HPC

Digital Learning Hub_
Academy
Powered by HPC

CS
ACADEMY

DIGITAL LEARNING HUB · CYBERSECURITY ACADEMY

Cybersecurity Academy Curriculum

Detailed overview of the courses, modules and key learning objectives.

DIGITAL LEARNING HUB · CYBERSECURITY ACADEMY

Cybersecurity Academy Curriculum

The Cybersecurity Academy prepares learners to defend, test and secure digital systems. The programme starts with a Common Core shared by all learners, continues with one of two specialisations, and ends with a Capstone Project in which learners apply everything they have learned to a real-world challenge.

Programme structure

PART 1
Common Core
Linux, networking and security foundations shared by all learners.

›

PART 2 · SPECIALISATION
Red Team
Offensive security and ethical hacking.

OR

PART 2 · SPECIALISATION
Blue Team
Defensive security and operations.

›

PART 3
Capstone Project
A real-world project in the chosen specialisation.

Two specialisations, two profiles

Red Team
Offensive security and ethical hacking

FOCUS
Understanding how attackers think and how systems are compromised.

APPROACH
Hands-on, methodology-driven labs: from reconnaissance and web exploitation to privilege escalation, Active Directory attacks and reporting.

LEARNERS BECOME
Penetration testers who can plan, execute and report on authorised security assessments.

Blue Team
Defensive security and operations

FOCUS
Detecting, investigating and responding to threats.

APPROACH
Security operations tooling such as SIEM, EDR and forensics, applied to realistic alerts and incidents, with threat hunting and AI security.

LEARNERS BECOME
Analysts who can monitor, investigate and respond to threats in a security operations centre.

PART 1

Common Core

The foundation for every cybersecurity path

Every learner starts here. The Common Core builds the technical foundation that all security work relies on: operating systems, networking and core security principles. By the end, learners are ready to choose the specialisation that matches their goals.

What you will learn

1 Operating Systems

The practitioner's toolkit.

- Linux command line, file systems and permissions
- Shell operations
- User and group administration
- Processes, networking basics and logs
- Bash scripting basics
- Synthesis Project: Secure OS configuration

2 Networking Fundamentals

How data moves across a network.

- OSI and TCP/IP models, subnetting and routing
- DNS, DHCP and VLANs
- Packet capture, Wireshark and insecure protocols
- Traffic analysis and identifying malicious traffic

3 Network Defence

Controlling and protecting traffic.

- Firewalls (iptables/nftables) and VPNs
- Proxies, TLS/SSL basics and content filtering
- Synthesis Project

4 Security Fundamentals

Principles, controls and risk.

- CIA triad, AAA and authentication
- RBAC, MAC, DAC and least privilege
- Threat actors, attack vectors and risk management
- Administrative, technical and physical controls
- Logging and monitoring fundamentals
- Incident response basics and policies
- Synthesis Project

PART 2 · SPECIALISATION

Red Team

Offensive security and ethical hacking

Develop the skills to think like an attacker and assess systems the way adversaries do. Learners follow a professional penetration-testing workflow, from scoping and reconnaissance through exploitation and Active Directory compromise to clear, actionable reporting.

What you will learn

1 Engagement Foundations

Scope, methodology and threat modelling.

- Legal considerations, rules of engagement and scope definition
- Threat modelling: STRIDE, PASTA and MITRE ATT&CK
- PTES methodology
- Reporting and environmental CVSS
- Synthesis Project

2 Reconnaissance and Enumeration

Passive and active information gathering, and mapping targets.

RECONNAISSANCE

- OSINT fundamentals, metadata and email harvesting
- Subdomain and DNS enumeration
- Shodan, Censys and FOCA
- Tech-stack fingerprinting
- Synthesis Project: Recon automation, active vs passive recon

ENUMERATION AND SCANNING

- Advanced Nmap usage and banner grabbing
- SMB, SNMP and LDAP enumeration
- NSE scripting and web technology enumeration
- Nikto, OpenVAS and Nessus
- Identifying vulnerabilities manually
- Synthesis Project: Assessment and reporting

3 Web Application Security

Attacking the OWASP Top 10.

- Burp Suite: Interceptor, Repeater, Intruder and Decoder
- Broken access control, identification and authentication failures
- Injection (XSS, SQL injection) and insecure design
- Cryptographic failures, security misconfiguration and integrity failures
- SSRF, and security logging and monitoring failures
- Synthesis Project: Full OWASP integration

4 Advanced Web Exploitation

Beyond the Top 10: chained and modern attacks.

- API reconnaissance and exploitation, JWT attacks
- Advanced SQL injection and WAF bypass techniques
- Server-side template injection (SSTI) and race conditions
- SSRF to RCE chains and deserialization attacks
- Synthesis Project: Advanced web recap

5 Exploitation and Privilege Escalation

From initial access to full system control.

