Certified Network Defender Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The global digital economy is facing an unprecedented surge in sophisticated cyber threats, making Network Defense a critical, in-demand field. Organizations are shifting from reactive breach response to proactive cyber resilience, creating an urgent need for highly-skilled Certified Network Defenders. Certified Network Defender Training Course is designed to transition IT professionals into Blue Team experts, mastering the protect, detect, respond, and predict methodology. Participants will gain real-world defensive skills in perimeter security, endpoint hardening, cloud security, and threat intelligence to safeguard vital network infrastructure against modern-day Advanced Persistent Threats and zero-day exploits. The CND certification validates the essential competencies required by global standards, including the NICE Framework, ensuring graduates are ready to secure complex, hybrid environments and maintain business continuity under duress.

This intensive training program moves beyond theoretical knowledge, emphasizing hands-on labs and incident response simulation to build immediate, job-ready expertise. We delve deep into essential defensive mechanisms, covering Firewall Management, IDS/IPS Configuration, Secure VPNs, Security Information and Event Management, and crucial log analysis techniques. Trending topics like IoT Security, Cloud Network Security, Mobile Device Management, and Operational Technology defense are integrated throughout the curriculum, ensuring relevance in today's multi-cloud and hyper-connected enterprise landscape. By achieving the CND certification, graduates significantly accelerate their career trajectory, positioning themselves for elite roles as Network Security Engineers, CND Analysts, and Security Operations Center personnel, and becoming indispensable assets in the fight for enterprise cybersecurity.

Programme Curriculum

Certified Network Defender Training Course

Introduction

The global digital economy is facing an unprecedented surge in sophisticated cyber threats, making Network Defense a critical, in-demand field. Organizations are shifting from reactive breach response to proactive cyber resilience, creating an urgent need for highly-skilled Certified Network Defenders. Certified Network Defender Training Course is designed to transition IT professionals into Blue Team experts, mastering the protect, detect, respond, and predict methodology. Participants will gain real-world defensive skills in perimeter security, endpoint hardening, cloud security, and threat intelligence to safeguard vital network infrastructure against modern-day Advanced Persistent Threats and zero-day exploits. The CND certification validates the essential competencies required by global standards, including the NICE Framework, ensuring graduates are ready to secure complex, hybrid environments and maintain business continuity under duress.

This intensive training program moves beyond theoretical knowledge, emphasizing hands-on labs and incident response simulation to build immediate, job-ready expertise. We delve deep into essential defensive mechanisms, covering Firewall Management, IDS/IPS Configuration, Secure VPNs, Security Information and Event Management, and crucial log analysis techniques. Trending topics like IoT Security, Cloud Network Security, Mobile Device Management, and Operational Technology defense are integrated throughout the curriculum, ensuring relevance in today's multi-cloud and hyper-connected enterprise landscape. By achieving the CND certification, graduates significantly accelerate their career trajectory, positioning themselves for elite roles as Network Security Engineers, CND Analysts, and Security Operations Center personnel, and becoming indispensable assets in the fight for enterprise cybersecurity.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Harden and secure heterogeneous host platforms, including Windows and Linux operating systems, against zero-day vulnerabilities.
2. Design and implement Defense-in-Depth strategies utilizing a Zero Trust Architecture across the network and cloud.
3. Configure, manage, and monitor Next-Generation Firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) for perimeter defense.
4. Master Network Traffic Analysis and Packet Analysis using tools like Wireshark to detect anomalies and Indicators of Compromise.
5. Develop and enforce comprehensive, regulatory-compliant Network Security Policies and Data Governance frameworks.
6. Secure Enterprise Cloud Networks by applying best practices in container security and Cloud Security Posture Management.
7. Implement advanced Data Loss Prevention (DLP), data encryption, and endpoint security solutions for mobile and remote workforces.
8. Conduct effective Incident Response lifecycle management, from detection and containment to eradication and post-incident digital forensics.
9. Apply Threat Intelligence and Attack Surface Analysis to proactively anticipate and mitigate emerging Advanced Persistent Threats.
10. Secure modern ecosystems, including Wireless Networks, IoT (Internet of Things), and OT (Operational Technology) environments.
11. Design and test robust Business Continuity (BC) and Disaster Recovery (DR) plans to ensure organizational resilience.

12. Perform secure configuration and management of remote access using IPSec/SSL VPNs and strong Multi-Factor Authentication (MFA).
13. Integrate Security Information and Event Management (SIEM) for centralized log correlation and real-time threat detection.

