Certified Network Defense

Course Duration: 40 Hrs. **Course code: C|NDv3**

Course Overview

The EC-Council Certified Network Defender (CND) course is a comprehensive, hands-on program designed to equip network administrators with the skills to defend, detect, and respond to network attacks, focusing on a "protect, detect, and respond" approach to network security.

What you'll learn?

- **Network Security Management:**
  Learn how to develop and implement security policies, procedures, and best practices for secure network architecture.
- **Perimeter and Endpoint Protection:**
  Understand how to secure network boundaries, endpoints, and applications with firewalls, intrusion detection/prevention systems (IDS/IPS), and other security tools.
- **Virtual and Cloud Security:**
  Gain knowledge of securing virtualized environments, cloud infrastructure, and wireless networks.
- **Incident Detection and Response:**
  Learn how to identify, analyze, and respond to security incidents, including forensic investigation and business continuity planning.

Target Audience

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

- **Network Administrators:**
  Individuals responsible for the day-to-day management and maintenance of network infrastructure.
- **Network Security Administrators:**
  Professionals focused on securing network infrastructure and implementing security policies.
- **Network Security Engineers:**
  Engineers who design, implement, and maintain network security systems.
- **Network Defense Technicians:**
  Technicians specializing in network security technologies and operations.

Pre-Requisites

Candidates should have a foundational understanding of networking concepts, including:

- Network security threats, vulnerabilities, and attacks.
- Network security controls, protocols, and devices.
- Network security policy design and implementation.
- Basic IT security concepts.

Course content

Module 01: Network Attacks and Defense Strategies

A. Explain essential terminologies related to network security attacks.
B. Describe the various examples of network-level attack techniques.
C. Describe the various examples of application-level attack techniques.
D. Describe the various examples of social engineering attack techniques.
E. Describe the various examples of email attack techniques.
F. Describe the various examples of mobile device-specific attack techniques.
G. Describe the various examples of cloud-specific attack techniques.
H. Describe the various examples of wireless network-specific attack techniques.
I. Describe the various examples of Supply Chain Attack techniques.
J. Describe Attacker's Hacking Methodologies and Frameworks
K. Understand fundamental goal, benefits, and challenges in network defense.

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

L. Explain Continual/Adaptive security strategy.
M. Explain defense-in-depth security strategy.

Module 02 Administrative Network Security

A. Learn to obtain compliance with regulatory framework and standards.
B. Discuss various Regulatory Frameworks, Laws, and Acts
C. Learn to design and develop security policies.
D. Learn to conduct different type security and awareness training.
E. Learn to implement other administrative security measures.
F. Discuss Asset Management
G. Learn How to Stay Up to Date on Security Trends and Threats

Module 03: Technical Network Security

A. Discuss access control principles, terminologies, and models.
B. Redefine the Access Control in Today's Distributed and Mobile Computing World
C. Discuss Identity and Access Management (IAM)
D. Discuss cryptographic security techniques.
E. Discuss various cryptographic algorithms.
F. Discuss security benefits of network segmentation techniques.
G. Discuss various essential network security solutions.
H. Discuss various essential network security protocols.

Module 04 Network Perimeter Security

A. Understand firewall security concerns, capabilities, and limitations.
B. Understand different types of firewall technologies and their usage.
C. Understand firewall topologies and their usage.
D. Distinguish between hardware, software, host, network, internal, and external firewalls.
E. Select firewalls based on its deep traffic inspection capability.
F. Discuss firewall implementation and deployment process.
G. Discuss recommendations and best practices for secure firewall Implementation and deployment.

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

H. Discuss firewall administration concepts.
I. Understand role, capabilities, limitations, and concerns in IDS deployment.
J. Discuss IDS classification.
K. Discuss various components of IDS.
L. Discuss effective deployment of network and host-based IDS.
M. Learn to how to deal with false positive and false negative IDS/IPS alerts.
N. Discuss the considerations for selection of an appropriate IDS/IPS solutions.
O. Discuss various NIDS and HIDS Solutions with their intrusion detection capabilities Snort.
P. Discuss router and switch security measures, recommendations, and best practices.
Q. Leverage Zero Trust Model Security using Software-Defined Perimeter (SDP)

Module 05 Endpoint Security-Windows Systems

A. Understand Window OS and Security Concerns
B. Discuss Windows Security Components
C. Discuss Various Windows Security Features
D. Discuss Windows Security Baseline Configurations
E. Discuss Windows User Account and Password Management
F. Discuss Windows Patch Management
G. Discuss User Access Management
H. Windows OS Security Hardening Techniques
I. Discuss Windows Active Directory Security Best Practices
J. Discuss Windows Network Services and Protocol Security

Module 06 Endpoint Security-Linux Systems

A. Understand Linux OS and security concerns.
B. Discuss Linux Installation and Patching
C. Discuss Linux OS Hardening Techniques
D. Discuss Linux User Access and Password Management
E. Discuss Linux Network Security and Remote Access
F. Discuss Various Linux Security Tools and Frameworks

Module 07 Endpoint Security- Mobile Devices

A. Common Mobile Usage Policies in Enterprises
B. Discuss Security Risk and Guidelines associated with Enterprises mobile usage policies.
C. Discuss and implement various enterprise-level mobile security management Solutions.
D. Discuss and implement general security guidelines and best practices on Mobile platforms.
E. Discuss Security guidelines and tools for Android devices.
F. Discuss Security guidelines and tools for iOS devices.