- Reverse and bind shells, file transfer methods
- Public exploits, exploit modification and workflow
- Metasploit Framework: MSFvenom and Meterpreter
- Password attacks (online and offline) and wordlists
- Linux privilege escalation: SUID, capabilities, cron jobs, kernel and service exploitation
- Windows privilege escalation: service permissions, token abuse and impersonation
- Synthesis Project: Exploit chaining

6 Active Directory

Attacking enterprise Windows environments.

- AD fundamentals and GPO misconfiguration
- Kerberoasting, Pass-the-Hash and Pass-the-Ticket
- Domain enumeration with BloodHound and SharpHound
- SMB relay attacks and NTLM abuse
- Internal pivoting and lateral movement
- DNS zone attacks and persistence
- AD exploitation paths
- Synthesis Project: Active Directory concepts

7 Binary Exploitation

Memory corruption fundamentals.

- Buffer overflow basics (32-bit)
- EIP control and bad characters
- Shellcode basics and the Mona.py workflow
- Structured Exception Handler (SEH) exploitation
- Synthesis Project

8 Post-Exploitation and Reporting

Pivoting, exfiltration and communicating results.

- Pivoting, tunnelling and proxying
- Data exfiltration scenarios
- Report writing and executive reporting
- Synthesis Project: All Concepts

9 AI and LLM Security

Securing AI systems and applying AI in the SOC.

- LLM security
- AI security
- Prompt injection
- AI governance
- AI SOC

PART 2 · SPECIALISATION

Blue Team

Defensive security and operations

Develop the skills to detect, investigate and respond to threats. Learners follow the path of a security operations analyst, from risk assessment and system hardening to SIEM, threat hunting, incident response, governance and the security of AI systems.

What you will learn

1 Security Foundations and Risk

Assessing assets, threats and risk.

- Asset discovery and security assessment
- Threat actors, attack vectors and STRIDE threat modelling
- Vulnerability analysis and prioritisation with CVSS
- Risk quantification (SLE, ARO, ALE) and control selection with CIS Controls
- Encryption, hashing and PKI

2 System and Network Hardening

Securing servers, endpoints and the perimeter.

- Linux server hardening: CIS Benchmarks, AppArmor and auditd
- Windows hardening and event monitoring: Sysmon, Group Policy and AppLocker
- EDR deployment and configuration
- Patch management and change control
- Firewalls, segmentation and intrusion detection

3 SIEM and Detection Engineering

Collecting, analysing and triaging security data.

- SIEM architecture and deployment
- Log formats, queries and dashboards
- Detection rules and correlation logic, including Sigma
- SOC alert workflow and false positive management
- Cross-platform SIEM proficiency

4 Threat Analysis and Hunting

Investigating phishing, traffic and malware.

- Email header analysis, SPF/DKIM/DMARC and IOC extraction
- Packet capture analysis and C2 detection
- Cyber threat intelligence, ATT&CK mapping and YARA rules
- Malware classification and kill chain reconstruction
- Hypothesis-driven threat hunting and detection gap analysis

5 Incident Response and Forensics

Preparing for, handling and learning from incidents.

- NIST 800-61 lifecycle, playbooks and communication
- Containment, eradication and service recovery
- Disk imaging, memory analysis and chain of custody
- Post-incident review and detection improvement
- Tabletop exercise design and facilitation

6 Governance, Resilience and Identity

Compliance, continuity and access.

- Compliance frameworks (NIST CSF, ISO 27001), policy authoring and vendor assessment
- Business impact analysis and disaster recovery
- Enterprise IAM, SSO and cloud security

7 SOC Automation and Security Culture

Automating the SOC and building awareness.

- SOAR workflows and automated triage
- Security awareness program design

8 AI and LLM Security

Securing AI systems and applying AI in the SOC.

- LLM security
- AI security
- Prompt injection
- AI governance
- AI SOC

PART 3

Capstone Project

Bring it all together

The capstone project is the culmination of your specialisation, designed to showcase your skills in real-world applications. It is primarily driven by your own idea, and may also be developed in collaboration with an industry partner

Examples of capstone projects

1. Build and document a virtual Security Operations Center that centralises logs, triggers alerts and supports analyst triage.
2. Plan and run a full penetration test against a lab environment, from reconnaissance to an executive-level report.
3. Deploy honeypots to capture real attacker activity and turn the findings into threat trend and hardening recommendations.
4. Emulate an adversary with MITRE ATT&CK and validate that the right detections fire.
5. Build an automated threat intelligence pipeline that collects, normalises and exports indicators of compromise.

BEYOND THE PROGRAMME

More than an Academy, a whole learning experience

The learning experience goes beyond the hands-on projects. Participants also get opportunities to connect with Luxembourg's cybersecurity and digital ecosystem through talks with industry professionals, researchers and companies, organised workshops, hackathons and outdoor events. These activities encourage networking, collaboration, knowledge sharing and community building, giving participants the chance to develop the skills and connections that support a career in cybersecurity.

Talks with professionals | **Workshops** | **Hackathons** | **Outdoor events** | **Networking**