C|ND: THE CREDENTIAL THAT SETS THE GLOBAL BENCHMARK FOR NETWORK SECURITY SKILLS AND BUILDS CAREERS IN NETWORK SECURITY & BLUE TEAM
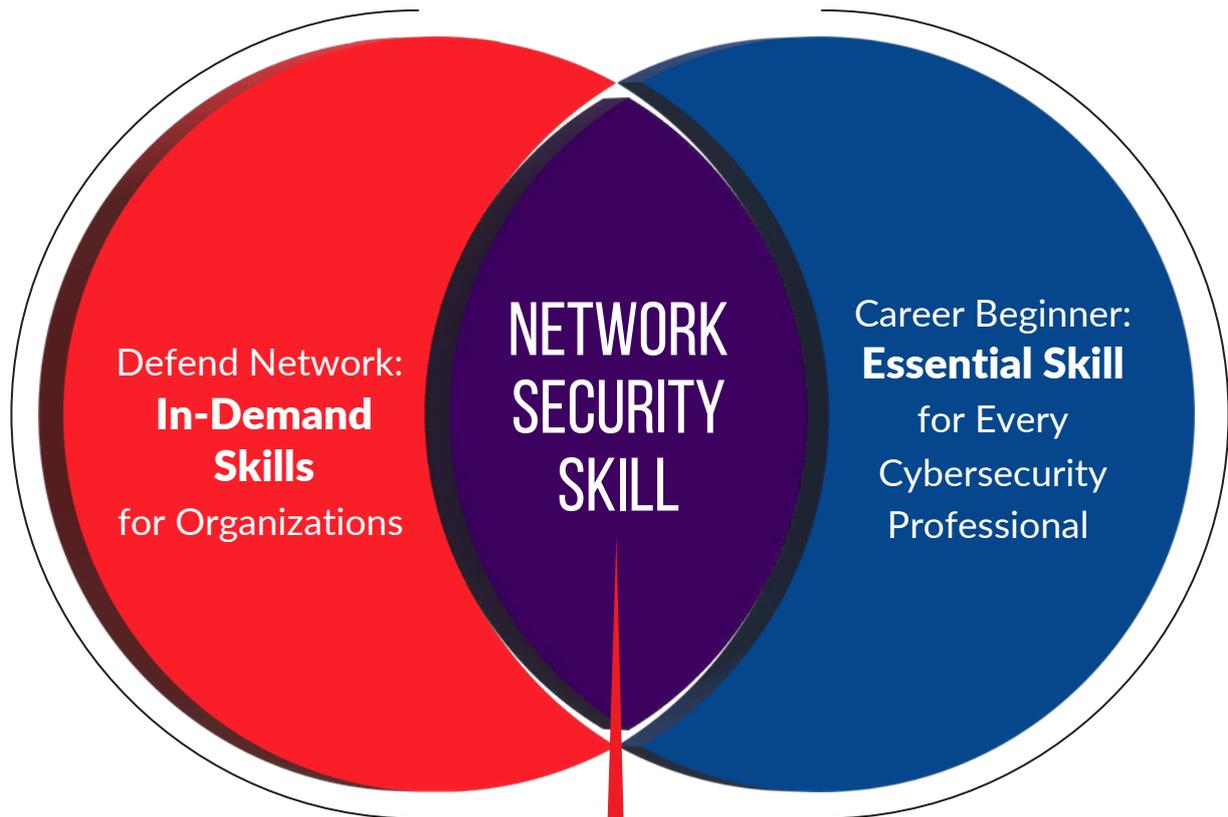
Network security skills are in high demand among organizations as well as cybersecurity aspirants.

1. HIGHLY SOUGHT AFTER BY ORGANIZATIONS:

The increasing frequency and sophistication of cyberattacks have contributed to a growing demand for network security professionals. Network security is a critical aspect of cybersecurity, as protecting data integrity, confidentiality, and availability within networks is a top priority for organizations.