Module 08 Endpoint Security-IoT Devices

A. Understanding IoT Devices, their need, and Application Areas
B. Understanding IoT Ecosystem and Communication models
C. Understand Security Challenges and risks associated with IoT-enabled environments.
D. Discuss the security in IoT-enabled environments.
E. Discuss Security Measures for IoT enabled IT Environments
F. Discuss IoT Security Tools and Best Practices
G. Discuss and refer various standards, Initiatives and Efforts for IoT Security

Module 09 Administrative Application Security

A. Discuss and implement Application Whitelisting and Blacklisting
B. Discuss and implement application Sandboxing.
C. Discuss and implement Application Patch Management
D. Discuss and implement Web Application Firewall (WAF)

Module 10: Data Security

A. Understand data security and its importance.
B. Understand Data Integrity and Its Importance
C. Discuss the implementation of data access controls.
D. Discuss the implementation of Encryption of Data at rest.

E. Discuss the implementation of Encryption of "Data at transit.
F. Discuss Data Masking Concepts
G. Discuss data backup and retention.
H. Discuss Data Destruction Concepts
I. Data Loss Prevention Concepts

Module 11: Enterprise Virtual Network Security

A. Discuss the evolution of network and security management concept in modern Virtualized IT Environments
B. Understand Virtualization Essential Concepts
C. Discus Network Virtualization (NV) Security
D. Discuss SDN Security
E. Discuss Network Function Virtualization (NFV) Security
F. Discus OS Virtualization Security
G. Discuss Security Guidelines, Recommendations and Best Practices for Containers
H. Discuss Security Guidelines, Recommendations and Best practices for Dockers.
I. Discuss Security Guidelines, Recommendations and Best Practices for Kubernetes

Module 12: Enterprise Cloud Security

A. Understand Cloud Computing Fundamentals
B. Understanding the Insights of Cloud Security
C. Evaluate CSP for Security before Consuming Cloud Service
D. Discuss security in Amazon Cloud (AWS)
E. Discuss security in Microsoft Azure Cloud
F. Discuss security in Google Cloud Platform (GCP)
G. Discuss general security best practices and tools for cloud security.

Module 13: Wireless Network Security

A. Understand wireless network fundamentals.
B. Understand wireless network encryption mechanisms.

C. Understand wireless network authentication methods.
D. Discuss and implement wireless network security measures.

Module 14: Network Traffic Monitoring and Analysis

A. Understand the need and advantages of network traffic monitoring.
B. Setting up the environment for network monitoring
C. Determine baseline traffic signatures for normal and suspicious network traffic.
D. Perform network monitoring and analysis for suspicious traffic using Wireshark.
E. Discuss network performance and bandwidth monitoring tools and techniques.
F. Understand Network Anomaly Detection with Behavior analysis.

Module 15: Network Logs Monitoring and Analysis

A. Understand logging concepts.
B. Discuss log monitoring and analysis on Windows systems.
C. Discuss log monitoring and analysis on Linux.
D. Discuss log monitoring and analysis on Mac.
E. Discuss log monitoring and analysis in Firewall.
F. Discuss log monitoring and analysis on Routers.
G. Discuss log monitoring and analysis on Web Servers
H. Discuss centralized log monitoring and analysis.

Module 16 Incident Response and Forensic Investigation

A. Understand incident response concept.
B. Understand the role of first responder in incident response.
C. Discuss Do's and Don'ts in first response.
D. Describe incident handling and response process.
E. Enhance Incident-Response using AI/ML
F. Learn how to Automate Incident Response - SOAR
G. Understand Incident Response using Endpoint Detection and Response (EDR)

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

H. Understanding Incident Response using Extended Detection and Response (XDR)
I. Describe forensics investigation process.

Module 17 Business Continuity and Disaster Recovery

A. Introduction to Business Continuity (BC) and Disaster Recovery (DR) concepts
B. Discuss BC/DR Activities
C. Explain Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)
D. Discuss BC/DR Standards

Module 18 Risk Anticipation with Risk Management

A. Understand risk management concepts.
B. Learn to manage risk though risk management program.
C. Learn different Risk Management Frameworks (RMF)
D. Learn to manage vulnerabilities through vulnerability management program.
E. Learn vulnerability Assessment and Scanning
F. Discuss Privacy Impact Assessment (PIA)

Module 19 Threat Assessment with Attack Surface Analysis

A. Understand the attack surface concepts.
B. Learn to understand and visualize your attack surface.
C. Learn to identify Indicators of Exposures (IoE)
D. Learn to perform attack simulation.
E. Learn to reduce the attack surface.
F. Understand Attack surface monitoring tools.
G. Discuss attack surface analysis specific to Cloud and IoT

Module 20 Threat Prediction with Cyber Threat Intelligence

A. Understand role of cyber threat intelligence in network defense
B. Understand the types of threat Intelligence.
C. Understand the Indicators of Threat Intelligence: Indicators of Compromise (IoCs) and Indicators of Attack (IoA)

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

D. Understand the layers of Threat Intelligence
E. Learn to leverage/consume threat intelligence for proactive defense.
F. Understand threat Hunting.
G. Discuss Leveraging AI/ML capabilities for threat intelligence.

Exam Preference

Exam Code	312-38
Number Of Questions	100
Length Of Test	100 Minutes