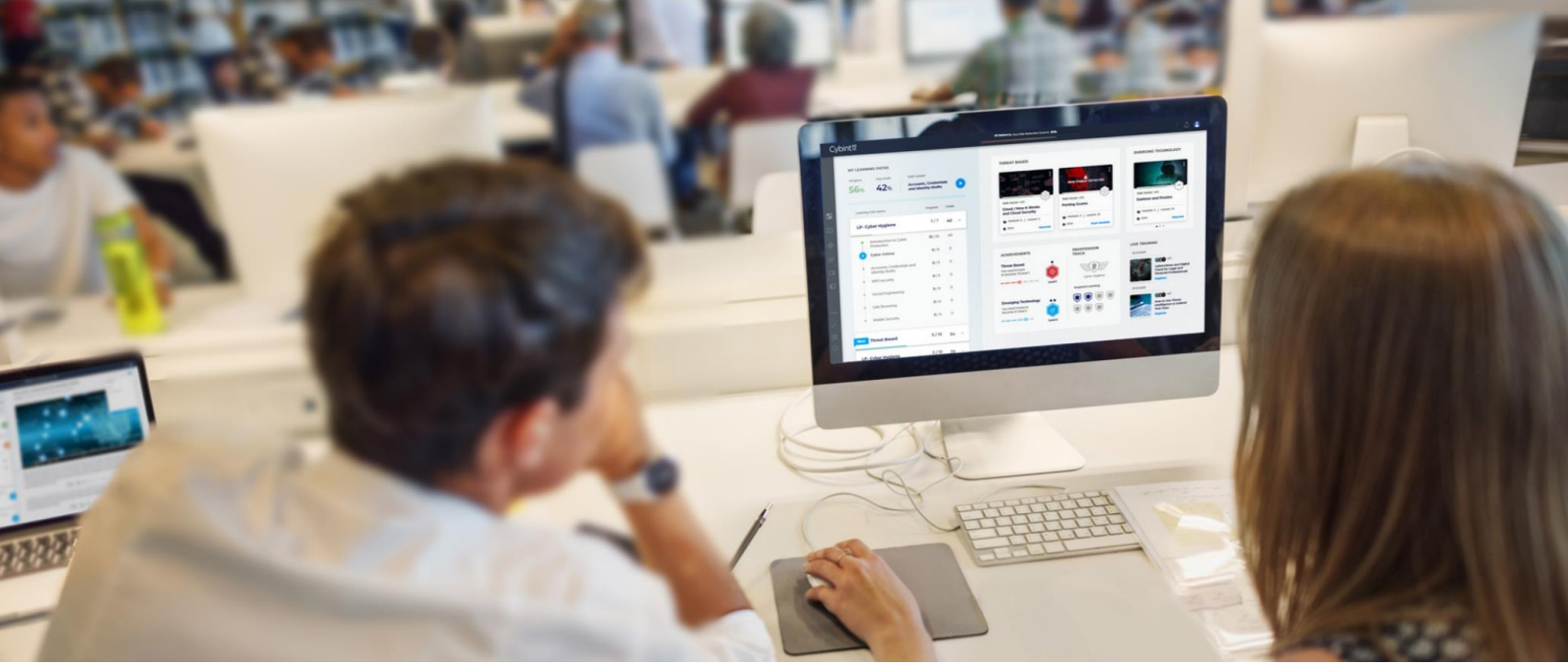
CYBER SECU RITY

SYLLABUS

Full time – 12 weeks



OVERVIEW

Our Cybersecurity Bootcamp covers the hands-on and practical skills necessary for our students to land high-paying careers in cybersecurity, one of the world's fastest growing industries.

The Cybersecurity Bootcamp is an accelerated cybersecurity training program designed to successfully prepare people with little or no background in IT for entry level jobs in cybersecurity, a highly in-demand and lucrative career path. The Bootcamp is delivered in a blended format with both on campus learning and online self-paced activities.

