

THE ULTIMATE CERTIFICATION FOR NETWORK ADMINISTRATORS

CND

Certified Network Defender

IF YOUR IT CREW IS NOT INTO
SECURITY,
YOU JUST WON'T HAVE
SECURITY

PROTECT - DETECT - RESPOND.



EC-Council

CERTIFIED NETWORK DEFENDER



Course Description

Certified Network Defender (CND) is a vendor-neutral, hands-on, instructor-led comprehensive network security certification training program. It is a skills-based, lab intensive program based on a job-task analysis and cybersecurity education framework presented by the National Initiative of Cybersecurity Education (NICE). The course has also been mapped to global job roles and responsibilities and the Department of Defense (DoD) job roles for system/network administrators. The course is designed and developed after extensive market research and surveys.

The program prepares network administrators on network security technologies and operations to attain Defense-in-Depth network security preparedness. It covers the protect, detect and respond approach to network security. The course contains hands-on labs, based on major network security tools and techniques which will provide network administrators real world expertise on current network security technologies and operations. The study-kit provides you with over 10 GB of network security best practices, assessments and protection tools. The kit also contains templates for various network policies and a large number of white papers for additional learning.

Course Duration: 5 days

Time: 9.00 AM to 5.00 PM

Exam details:

**Exam title:**

Certified Network Defender (CND)

**Exam code:**

312-38

**Number of questions:**

100

**Duration:**

4 Hours

**Availability:**

ECCEXAM

**Test Format:**

Interactive Multiple Choice Questions

What will you learn?

Student will learn about various network security controls, protocols, and devices

Student will be able to determine appropriate location for IDS/IPS sensors, tuning IDS for false positives and false negatives, and configurations to harden security through IDPS technologies

Students will be able to troubleshoot their network for various network problems

Students will be able to implement secure VPN implementation for their organization

Student will be able to identify various threats on organization network

Student will be able to identify various threats to wireless network and learn how to mitigate them

Student will learn how to design and implement various security policies for their organizations

Student will be able to monitor and conduct signature analysis to detect various types of attacks and policy violation activities.

Student will learn the importance of physical security and be able to determine and implement various physical security controls for their organizations

Student will be able to perform risk assessment, vulnerability assessment/scanning through various scanning tools and generate detailed reports on it

Student will be able to harden security of various hosts individually in the organization's network

Student will be able to identify the critical data, choose appropriate backup method, media and technique to perform successful backup of organization data on regular basis

Student will be able to choose appropriate firewall solution, topology, and configurations to harden security through firewall

Student will be able to provide first response to the network security incident and assist IRT team and forensics investigation team in dealing with an incident.

Why Certified Network Defender?



Organizational focus on cyber defense is more important than ever as cyber breaches have a far greater financial impact and can cause broad reputational damage.

Despite best efforts to prevent breaches, many organizations are still being compromised. Therefore organizations must have, as part of their defense mechanisms, trained network engineers who are focused on protecting, detecting, and responding to the threats on their networks.

Network administrators spend a lot of time with **network environments**, and are familiar with network components, traffic, performance and utilization, network topology, location of each system, security policy, etc.

So, organizations can be much better in defending themselves from vicious attacks if the IT and network administrators are equipped with adequate network security skills. Thus Network administrators can play a significant role in network defense and become first line of defense for any organizations.

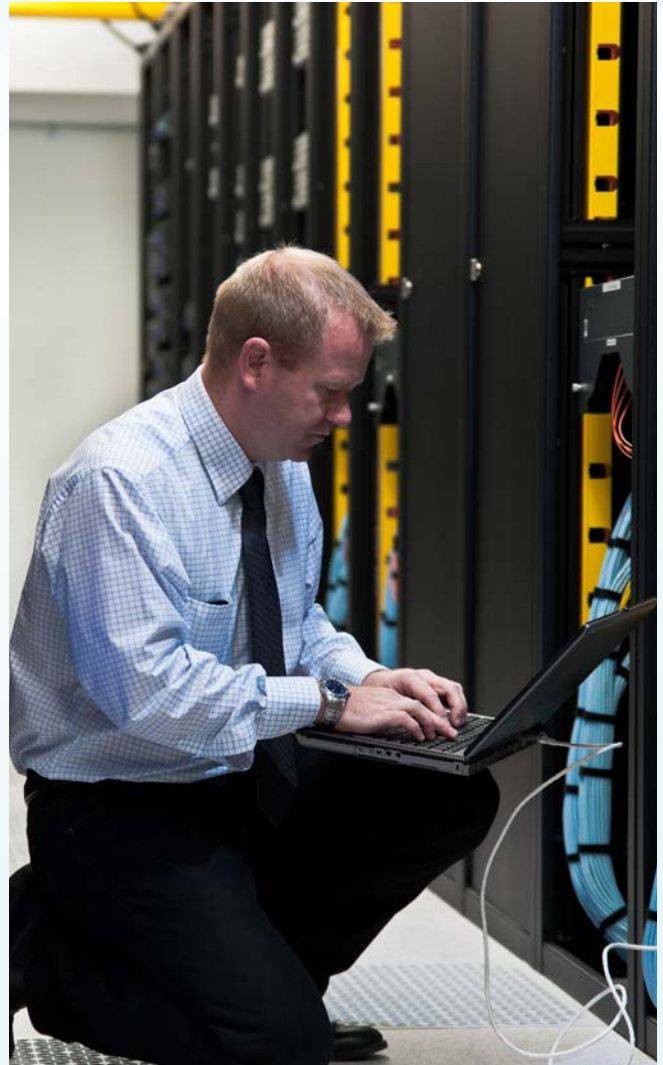
“While there will be over 1.5 million cyber security jobs that remain unfilled by 2019, millions of IT and Network administrators remain untrained on network defense techniques”