Target Audience

1. Network Administrators and System Administrators
2. Network Security Engineers and Network Defense Technicians.
3. Security Analysts and Security Operations Center Analysts.
4. IT Security Professionals who manage network perimeter defenses.
5. IT Auditors and Security Consultants who need a defense-side perspective.
6. Mid-Level Penetration Testers seeking to understand Blue Team methodologies.
7. Anyone preparing for the official EC-Council CND certification exam.
8. Senior Technical Support Engineers responsible for troubleshooting security issues.

Course Modules

Module 1: Network Defense Fundamentals and Architecture

- Introduction to the Protect, Detect, Respond, Predict security model and the NICE Framework.
- Implementing a Defense-in-Depth strategy using a layered security approach and Zero Trust.
- Understanding the role of network components and securing the OSI Model layers.
- Analyzing common network attacks and their defensive countermeasures.
- Case Study: Analyzing the network architectural failure during a major DDoS attack and designing a multi-layered defense using CDN and scrubbers.

Module 2: Perimeter Protection and Firewall Management

- Secure configuration and deployment of stateful firewalls and Next-Generation Firewalls
- Setting up and managing Intrusion Detection Systems and Intrusion Prevention Systems
- Implementing Network Segmentation, including DMZ design, to isolate high-risk services.
- Securely configuring IPSec and SSL VPNs for remote user and site-to-site connectivity.
- Case Study: Troubleshooting a firewall policy failure that allowed lateral movement, leading to a ransomware outbreak, and implementing a least-privilege policy.

Module 3: Host and Endpoint Security Hardening

- Applying OS Hardening techniques for Windows Server and Linux
- Configuring and managing modern Endpoint Detection and Response solutions and Next-Gen Antivirus.
- Implementing robust Patch Management and Vulnerability Management programs to reduce the attack surface.
- Securing user access via Authentication, Authorization, and Accounting protocols and Multi-Factor Authentication
- Case Study: Remediating a breach caused by a privileged account compromise on a legacy server by implementing ZTA principles and EDR.

Module 4: Cloud and Virtualized Network Security

- Understanding and securing the Shared Responsibility Model in IaaS, PaaS, and SaaS environments.
- Applying security best practices for AWS/Azure/GCP virtual networks, including Security Groups and VPC flow logs.

- Implementing Container Security and securing virtual machine hypervisors and tenants.
- Utilizing Cloud Security Posture Management tools for continuous compliance and misconfiguration detection.
- Case Study: Securing a development environment deployed in a public cloud, focusing on hardening an insecure Kubernetes cluster configuration.

Module 5: Network Traffic Monitoring and Analysis

- Performing deep-dive Packet Analysis using Wireshark to interpret network conversations and identify malicious payloads.
- Configuring Log Management systems for central collection, retention, and time synchronization.
- Implementing Security Information and Event Management for real-time log correlation and alert generation.
- Techniques for Network Anomaly Detection using baselining and statistical analysis.
- Case Study: Analyzing a compromised host's network traffic to identify Command and Control (C2) communication and the data exfiltration channel.

Module 6: Wireless, Mobile, and IoT Security

- Securing Enterprise Wireless Networks by configuring WPA3, disabling legacy protocols, and using Network Access Control.
- Implementing Mobile Device Management and Mobile Application Management (MAM) policies for corporate and BYOD devices.
- Identifying and mitigating unique threats and vulnerabilities in IoT and SCADA/OT environments.
- Implementing secure network access controls and micro-segmentation for connected devices.
- Case Study: Responding to a security incident involving unauthorized access to an internal network via a poorly secured corporate IoT device.

Module 7: Incident Response and Digital Forensics

- Executing the complete Incident Response Lifecycle.
- Developing and testing a clear Communication Plan and defining roles during a major security incident.
- Performing initial Digital Forensics on compromised systems, including volatile data collection and maintaining the Chain of Custody.
- Implementing quick containment strategies, such as network isolation and process termination, to limit damage.
- Case Study: Leading a simulated ransomware incident response, including forensic data collection, decryption, and full system recovery.

Module 8: Business Continuity, Disaster Recovery, and Policy

- Developing comprehensive Business Continuity Plans and Disaster Recovery Plans.
- Implementing and testing data Backup and Restoration strategies, including offsite and immutable storage.
- Designing and implementing foundational Security Policies
- Conducting Risk Assessment and Threat Modeling to prioritize defensive efforts and resource allocation.
- Case Study: Creating a full BCP and DRP following a simulated environmental disaster that took a primary data center offline, focusing on RTO and RPO metrics.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com