2. ESSENTIAL FUNDAMENTAL SKILL:

Mastering network security is an essential fundamental skill for aspiring cybersecurity professionals as it entails fortifying firewalls, implementing robust encryption protocols, and configuring intrusion detection systems-foundational elements vital to securing the intricate web of interconnected systems against sophisticated cyber threats, ensuring data integrity, confidentiality, and seamless network operations.

C|ND
Certified Network Defender

EC-Council
Building A Culture Of Security

Defend Network:
In-Demand Skills
for Organizations

NETWORK
SECURITY
SKILL

Career Beginner:
Essential Skill
for Every
Cybersecurity
Professional

CERTIFIED NETWORK DEFENDER

**World's Most Comprehensive &
Practical Network Security
Training Program**
Network Security is one of
the Top In-Demand Cybersecurity Skills.
(TechTarget, LinkedIn, Shiksha, Harvard blog, EC-Council)

C|ND
Certified | Network Defender

EC-Council
Building A Culture Of Security

WHAT IS THE

EC-COUNCIL CERTIFIED NETWORK DEFENDER

(C|ND) PROGRAM?

EC-Council's Certified Network Defender (C|ND) is an essential vendor-neutral network security certification for every IT and systems administrator who needs to operate with a secure mindset.

Students will learn the critical skills required to defend their networks and operating environments across local networks, endpoints, cloud infrastructure, applications, OT, and Mobile. They will also acquire knowledge of effective proper log analysis, network traffic monitoring, basic investigation and response, as well as business continuity and disaster recovery. Additionally, they will dive into threats, analyzing the attack surface, and studying threat prediction and threat intelligence as it relates to their administration and defense responsibilities. Often referred to as blue-teaming, C|NDs will be able to apply defense and countermeasure strategies in their organizations, playing a critical role not only in attack prevention but also in detection, response, and remediation as they configure networks and systems to operate securely. The C|ND program will cover the concepts and fortify skills through hands-on practice across over 100+ labs delivered on live target machines.

The C|ND program designed by industry experts prepares network defenders with strategic, technological, and operational network security capabilities, enabling them to design, develop, and maintain secure networks.
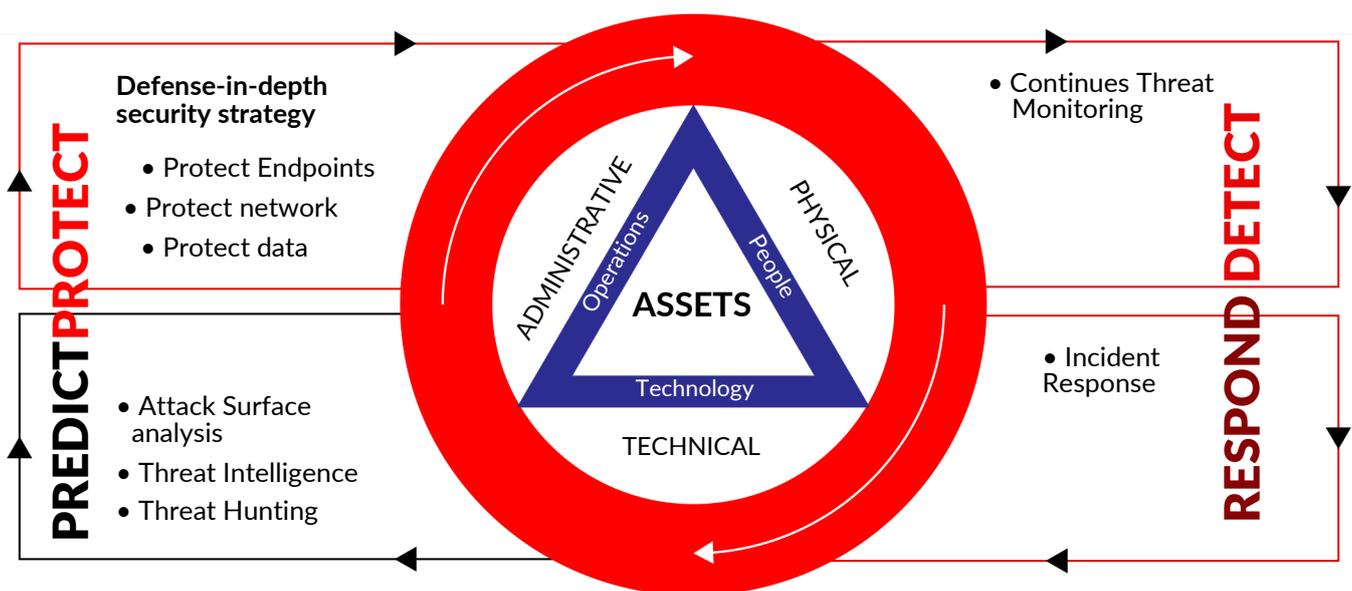
C|ND
Certified | Network Defender

