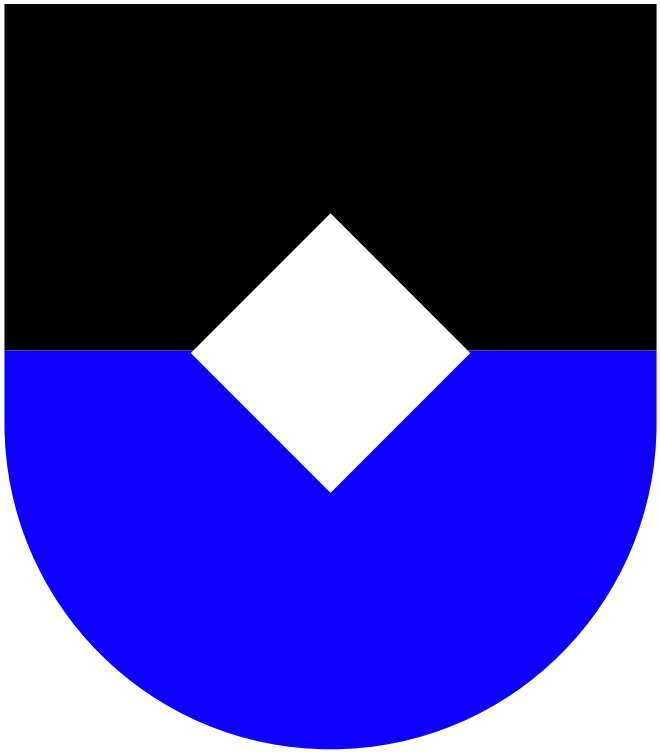
Code Academy

A: Upės g. 21, Vilnius
T: +370 663 66 555



CodeAcademy.lt

Cyber Security (223003115)

656 hours

A: Upės g. 21, Vilnius
T: +370 663 66 555

Cyber Security

Within the Cybersecurity program, students will learn the skills necessary to assist in the identifi cation, assessment, reporting, and mitigation of technology and information security risks. The program will also provide students with the knowledge necessary to determine information system vulnerabilities and residual risks based on the analysis of technical artifacts, interviews, and evaluations of IT systems.

The course will also cover the leading approaches to managing cybersecurity, including 'defense in depth' and the National Institute of Standards and Technology (NIST) Cybersecurity Frame work. The Cybersecurity Bootcamp program includes instruction towards CompTIA Security+ and CySA+ certifications. Through labs with sandboxed virtual machines, the course provides hands-on training in CEH-inspired scenarios, defensive and o ensive cybersecurity, networking, systems, web technologies, and databases. Assignments will span PC and server so ware, application, and code with a solid technical background in computer vulnerabilities, a ack vectors, exploits, and mitigation controls.

To round out the program, students will conduct event and incident investigations to include computer intrusions, infections, and unauthorized access or usage and provide reports to mana gement and recommend sound remediation and mitigation

Expected outcomes:

Assist in the identification, assessment, and reporting of technology and information security risks. Data analysis by students will produce meaningful, measured metrics from risk manage ment programs.

Understand leading approaches to managing cybersecurity, including 'defense in depth' and the National Institute of Standards and Technology (NIST) Cybersecurity Framework
Hands-on training in CEH-inspired scenarios, defensive and o ensive cybersecurity, networking, systems, web technologies, and databases.

Conduct technical analysis, suggest change control recommendations, and communicate with business customers

A: Upės g. 21, Vilnius
T: +370 663 66 555

Cyber Security Course TOPICS	HOURS	DESCRIPTION
Cybersecurity core	**240**	Cybersecurity basics including: Controls, Frameworks, Benchmarks, Virtual Machines, Threats, Vulnerabilities, Defenses, Secure Software, Testing, Cryptography How to build out a Kali Linux machine while learning about networking and data security. Network configurations and data security, including Network Design, Firewall Configuration, Access Control Viruses and Ransomware, intrusion detection, useful tools, introduction to embedded (control) systems, secure shell, mobile & endpoint security. Virtual Machines, malicious code, Disaster Recovery, and Powershell Identifying and responding to incidents, technical and legal elements of forensics Learn how resiliency, automation, and backups provide essential and fundamental protection Start learning what a career in cybersecurity looks like

A: Upės g. 21, Vilnius
T: +370 663 66 555

Cybersecurity intermediate	**200**	Understand roles and responsibilities, security controls, indicators of compromise, understanding threats, attack tools, monitoring networks Protect networks, monitor and analyze various services for signs of compromise, run scripts, understand and use SIEM (Security Information and Event Management) Examine 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. Learn intermediate incident response as well as effective recovery. How to conduct a risk analysis and vulnerability assessment Understand regulations in cybersecurity Learn technical and non-technical controls, the relationship of security and privacy, & how to configure and analyze share permissions Learn cloud technologies and how to protect your cloud-based solutions with OWASP
Cybersecurity professional	**200**	Discuss the ethics of hacking Penetration testing, Metasploitable2 and Eternal Blue

A: Upės g. 21, Vilnius
T: +370 663 66 555

		Understanding the underlying capabilities of search engines, WHOIS, DNS, nmap, dirbuster and gobuster, nikto, social engineering, specialized scanners, SNB enumeration Proactive threat hunting. Local File Inclusion and Remote File Inclusion, SQL injection techniques and defenses, hacking and testing mobile devices. Counter and create a buffer overflow attack Add to your malware knowledge with advanced techniques and tools. Elevate privilege to fully exploit platforms, monitor the network, or access other systems during an attack. Learn various sources for exploits and how to use them, including password attacks.
Soft skills	**16**	CV, LinkedIn, job interview workshops, individual activities and fees, IT specialist competencies
Total	**504**	