

CYBER DEFENDER COURSE

SYLLABUS | 215 HOURS

Module 1	• Introduction to cybersecurity	5 Hours
Module 2 Networking	• General communication concept • Functional end-point network components • IPv4 assignment options • MAC address and vendors • The VLSM concept • DHCP configuration • Dynamic routing (OSPF/RIP) • HTTP authentication and analysis	35 Hours
Module 3 Microsoft Technologies On-Prem	• VirtualBox network adapters • Windows OS • Windows shells (CMD and PowerShell) • What is a server • Active directory centralized unit • AD objects management • Applying group policy • GPO templates • AD authentication • NTLM authentication • Kerberos authentication • Active Directory Hardening	35 Hours
Module 4 Linux	• Open-source concepts • Importing the VM • Introduction to the shell • Users and groups & Permissions • Remoting (SSH Client) • SSH protocol explained • Processing text with delimiters • Package management • Hash algorithms • Find binaries and documentation (which, where is)	50 Hours
Module 5 Anatomy of an Attack	• The cyber kill chain and MITRE • Introduction to reconnaissance (OSINT) • Active scanning • Brute force attacks • Introduction to vulnerabilities and CVEs • Remote control	40 Hours
Module 6 SIEM/SOC	• The importance of SOC • SOC Roles • Mitre Attack • IP Investigation / Public Tools • What is Incident Response • Common Attack Investigation - DDoS / Malware / Ransomware • Event Viewer • SIEM Introduction • Definitions and Terms • SIEM Architecture - Wazuh / Qradar / Splunk	45 Hours
Module 7 Introduction to AI	• Introduction to AI	5 Hours