EC-Council
Building A Culture Of Security

C|ND IS THE WORLD'S FIRST

NETWORK SECURITY PROGRAM

WITHACONTINUAL/ADAPTIVESECURITY STRATEGY:

1.Protect 2. Detect 3. Respond 4. Predict

According to Gartner, 'traditional "prevent and detect" approaches are inadequate.' Opportunistic by nature, malicious actors look for the easiest ways to attack most users and siphon off maximum gains. Developing a continuous Adaptive Security Cycle helps organizations stay ahead of cybercriminals by creating and improving security systems. And that's what you learn in the **C|ND** program.

PREDICT **PROTECT**

Defense-in-depth security strategy

- Protect Endpoints
- Protect network
- Protect data

- Attack Surface analysis
- Threat Intelligence
- Threat Hunting

ADMINISTRATIVE
PHYSICAL
Operations
People
ASSETS
Technology
TECHNICAL

RESPOND **DETECT**

- Continues Threat Monitoring

- Incident Response

EC-Council
Building A Culture Of Security

C|ND
Certified Network Defender

C|ND Course Modules:

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

WHAT WILL YOU LEARN?

1. Planning and administering network security for organizations

2. Recognizing security risks, threats, and vulnerabilities

3. Ensuring compliance with regulatory standards

4. Designing and implementing network security policies

5. Applying security principles in distributed and mobile computing environment

6. Implementing Identity and Access Management, encryption, and network segmentation

7. Managing Windows and Linux Security Administration

8. Addressing security risks in mobile devices and IoT

9. Implementing strong data security techniques

10. Managing security in virtualization technologies and cloud platforms

11. Implementing wireless network security

12. Conducting risk and vulnerability assessments

13. Providing first response to security incidents

14. Identifying Indicators of Compromise and Attack

15. Integrating threat intelligence for proactive defense

16. Conducting Attack Surface Analysis

17. Assisting in Business Continuity and Disaster Recovery planning

18. Monitoring network traffic and performing log management

19. Managing proxy, content filtering, and troubleshooting network issues

20. Hardening security of endpoints and selecting firewall solutions

21. Configuring IDS/IPS for enhanced security

22. Maintaining an inventory of network devices

23. Providing security awareness guidance and training

24. Managing AAA for network devices

25. Reviewing audit logs and analyzing security anomalies

26. Maintaining and configuring security platforms

27. Evaluating security products and operations procedures

28. Identifying and classifying organizational assets

29. Implementing system integrity monitoring tools

30. Understanding EDR/XDR and UEBA solutions

31. Conducting PIA processes for privacy assessment

32. Collaborating on threat hunting and incident response

33. Understanding SOAR platforms in cybersecurity operations

34. Integrating Zero Trust principles into security architectures

35. Staying updated on emerging cyber threats

36. Understanding the role of AI/ML in cyber defense.

4 KEY FEATURES

AND CRITICAL COMPONENTS OF
THE C|ND PROGRAM

1 | **The World's First Network Security Program with**

1. Protect 2. Detect 3. Respond 4. Predict

2 | **Covers Defense-In-Depth Security Strategy:**

1. Policies, Procedures, and Awareness 2. Physical 3. Perimeter
4. Internal Network 5. Host 6. Application 7. Data

3 | **Covers Four Security Approaches:**

1. Preventive Approach 2. Reactive Approach
3. Retrospective Approach 4. Proactive Approach

4 | **Covers All Five Functions of the NIST**

1. Identify 2. Protect 3. Detect 4. Respond 5. Recover

C|ND
Certified | Network Defender

EC-Council
Building A Culture Of Security

BUILD YOUR NETWORK SECURITY CAREER WITH C|ND

Advantages of the C|ND Program

- Accredited by the ANSI National Accreditation Board under ANSI ISO/IEC 17024

- Approved by the US DoD under Directive 8570/8140

- Recognized by the National Cyber Security Centre NCSC – part of GCHQ (UK's intelligence, security, and cyber agency) approves EC-Council Training as meeting CYBOK requirements.

- 100+ hands-on labs: More labs than any globally recognized network security certification.

- Lab-intensive program (More than 50% lab)

- Covers modern and advanced network security requirements

- Mapped with NICE Framework under the following category, specialty areas, and work roles

- Your pathway to a career in the blue team

- Master mobile & IoT security defense

- Learn tactical defense of cloud services (AWS, Azure, and GCP)

- Learning beyond technical aspects

- Building perimeter defense skills

- Build job-ready practical skills in live ranges

- Learn the latest technologies and concepts to match modern network security requirements.

- Build hands-on skills with 100+ labs simulating real-time environment

- Learn in-depth attack surface analysis

- Mapped with real-time job roles and responsibilities of network defenders

- Designed and developed by SMEs across the globe

C|ND Certified Network Defender

EC-Council Building A Culture Of Security

C|ND COVERS MODERN AND ADVANCED NETWORK

SECURITY REQUIREMENTS:

- Enterprise Mobile Device Security
- Enterprise IoT Device Security
- Cloud Security
- Virtual Network Security
- SDN Security
- NFV Security
- Docker Security
- Container Security

- Kubernetes Security
- Threat Intelligence
- Threat Hunting
- Endpoint Detection and Response (EDR)
- Extended detection and response (XDR)
- User and Entity Behavior Analytics (UEBA)
- Security Orchestration, Automation, and Response (SOAR)

TRAINING AND EXAM DETAILS

Training Details:

iLearn (Self-Study)

This solution is an asynchronous, self-study environment in a video streaming format.

iWeek (Live Online)

This solution is a live, online, instructor-led training course.

Training Partner (In Person)

This solution offers "in-person" training so what you can benefit from collaborating with your peers and gaining real-world led by expert, certified instructors.

Exam Details:

Exam Code:	Duration:	Availability:	Test Format:
312-38	4 hours	EC-Council Exam Portal	Multiple Choice

C|ND
Certified | Network Defender

EC-Council
Building A Culture Of Security

JOB ROLES WITH C|ND

C|ND is a network security course designed to help organizations create and deploy the most comprehensive network security system. C|ND is mapped to the below job roles based on common job role frameworks recognized by organizations worldwide. C|NDis a network security course designed to help organizations create and deploy the most comprehensive network defense system.

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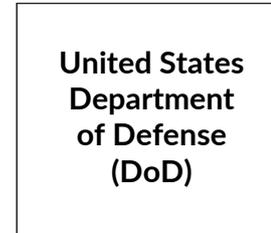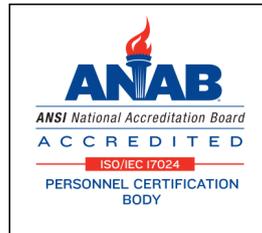- Network Security

Who Can Apply?

Students/IT Professionals/Any other industry professionals planning a career in cybersecurity. Anyone who wants to start a career in the blue team and network security.

Salaries

The average salary for a network security engineer in the
United States is $125,014.

C|ND
Certified Network Defender

EC-Council
Building A Culture Of Security

RECOGNITION/ENDORSEMENT/ MAPPING

NICE

100% mapping to NICE Workforce Framework for Cybersecurity

ANAB
ANSI National Accreditation Board
A C C R E D I T E D
ISO/IEC I7024
PERSONNEL CERTIFICATION BODY

United States Department of Defense (DoD)

Why Do Top Network Security Professionals Across the Globe Love the C|ND Program?

Robinson Shai

South Africa

Cybersecurity
Professional

Other programs emphasize the understanding of networks, but C|ND shows the weaknesses in a network and how to cover them to protect the networks. C|ND is the single most certification that pays so much attention to security. To enter cybersecurity, you should go for a certification that gives you an understanding of a network and teaches you how to secure it. There is no way to defend a network without knowing how it works. C|ND teaches you about a network and how you can incorporate security within a network. C|ND covers a wide range of topics, including securing data storage, protecting machines, configuring network sites, and even delves into physical security measures such as cameras and access control systems.

C|ND
Certified | Network Defender

EC-Council
Building A Culture Of Security

It has also helped me achieve a lot and higher certifications in the field because it laid a great foundation for my life and career. One of the good things about C|ND, is that you can never compare it with any program. C|ND, comes with this unique approach to networking, and the way it puts security together makes it easy to understand. In C|ND, you learn the seven layers of the OSI model, understand the basic concept of putting things together, and understand your network is the key area. C|ND, teaches you to monitor the log analysis side, which shows how logs can be analyzed and investigated. And that is my favorite part. C|ND, provides knowledge on securing your systems, the infrastructure, and every part of your Internet of Things. It shows you everything that you need to know about security.

Samuel Boateng
USA
President and CEO of Slamm Technologies

C|ND has upgraded my knowledge in a way that I was able to use that knowledge in the operational and strategical environment and apply that knowledge to increase the security of the company networks. There are plenty of security vendors and training programs in the market. But, they cannot compare it to C|ND. C|ND is the most complete program that covers all necessary topics regarding network security.

The first thing I like about the C|ND program is that it covers major cybersecurity approaches like preventive, reactive retrospective, and proactive security. This will help plan, establish, and maintain the security in the network as well as properly react in the case of an incident.

Ivica Gjorgjevski
USA
Information Security Officer
Stopanska Banka
Macedonia

ORGANIZATIONS THAT EMPLOY C|ND CERTIFIED MEMBERS

EC-Council

Building A Culture Of Security

About EC-Council

EC-Council invented the Certified Ethical Hacker. Founded in 2001 in response to 9/11, EC-Council's mission is to provide the training and certifications apprentice and experienced cyber security professionals need to keep corporations, government agencies, and others who employ them safe from attack.

Best known for its Certified Ethical Hacker program, EC-Council today offers 200 different training programs, certifications, and degrees in everything from Computer Forensic Investigation and Security Analysis to Threat Intelligence and Information Security. An ISO/IEC 17024 Accredited Organization recognized under the US Defense Department Directive 8140/8570 and many other authoritative cybersecurity bodies worldwide, the company has certified over 350,000 professionals across the globe. Trusted by seven of the Fortune 10, half of the Fortune 100, and the various agencies public and private across 140 nations, EC-Council is the gold standard in cybersecurity education and certification.

A truly global organization with a driving belief in bringing diversity, equity, and inclusion to the modern cybersecurity workforce, EC-Council maintains 11 offices in the U.S., the UK, India, Malaysia, Singapore, and Indonesia.

www.eccouncil.org