EC-Council Certified Network Defender (CND)

ID CND **Price** CHF 4,790.—(excl. VAT) **Duration** 5 days

Who should attend

- Network Administrators
- Network Security Administrators
- Network Engineer
- Data Security Analyst
- Network Security Engineer
- Network Defense Technician
- Security Analyst
- Security Operator
- Network security
- Cybersecurity Engineer

Prerequisites

Basic Knowledge in Networking Concepts

Course Objectives

- Plan, implement, and administer network security management for an organization.
- Gain knowledge of various security risks, threats, and vulnerabilities.
- Assist in obtaining and maintaining an organization's compliance with required regulatory standards and frameworks.
- Design and implement network security policies and procedures .
- Apply security principles, protocols, and controls that suit today's distributed and mobile computing environment.
- Apply strong Identity and Access Management (IAM), network segmentation, and encryption techniques to strengthen the organization's network.
- Manage and maintain Windows Security Administration.
- Manage and maintain Linux Security Administration.
- Manage and mitigate the security risks and challenges associated with the enterprise's mobile device usage policies.
- Manage and mitigate the security risks and challenges associated with IoT devices used in enterprises.
- Implement strong data security techniques to secure an organization's data.
- Implement and manage the security of virtualization technologies, i.e., Network Virtualization (NV), Software Defined Network (SDN),
- Network Function Virtualization (NFV), OS Virtualization, Containers, Dockers, and Kubernetes used in modern-day networks.
- Implement and manage cloud security on various cloud platforms such as AWS, Azure, Google Cloud Platform, etc.
- Implement and manage wireless network security.
- Perform risk assessment and vulnerability assessment/scanning through various scanning tools and generate detailed reports.
- Identify the critical data and choose an appropriate backup method, media, and technique to regularly perform a successful backup of organization data.
- Provide a first response to the network security incident and assist the IRT and forensics investigation teams in dealing with an incident.
- Identify the Indicators of Compromise (IoC) and Indicators of Attack (IoA) on networks .
- Integrate threat intelligence capabilities to leverage/consume threat intelligence for proactive defense.
- Conduct attack surface analysis by identifying Indicators of Exposures (IoE).
- Assist in Business Continuity (BC) and Disaster Recovery (DR) planning.
- Monitor network traffic and ensure its security .
- Perform log management.
- Monitor network logs against any anomalies.
- Manage proxy and content filtering .
- Troubleshoot the network for various network problems.
- Identify various threats to an organization’s network .
- Harden security of various endpoints individually in the organization’s network .
- Select the appropriate firewall solution, topology, and configurations to harden security through the firewall.
- Determine an appropriate location for IDS/IPS sensors, tuning IDS for false positives and false negatives, and configurations to harden security through IDPS technologies
- Maintain the inventory of computers, servers, terminals, modems, and other access devices .
- Provide security awareness guidance and training.
- Add, remove, or update user account information.
- Apply operating system updates and patches and make configuration changes.
- Update system configurations to maintain an updated security posture using current patches, device and operating system hardening techniques, and access control

lists.
- Manage network authentication, authorization, and accounting (AAA) for network devices.
- Review audit logs from the Firewall, IDS/IPS, servers, and hosts on the internal, protected network.
- Analyze, troubleshoot, and investigate security-related information systems' anomalies based on the security platform.
- Maintain, configure, and analyze network and host-based security platforms.
- Evaluate security products as well as security operations procedures and processes.
- Identify and classify organizational assets, including hardware, software, data, and critical infrastructure.
- Implement system integrity monitoring tools and techniques to identify alterations in critical files, configurations, or system states.
- Understand the role and functionality of EDR/XDR solutions implemented to contain and remediate threats.
- Understand the role and functionality of UEBA solutions implemented to monitor and analyze user and entity activities for anomalous behavior patterns.
- Conduct PIA processes to evaluate and assess the potential impact of new systems, processes, or initiatives on individual privacy.
- Collaborate with security teams to enhance threat-hunting strategies and incident response capabilities.
- Understand the role of Security Orchestration, Automation, and Response (SOAR) platforms in cybersecurity operations.
- Plan and execute the integration of zero trust principles into existing security architectures and infrastructures.
- Stay updated about the newly emerging cyber threats with the help of the latest cybersecurity news, industry publications, and reputable sources of information, including security blogs, research reports, and whitepapers.
- Understand the role of AI/ML in enhancing cyber defense, threat detection, and response.

