Network Defense Essentials (NDE) 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 rapid proliferation of digital transformation and the escalating sophistication of cyber threats have made foundational Network Security a mission-critical skill for every IT professional. The Network Defense Essentials (NDE) course is your gateway to mastering the core principles of protecting modern network infrastructures. Network Defense Essentials (NDE) Training Course provides a holistic overview of essential defensive strategies, focusing heavily on practical, hands-on experience to prepare learners for real-world challenges in the field of Information Security. You will delve into core concepts like Access Control, Security Policies, and crucial Technical Controls such as firewalls, IDS/IPS, and SIEM (Security Information and Event Management).

This cutting-edge training course is meticulously structured to build job-ready competencies, ensuring participants can effectively implement, monitor, and defend against the latest network attacks. Beyond traditional network components, the curriculum incorporates trending topics like Cloud Security, IoT Device Security, and advanced Data Security measures, including Cryptography and Data Loss Prevention (DLP). With a strong emphasis on practical labs and real-world case studies, NDE equips aspiring Security Analysts and IT administrators with the knowledge to maintain network resilience and safeguard critical digital assets in an ever-evolving threat landscape.

Programme Curriculum

Network Defense Essentials (NDE) Training Course

Introduction

The rapid proliferation of digital transformation and the escalating sophistication of cyber threats have made foundational Network Security a mission-critical skill for every IT professional. The Network Defense Essentials (NDE) course is your gateway to mastering the core principles of protecting modern network infrastructures. Network Defense Essentials (NDE) Training Course provides a holistic overview of essential defensive

strategies, focusing heavily on practical, hands-on experience to prepare learners for real-world challenges in the field of Information Security. You will delve into core concepts like Access Control, Security Policies, and crucial Technical Controls such as firewalls, IDS/IPS, and SIEM (Security Information and Event Management).

This cutting-edge training course is meticulously structured to build job-ready competencies, ensuring participants can effectively implement, monitor, and defend against the latest network attacks. Beyond traditional network components, the curriculum incorporates trending topics like Cloud Security, IoT Device Security, and advanced Data Security measures, including Cryptography and Data Loss Prevention (DLP). With a strong emphasis on practical labs and real-world case studies, NDE equips aspiring Security Analysts and IT administrators with the knowledge to maintain network resilience and safeguard critical digital assets in an ever-evolving threat landscape.

Course Duration

5 days

Course Objectives

Upon completion, learners will be able to:

1. Analyze the current cyber threat landscape and apply core Information Assurance (IA) principles to a network.
2. Implement robust Identity and Access Management (IAM) concepts, including authentication and authorization mechanisms.
3. Develop and enforce effective Administrative Controls such as security policies, regulatory frameworks, and compliance adherence.
4. Design and maintain Physical Security Controls to protect network infrastructure from environmental and insider threats.
5. Configure and manage foundational Technical Controls, including firewalls, IDS/IPS, and proxy servers.
6. Understand and secure Network Segmentation principles to limit the scope of network breaches.
7. Deploy and optimize a Virtual Private Network (VPN) for secure remote access and data transmission.
8. Explain the fundamentals of Virtualization and apply essential Cloud Security best practices.
9. Secure common Wireless Networks by implementing strong encryption protocols and security measures.
10. Identify and mitigate specific IoT Device Security and Mobile Security risks within a corporate environment.
11. Implement Cryptography techniques, including PKI (Public Key Infrastructure), for data protection in transit and at rest.
12. Establish protocols for Data Security, including backup strategies and Data Loss Prevention (DLP) controls.
13. Perform continuous Network Traffic Monitoring and Incident Response using tools like Wireshark and SIEM for suspicious activity analysis.

Target Audience

1. Aspiring Cybersecurity Professionals
2. IT Technicians/Help Desk Staff
3. Network Administrators
4. Junior Security Analysts (SOC Tier 1)
5. System Administrators
6. IT Audit and Compliance Professionals
7. Career Changers seeking a foundational security certification

8. Students in Information Technology or Computer Science

Course Modules

Module 1: Network Security Fundamentals & Information Assurance

- Key issues plaguing network security and defining the threat landscape.
- Understanding and applying Information Assurance principles
- Overview of essential network security protocols
- Network Defense Approaches and best practices for hardening a network.
- Introduction to network security controls
- Case Study: The Maersk NotPetya Attack.

Module 2: Access Control & Identity Management (IAM)

- Principles, terminologies, and models of Access Control
- Core concepts of Identification, Authentication, and Authorization.
- Implementing Identity and Access Management solutions.
- Different types of authentication methods and managing user accounts.
- Security risks associated with poor access control and common vulnerabilities.
- Case Study: The Colonial Pipeline Breach.

Module 3: Administrative and Physical Controls

- Overview of Regulatory Frameworks and Acts governing security.
- Designing and developing robust Security Policies and procedures.
- Conducting effective Security Awareness Training for employees.
- Importance and implementation of Physical Security Controls
- Workplace security and environmental controls to protect hardware.
- Case Study: The Target Data Breach.

Module 4: Technical Controls: Perimeter Defense

- Fundamentals of Network Segmentation and its use in risk reduction.
- Functionality, types, and configurations of Firewalls
- Deployment and management of Intrusion Detection/Prevention Systems
- Understanding Proxy Servers and Honeypots for threat deception.
- Implementing and securing Virtual Private Networks
- Case Study: A Major Financial Institution's DDoS Mitigation.

Module 5: Virtualization and Cloud Security

- Essential concepts of Virtualization and securing virtual machines.
- Fundamentals of Cloud Computing
- Key security concerns and shared responsibility models in the Cloud.
- Implementing Cloud Security best practices and configuration hardening.
- Introduction to Cloud Identity and Access Management and network security groups.
- Case Study: The Capital One Data Breach.

Module 6: Wireless, Mobile, and IoT Device Security

- Fundamentals of Wireless Networks and common encryption mechanisms

- Securing wireless access points and preventing unauthorized access.
- Risks and security measures for Mobile Devices
- Working of IoT Devices, application areas, and communication models.
- Implementing security best practices for IoT Security in an enterprise.
- Case Study: The Casino Fish Tank Hack.

Module 7: Cryptography and Data Security

- Introduction to Cryptography Techniques and algorithms
- Concepts and implementation of Public Key Infrastructure
- Importance of Data Security and security controls for data encryption.
- Strategies for Data Backup and Retention
- Understanding and deploying Data Loss Prevention concepts.
- Case Study: The Equifax Breach.

Module 8: Network Traffic Monitoring & Incident Response

- Need and advantages of Network Traffic Monitoring and establishing a baseline.
- Using tools like Wireshark to capture and analyze network packets.
- Analyzing common network traffic signatures for suspicious activity.
- Introduction to Security Information and Event Management and User Behavior Analytics
- Foundational steps of Incident Response and handling security alerts.
- Case Study: A Zero-Day Exploit Detection.

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.com 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
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100
05 Oct 2026	09 Oct 2026	Online	$1,100
12 Oct 2026	16 Oct 2026	Online	$1,100
19 Oct 2026	23 Oct 2026	Online	$1,100
26 Oct 2026	30 Oct 2026	Online	$1,100

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

Register Online Now

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