MedTech Programs

MedTech Mediterranean Institute of Technology

Certified Network Defender

EC-COUNCIL | ACADEMIA PARTNER

I. Program overview & Benefit:

In the evolving landscape of cybersecurity, the Certified Network Defender (CND) v2 program stands as a cornerstone for professionals aiming to master network defense in a post-pandemic world. This program, designed to address the challenges of remote work and expanded digital perimeters, equips participants with the skills necessary to protect, detect, respond to, and predict cybersecurity threats. By integrating the latest tools, technologies, and strategies, the CND v2 ensures that learners are prepared for the dynamic challenges of securing modern networks.

Key features of the program include a hands-on learning approach, covering essential topics such as network defense management, endpoint protection, and threat prediction. It is tailored for professionals in network administration and cybersecurity roles, aiming to enhance their capabilities in a comprehensive manner. Participants benefit from an immersive learning experience, guided by the latest industry practices and the NICE 2.0 Framework.

The CND v2 is more than just a training program; it is a pathway to becoming a proficient network defender capable of navigating the complexities of cybersecurity in today's interconnected world.

II. Intended Participants:

The intended participants for the Certified Network Defender (CND) v2 program are individuals working in the network administration/cybersecurity domain. This includes roles such as:

- Network Administrators/Engineers Network Security
- Administrators/Engineers/Analysts
- Cybersecurity Engineers
- Security Analysts
- Network Defense Technicians
- Security Operators

The program is designed for all cybersecurity operations roles, and anyone looking to build or advance their career in cybersecurity.

III. Program Curriculum

The Certified Network Defender (CND) v2 program curriculum is structured to provide a comprehensive understanding of network defense, covering a wide range of topics essential for cybersecurity professionals and, is designed to equip participants with the skills needed to protect, detect, respond to, and predict cybersecurity threats in a dynamic and evolving digital landscape. With a focus on hands-on learning, the program ensures that participants gain practical experience through EC-Council labs, covering a variety of domains crucial for effective network defense.

IV. Core program curriculum:

includes a comprehensive set of 20 refreshed modules, designed to cover the essentials of network defense. Here's a brief overview of the modules:

1. **Network Attacks and Defense Strategies:** Exploration of various network attacks and the strategies to defend against them, ensuring a strong foundation in network defense mechanisms.
2. **Administrative Network Security:** Focuses on the establishment of network security policies and procedures to manage and secure an organization's information.
3. **Technical Network Security:** Delve into the technical aspects of securing a network, including the implementation of security measures and technologies.
4. **Network Perimeter Security:** Techniques and tools for securing the network perimeter against unauthorized access and attacks.
5. **Endpoint Security-Windows Systems:** Specific strategies for securing Windows-based systems from vulnerabilities and threats.
6. **Endpoint Security-Linux Systems:** Tailored security measures for Linux systems, addressing the unique challenges they face.
7. **Endpoint Security- Mobile Devices:** Covers the security of mobile devices, emphasizing the growing need for protection in a mobile-first world.
8. **Endpoint Security-IoT Devices:** Focuses on the security concerns associated with IoT devices and strategies to mitigate them.
9. **Administrative Application Security:** Strategies for securing applications from an administrative perspective, ensuring application integrity.
10. **Data Security:** Methods and techniques for ensuring the confidentiality, integrity, and availability of data.
11. **Enterprise Virtual Network Security:** Security measures for virtual networks, critical in today's cloud-driven environment.
11. **Enterprise Cloud Network Security:** Focuses on securing cloud environments, addressing the unique challenges posed by cloud computing.
12. **Enterprise Wireless Network Security:** Strategies for securing wireless networks, an essential component of modern network infrastructures.
14. **Network Traffic Monitoring and Analysis:** Techniques for monitoring and analyzing network traffic to detect and respond to potential threats.
15. **Network Logs Monitoring and Analysis:** Utilizing log data for the detection and analysis of security incidents and trends.
16. **Incident Response and Forensic Investigation:** Procedures and techniques for responding to cybersecurity incidents and conducting forensic investigations.
17. **Business Continuity and Disaster Recovery:** Planning and implementing strategies to ensure business continuity and effective disaster recovery.
18. **Risk Anticipation with Risk Management:** Identifying and managing risks to minimize their impact on the organization.
19. **Threat Assessment with Attack Surface Analysis:** Techniques for assessing threats by analyzing the attack surface of an organization.
20. **Threat Prediction with Cyber Threat Intelligence:** Utilizing cyber threat intelligence to predict and prepare for potential future threats.

This detailed curriculum is designed to provide participants with a robust understanding of network defense principles, strategies, and practical applications, equipping them with the skills needed to protect, detect, respond to, and predict cybersecurity threats effectively.

V. Schedule:

The certificate program entails a commitment of 40 hours, with sessions lasting 4 hours each week. Candidates have the flexibility to select their preferred schedule from the following options:

Evening classes

From 6:30 PM to 8:30 PM

Monday and Tuesday or Thursday and Friday

Weekend classes

From 10:00 AM to 12:00 PM:

Saturday and Sunday

VI. Enrollment requirements:

Enrollment requirements are straightforward: there are no specific prerequisites. However, participants are expected to have a basic understanding of networking, operating systems, and coding principles.

VII. The Benefits of the program:

- **Comprehensive Skills:** Incorporates Protect, Detect, Respond, and Predict for network security.
- **NICE 2.0 Alignment:** Ensures skills meet industry standards.
- **Current Tools and Techniques:** Offers knowledge on the latest in cybersecurity.
- **Practical Learning:** Focuses on hands-on training for real-world application.
- **Strategic Preparedness:** Emphasizes on anticipating threats and ensuring business continuity.

These benefits make the CND v2 program a must-have for individuals and organizations aiming to equip themselves with the best possible defense against network breaches, emphasizing practical skills and up-to-date knowledge in network security.

Contacts :

cybersecuritycontact@medtech.tn

Les jardins du LAC 2, 1053, Tunis - Tunisie