Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

EC-Council Certified Network Defender (CND)

CODE:	LENGTH:	PRICE:
ECC_CND	40 Hours (5 days)	kr35,900.00

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

2. Maps to NICE 2.0 Framework
3. Comes packed with the latest tools, technologies, and techniques
4. Deploys a hands-on approach to learning
5. 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 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.

Objectives

What will you learn?

- 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

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

Follow on courses

For more information, please read:
CND brochure >>
CND Course Outline >>

Test and Certification

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.

Further Information

Certification test:
Exam title: CND
Exam code: 312-38
Number of questions: 100
Duration: 4 Hours
Availability: ECC Exam
Test Format: Interactive Multiple Choice Question
Arrow ECS is an official EC-Council test center. We shdedule test appr. 4 weeks after course. If you wish to take the test later, please contact our education team to book the test.
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%

Session Dates

På begäran, kontakta oss

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.