***- Michael Brown, CEO at Symantec,
the world's largest security software vendor.***

There is no proper tactical network security training that is made available for network administrators which provides them core network security skills.

Students enrolled in the Certified Network Defender course, will gain a detailed understanding and hands on ability to function in real life situations involving network defense. They will gain the technical depth required to actively design a secure network in your organization. This program will be akin to learning math instead of just using a calculator. This course gives you the fundamental understanding of the true construct of data transfer, network technologies, software technologies so that you understand how networks operate, understand what software is automating and how to analyze the subject material.

You will learn how to protect, detect and respond to the network attacks. You will learn network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN and firewall configuration. You will then learn the intricacies of network traffic signature, analysis and vulnerability scanning which will help you when you design greater network security policies and successful incident response plans. These skills will help you foster resiliency and continuity of operations during attacks.



“Cyber Security is commonly the first thing on the minds of CIO but is, in many cases, an after thought for the IT department”

***- Jay Bavisi
President, EC-Council***

[illegible]

Source: <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

What are the Domains of CND?

Module 01

Computer Network and Defense Fundamentals

Module 02

Network Security Threats, Vulnerabilities, and Attacks

Module 03

Network Security Controls, Protocols, and Devices

Module 04

Network Security Policy Design and Implementation

Module 05

Physical Security

Module 06

Host Security

Module 07

Secure Firewall Configuration and Management

Module 08

Secure IDS Configuration and Management

Module 09

Secure VPN Configuration and Management

Module 10

Wireless Network Defense

Module 11

Network Traffic Monitoring and Analysis

Module 12

Network Risk and Vulnerability Management

Module 13

Data Backup and Recovery

Module 14

Network Incident Response and Management

Who Is It For?

**Network
Administrators**

**Network security
Administrators**

**Network Security
Engineer**

**Network Defense
Technicians**

CND Analyst

Security Analyst

Security Operator

**Anyone who
involves in network
operations**

What job roles would need the CND specific skills?

MAPPING SUMMARY

I/A Framework Categories	I/A Framework Specialty Areas	EC-Council Certification	Estimated Framework Proficiency Level Match (1-4)	C3 Relation Category
Securely Provision				
Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems	Information Assurance (IA) Compliance	CND	2	Related
	Software Assurance and Security Engineering	ECSP	2	Related
	Systems Security Architecture	CND	3	Related
	Technology Research and Development	CND	3	Related
	System Requirements Planning	CND	2	Related
	Test and Evaluation	CND	3	Related
	Systems Development	CND	2	Related
Operate & Maintain				
Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.	Data Administration	N/A		
	Knowledge Management	N/A		
	Customer Service and Technical Support	CND	3	Specialist
	Network Services	CND	3	Related
	System Administration	CND	3	Specialist
	Systems Security Analysis	CND	3	Specialist

I/A Framework Categories	I/A Framework Specialty Areas	EC-Council Certification	Estimated Framework Proficiency Level Match (1-4)	C3 Relation Category
Protect and Defend				
Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.	Computer Network Defense (CND) Analysis	CEH	2	Related
	Incident Response	ECIH	3	Related
	Computer Network Defense (CND) Infrastructure Support	CND	3	Specialist
	Vulnerability Assessment and Management	ECSA/LPT	3	Specialist
Investigate				
Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.	Investigation	CHFI	4	Specialist
	Digital Forensics	CHFI	3	Specialist
Collect and Operate				
Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.	Collection Operations	ECSA/LPT	2	Related
	Cyber Operations Planning	CND	3	Specialist
	Cyber Operations	ECSA/LPT	3	Specialist

I/A Framework Categories	I/A Framework Specialty Areas	EC-Council Certification	Estimated Framework Proficiency Level Match (1-4)	C3 Relation Category
Analyze				
Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.	Threat Analysis	ECSA/LPT	3	Specialist
	Exploitation Analysis	CHFI	3	Specialist
	Targets	ECSA/LPT	2	Related
	All Source Intelligence	ECSA/LPT	2	Related
Oversight and Development				
Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.	Legal Advice and Advocacy	CCISO	3	Specialist
	Education and Training	CEI	3	Related
	Strategic Planning and Policy Development	CCISO	3	Specialist
	Information Systems Security Operations (ISSO)	CCISO	4	Specialist
	Security Program Management (CISO)	CCISO	3	Related



EC-Council
www.eccouncil.org