Cybersecurity is the fastest growing market in technology with 30x growth over the last decade. Not only is it a hot topic, but the field has had 0% unemployment for nearly a decade. With plentiful opportunities and competitive compensation, the only thing standing in your way of a lucrative, future-proof career is skill.

In short, our Cybersecurity Bootcamp is for anyone interested in becoming a cybersecurity professional. If a dynamic and rewarding career is something you're looking for, then you've come to the right place. Cybersecurity opens doors to many opportunities and future work roles.

WHAT YOU WILL LEARN

12 weeks with various exercises along the training

Timeline	Key concepts	
Week 1	• Introduction to the Bootcamp. • Overview of the cybersecurity landscape and industry. • Basics of computer and device hardware, software, operating systems and processes.	• Basics of networking traffic, hardware components and topology. • Network communication principles and methods.
Week 2	• Network and routing protocols / services. • Packet level traffic analysis. • Hands-on operation of a computer network and equipment, monitoring and	analysing network traffic flow, patterns and performance. • Hands-on creation and analysis of critical network servers.
Week 3	• Hands-on creation and analysis of telnet, web, data and active directory servers. • Hands-on analysis of network topologies, network mapping and OS fingerprinting. • Telecommunication concepts	and range. • System and network admin concepts, management principles and controls. • Hands-on creation and use of virtual machines and bootable USB OS.
Week 4	• Overview of threats, classes, attackers, tactics, and application security risks (OWASP). • Hands-on communications security through encrypting and decrypting data and	medias. • Hands-on backup and recovery of data, devices and servers. • Network security principles, methods, protocols, components and architectures.

WHAT YOU WILL LEARN

The Cybersecurity Bootcamp is for anyone interested in becoming a cybersecurity professional.

Timeline	Key concepts
Week 5	• Hands-on assessment of access controls and hardening techniques to ensure a network's security. • Hands-on configuration and utilization of a firewall (on Windows, Linux and hardware firewall). • Hands-on configuration and utilization of a network/host intrusion detection/ prevention system to alert and prevent malicious activity on a network.
Week 6	• Hands-on configuration and utilization of a security information and event management system to correlate, research, analyse logs and provide timely detection of misuse, threats and malicious activity on the network. • Hands-on malware detection, analysis, isolation and removal.
Week 7	• Cyber-forensic investigation methodologies, mindset, tools. • Hands-on forensics investigation: logs, system files, media, memory dump and traffic monitoring and analysis.
Week 8	• Overview of network vulnerabilities, associated attacks; ethical hacking methodologies, stages, principles, tools and techniques. • Hands-on conducting of vulnerability and compliance scanning; and correction recommendation. • Hands-on performing incident response, damage assessment, incident triage, tracking and reporting.

WHAT YOU WILL LEARN

We focus on skills, not exams

Timeline	Key concepts	
Week 9	• Full day scenarios: hands-on protecting a network from a range of cyber-attacks (DDOS, SQL injection, XSS,	ransomware, MITM, ARP poisoning, etc.).
Week 10	• Analysis of system security and organizational posture trends. • Analysis of cyber-defense trends and staying at the cutting edge of the industry.	• Performing of security design and architecture evaluation and ensuing recommendation.
Week 11	• Hands-on performing of static and dynamic analysis of drive images and other data sources, recovery and mitigation/remediation of an enterprise system.	• Hands-on process of the whole chain of custody for handling digital evidence.
Week 12	• Risk and security management processes and security models. • Cybersecurity and privacy principles. • Advising on disaster recovery, contingency and continuity. • Summary and presentation by	Students. • Technical and soft-skill preparation of a job interview. • Final hands-on scenario.

YOU ARE CLOSE TO CHANGE YOUR LIFE AND ENTERING A NEW WORLD OF POSSIBILITIES...

 www.weecode.co

support@weecode.co 

 *WeecodeLuxembourg*

 *weecode_luxembourg*

 *Weecode Luxembourg*