Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå os her

.

Email: training.ecs.dk@arrow.com
Phone: +45 7025 4500

Certified Network Defender (CND)
Blueteamingbrother to Certified ethical Hacker

CODE:	LENGTH:	PRICE:
ECC_CND	40 Hours (5 dage)	kr 25,000.00

Description

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 postpandemic 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

Objectives

- Understanding network security management
- Learn basics of first response and forensics
- Building threat intelligence capabilities
- Establishing and monitoring log management
- Implementing endpoint security
- Configuring optimum firewall solutions
- Understanding and using IDS/IPS technologies
- Establishing Network Authentication, Authorization, Accounting (AAA)
- Understanding indicators of Compromise, Attack, and Exposures (IoC, IoA, IoE)

- Establishing network security policies and procedures
- Windows and Linux security administration
- Embedding virtualization technology security
- Determining cloud and wireless security
- Deploying and using risk assessment tools
- Setting up mobile and IoT device security
- Implementing data security techniques on networks

Audience

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.

Programme

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

Test and Certification

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%

Options

- **Exam title:** CND
- **Exam code:** 312-38
- **Number of questions:** 100
- **Duration:** 4 Hours
- **Availability:** ECC Exam
- **Test Format:** Interactive Multiple Choice Question

Further Information

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 nonsanitized 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. 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.

Session Dates

På anmodning. Kontakt os venligst

Yderligere Information

Denne træning er også tilgængelig som træning på stedet. Kontakt os for at finde ud af mere.