Course Content

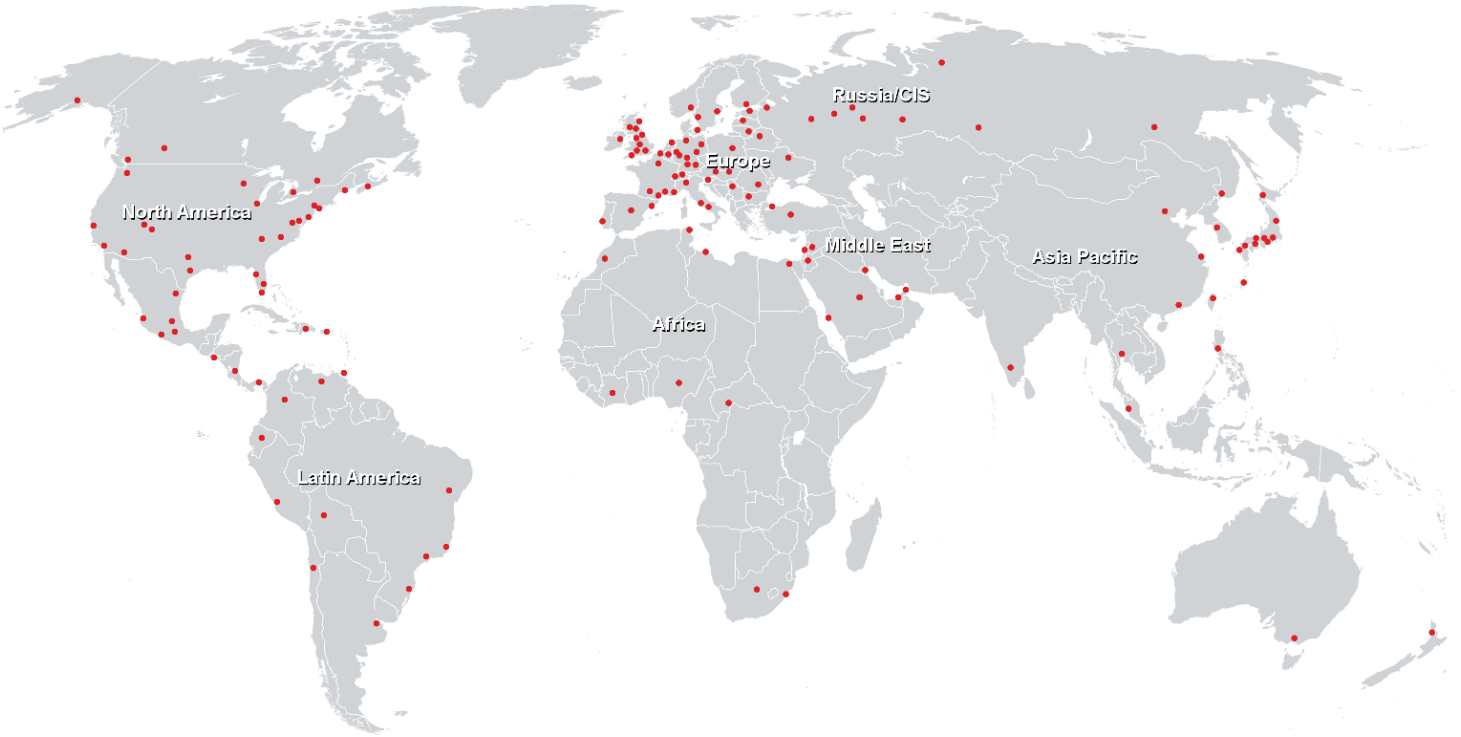
- Network Attacks and Defense Strategies
- Administrative Network Security
- Technical Network Security
- Network Perimeter Security
- Endpoint Security-Windows Systems
- Endpoint Security-Linux Systems
- Endpoint Security- Mobile Devices
- Endpoint Security-IoT Devices
- Administrative Application Security
- Data Security
- Enterprise Virtual Network Security
- Enterprise Cloud Network Security
- Enterprise Wireless Network Security
- Network Traffic Monitoring and Analysis
- Network Logs Monitoring and Analysis
- Incident Response and Forensic Investigation
- Business Continuity and Disaster Recovery
- Risk Anticipation with Risk Management
- Threat Assessment with Attack Surface Analysis
- Threat Prediction with Cyber Threat Intelligence

APPENDIX (Self-Study)

- APPENDIX A: Computer Network Fundamentals
- APPENDIX B: Physical Network Security
- APPENDIX C: Virtual Private Network (VPN) Security
- APPENDIX D: Endpoint Security – MAC Systems

EC-Council Certified Network Defender (CND)

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch