pue

EC-Council

C|ND v2

Certified Network Defender

CERTIFIED NETWORK DEFENDER

Protect. Detect. Respond. Predict.

Certified Network Defender v2

The only true blue team network defense program!

Cybersecurity now dominates the priorities of every enterprise striving to adapt to a post-COVID world. Forced to go remote, their workers' identities and devices are the new security perimeter. In fact, cybersecurity for business is now as critical as internet access itself.

The only program built for the world's largest work-from-home experiment!

Studies and news reports had demonstrated that cyber attackers are quick to attack the new, unprotected threat surfaces created when millions of employees started working from home. Providing network security to such an unprecedented, distributed ecosystem in this post-pandemic world is every Network Defense Team's acid test.

The Certified Network Defender v2 program has been upgraded and loaded with battle-ready ammunition to help Blue Teams defend and win the war against network breaches. Individuals and corporations looking to strengthen their Network Defense Skills will find CND v2 a must-have for 5 reasons:

Only comprehensive network defense program built to incorporate critical secure network skills - Protect, Detect, Respond and Predict

Maps to NICE 2.0 Framework

Comes packed with the latest tools, technologies, and techniques

Deploys a hands-on approach to learning

Designed with an enhanced focus on Threat Prediction, Business Continuity and Disaster Recovery

An Adaptive Security Strategy – Protect, Detect, Respond, and Predict

Cybersecurity is a continuous, non-linear process. Therefore, your approach to mitigating cyber risks cannot be static. This is particularly important when the new "normal" has millions of employees working from remote locations on fragile, home-based WiFi networks and non-sanitized personal devices.

According to Gartner, traditional "prevent and detect" approaches are inadequate. Opportunistic by nature, malicious actors look for the easiest ways to attack the most users and siphon off the maximum gains. Developing a continuous Adaptive Security Cycle helps organizations stay ahead of cybercriminals by creating and improving security systems. Enter CND v2.

Protect

- Defense-In-Depth Security
- Properly Designed, Implemented, and Enforced Security Policies
- Security Architectures
- Appropriate Configuration
- Right Selection of Security Controls

Detect

- Traffic Monitoring
- Log Management
- Log Monitoring
- Anomalies Detection

Respond

- Incident Response
- Forensics Investigation
- Business Continuity (BC)
- Disaster Recovery (DR)

Predict

- Risk and Vulnerability Assessment
- Attack Surface Analysis
- Threat Intelligence

As Hands-On as Network Defense Can Get

Created based on a thorough job task analysis

CND v2 is based on the cybersecurity education framework and work role task analysis presented by the National Infocomm Competency Framework (NICF). The program is also mapped to the Department of Defense (DoD) roles for system/network administrators as well as global work roles and responsibilities laid out by the revised NICE Framework 2.0

Adaptive Security Strategy

CND v2 includes the Adaptive Security Strategy, thereby increasing the scope from Protect – Detect – Respond to Protect – Detect – Respond – Predict.

Increased Lab Time and Hands-On Focus

More than 50% of the CND v2 program is dedicated to practical skills in live ranges via EC-Council labs covering domains like Network Defense Management, Network Perimeter Protection, Endpoint Protection, Application and Data Protection, Enterprise Virtual, Cloud, and Wireless Network Protection, Incident Detection and Response, and Threat Prediction.

A Dedicated Module on IoT Security

IoT security, previously ignored, is now an issue of great concern. IoT devices are not primarily designed with security in mind. This leaves serious vulnerabilities while configuring IoT devices in a network. CND v2 introduces candidates to the various challenges that IoT devices pose and the measures required to mitigate them.

Network Virtualization Practices for the Remote Workforce

Tracking security applications and configurations of remote work environments as workforce span across servers is very difficult. The CND v2 program teaches candidates to implement and manage the security of virtualization technologies Network Virtualization (NV), Software-Defined Network (SDN), Network Function Virtualization (NFV), OS Virtualization, Containers, Dockers, Kubernetes used in modern-day networks.

An Upgrade on Mobile Security Measures

Research firm Gartner predicts that by 2021, 27% of corporate data traffic will bypass perimeter security and flow directly from mobile and portable devices to the cloud. With the CND v2, you will learn Enterprise Mobile Device Security, Redefine Access Control Security, and other platforms to ensure that this endpoint remains secure.

Enhanced Focus on Cloud Security

While the adoption of cloud computing in organizations has increased, so have the challenges. Candidates will learn different ways to ensure security across various cloud platforms - AWS, Microsoft Azure Cloud, and Google Cloud Platform.

An Introduction to Threat Intelligence

Having a proactive approach to security is the new requirement of all organizations. Without threat intelligence, your cybersecurity posture is only reactive. CND v2 helps you take a more effective, proactive approach using threat intelligence.

In-Depth Attack Surface Analysis

The key to cyber risk management is in-depth attack surface analysis. CND v2 trains you to identify what parts of your organization need to be reviewed and tested for security vulnerabilities, and how to reduce, prevent, and mitigate network risks.

Includes the Latest Technology

CND v2 covers the latest technologies such as Software Defined Network (SDN) security, Network Function Virtualization (NFV) security, container security, docker security, and Kubernetes security.

About the Exam

Number of Questions: **100**	Test Duration: **4 Hours**	Test Format: **Multiple Choice**
Test Delivery: **ECC EXAM**	Exam Prefix: **312-38 (ECC EXAM)**	

Passing score

In order to maintain the high integrity of our certification exams, EC-Council Exams are provided in multiple forms (i.e., different question banks). Each form is carefully analyzed through beta testing with an appropriate sample group under the guidance of a committee of subject matter experts. This approach ensures our exams offer academic difficulty, as well as "real world" applications. We also have a process to determine the difficulty rating of each question. The individual rating then contributes to an overall "Cut Score" for each exam form. To ensure each form adheres to assessment standards, Cut Scores are set on a "per exam form" basis. Depending on which exam form is challenged, Cut Scores can range from 60% to 85%

Course Outline

Module 01	Network Attacks and Defense Strategies
Module 02	Administrative Network Security
Module 03	Technical Network Security
Module 04	Network Perimeter Security
Module 05	Endpoint Security-Windows Systems
Module 06	Endpoint Security-Linux Systems
Module 07	Endpoint Security- Mobile Devices
Module 08	Endpoint Security-IoT Devices
Module 09	Administrative Application Security
Module 10	Data Security
Module 11	Enterprise Virtual Network Security
Module 12	Enterprise Cloud Network Security
Module 13	Enterprise Wireless Network Security
Module 14	Network Traffic Monitoring and Analysis
Module 15	Network Logs Monitoring and Analysis
Module 16	Incident Response and Forensic Investigation
Module 17	Business Continuity and Disaster Recovery
Module 18	Risk Anticipation with Risk Management
Module 19	Threat Assessment with Attack Surface Analysis
Module 20	Threat Prediction with Cyber Threat Intelligence

What will you learn?

- Understanding network security management
- Learn basics of first response and forensics
- Establishing network security policies and procedures
- Understanding indicators of Compromise, Attack, and Exposures (IoC, IoA, IoE)
- Windows and Linux security administration
- Building threat intelligence capabilities
- Setting up mobile and IoT device security
- Establishing and monitoring log management
- Implementing data security techniques on networks
- Implementing endpoint security
- Embedding virtualization technology security
- Configuring optimum firewall solutions
- Determining cloud and wireless security
- Understanding and using IDS/IPS technologies
- Deploying and using risk assessment tools
- Establishing Network Authentication, Authorization, Accounting (AAA)

Who is it for?

CND v2 is for those who work in the network administration/cybersecurity domain in the capacity of Network Administrator/Engineer, Network Security Administrator/Engineer/Analyst, Cybersecurity Engineer, Security Analyst, Network Defense Technician, Security Operator. CND v2 is for all cybersecurity operations, roles, and anyone looking to build a career in cybersecurity.

Suggested Duration: 5 Days (9:00 AM – 5:00 PM)

Eligibility Criteria

To be eligible to challenge the EC-Council CND certification examination, the candidate has two options:

Attend Official Network Security Training by EC-Council:

If a candidate has completed an official EC-Council training either at an Accredited Training Center, via the iClass platform, or at an approved academic institution, the candidate is eligible to challenge the relevant EC-Council exam without going through the application process.

Attempt the Exam without Official EC-Council Training:

In order to be considered for the EC-Council CND v2 exam without attending official network security training, the candidate must have at least 2 years of work experience in the Information Security domain. If the candidate has the required work experience, they can submit an eligibility application form along with USD 100.00, a non-refundable fee.

Training options

EC-Council | iClass

iLearn (Self-Study)

This solution is a self-directed study environment to deliver EC-Council's CND v2 program in a streaming video format.

iWeek
LIVE.ONLINE

iWeek (Live Online)

This solution provides live, online, instructor-led CND v2 training. You can attend it from anywhere as long as you have an internet connection.

EC-Council
Masterclass

Masterclass

This solution offers you the opportunity to learn Certified Network Defender from the world-class instructors in collaboration with top information security professionals.

Training Partner (Instructor-led Training)

CND v2 is available globally through EC-Council's Authorized Training Partners and are conveniently located in your area and offers you the benefit of learning through experienced certified EC-Council instructors along with your peers, gaining the real-world skills together.

Education Partner (In-Person or Online)

This solution offers CND v2 through EC-Council Academia Partner institutions and is for students enrolled in the applicable college or university degree programs.

Accreditations, Recognitions, and Endorsements

American National Standards Institute (ANSI)

Government Communications Headquarters (GCHQ)

United States Department of Defense (DoD)

National Infocomm Competency Framework (NICF)

Testimonials

EC-Council offers thorough programs with elaborate training content. My learning from the Certified Network Defender (C|ND) program helped me in my professional life. With this obtained knowledge, I was able to analyze the vulnerabilities in our organization's network security. I also contributed my inputs to strengthen the existing security infrastructure at my workplace.

- Raymond Philip Gamboa
Assistant Manager - Service Operations,
Daimler Mobility AG, Singapore

For me, EC-Council's Certified Network Defender (C|ND) program covered the whole network security domain. It is a vendor-neutral, comprehensive program focusing network protocols, controls, vulnerabilities, devices, and much more. The program includes hands-on labs to offer a better understanding of all the major network security tools and techniques.

- George L. S.
Endpoint Protection/ACAS Administrator,
Jacobs, USA

For all those, who are passionate to learn network security, your first stop should be EC-Council Certified Network Defender (C|ND). The C|ND courseware helped me understand the different modules in the program. Plus, there is no other training program that can cover this domain with such information. I wouldn't have been able to attain the C|ND credential without going through this advanced training. My experience involves high-quality labs, brilliant content delivery by an experienced instructor, and encyclopedic knowledge of the domain. It also covered various important networking topics which made this entire learning experience very relatable to real-world scenarios. After this, I am planning on progressing further through the path of credentials.

- Geoffrey Chisnall
Network Security Administrator,
Experian, South Africa

My experience with EC-Council beginning from the first training in 2015, until now has been an excellent opportunity. The courseware and the training material, when compared to other vendor training courses, are much better, improving over the years with every new version update and credential release.

– Ivica Gjorgjevski

Head of Department for Security Accreditation of Classified information and ICT support, Directorate for Security of Classified Information, North Macedonia

After finishing my contract with the Army, New Horizons Computer Learning Centers offered me career training in Cybersecurity. I wanted to take up EC-Council's Certified Network Defender (C|ND) because of its massive amount of training material. I was thrilled to be able to learn and test my abilities in different network security concepts. I found its source material well written and full of new information. The C|ND training reminded me always to stay vigilant. Never stop learning because there's always something new out there to discover.

Kenneth P.

Researcher
IEEE, Spain

https://www.pue.es/cursos/ec-council/cnd-certified-network-defender

EC-Council

www.eccouncil.org