



Asia Masters Center

EC-Council Certified Network Defender (ECND) v1



Asia Masters Centre (AMC), Suite 2 B, level 6, Office Block, Grand Millennium Hotel, Bukit Bintang Street,
55100 Kuala Lumpur, Malaysia. | Tel: +60327326992 | Mobile: +601 8909 0379 | Fax: +60327326992
Website: <http://www.asiamasters.org/> | Email: info@asia-masters.com



EC-Council Certified Network Defender (ECND) v1

➔ Course Objective

- This program will be akin to learning math instead of just using a calculator.
- This program teaches a fundamental understanding of the true construct of data transfer, network technologies, and software technologies so that you understand how networks operate, the processes software is automating, and how to analyze the subject material.
- learn how to mitigate, harden, and defend from the attacks.
- learn network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall configuration.
- learn the intricacies of network traffic signature, analysis and vulnerability scanning which will help you when you design greater network security policies and successful incident response plans.
- These skills will help you foster resiliency and continuity of operations during attacks. identify different issues arising during an organization-wide security planning and how to avoid and eliminate them.

➔ Target Audience

- System Administrators
- System Engineers
- Firewall Administrators

- Network Managers
- IT Managers
- IT Professionals
- Anyone interested in network Security technologies
- Managers who want to understand cyber security core principles and practices



Course Outline

- Module 1: Computer Network Defense Fundamentals
 - Network Fundamentals
 - Network Components
 - TCP/IP Networking Basics
 - TCP/IP Protocol Stack
 - IP Addressing
 - Computer Network Defense (CND)
 - CND Triad
 - CND Process
 - CND Actions
 - CND Approaches
- Module 2: Network Security Threats, Vulnerabilities, and Attacks
 - Essential Terminologies
 - Network Security Concerns
 - Network Security Vulnerabilities
 - Network Reconnaissance Attacks
 - Network Access Attacks
 - Denial of Service (DoS) Attacks
 - Distributed Denial-of-Service Attack (DDoS)
 - Malware Attacks



Asia Masters Center

- Module 3: Network Security Controls, Protocols, and Devices
 - Fundamental Elements of Network Security
 - Network Security Controls
 - User Identification, Authentication, Authorization and Accounting
 - Types of Authorization Systems
 - Authorization Principles
 - Cryptography
 - Security Policy
 - Network Security Devices
 - Network Security Protocols
- Module 4: Network Security Policy Design and Implementation
 - What is Security Policy?
 - Internet Access Policies
 - Acceptable-Use Policy
 - User-Account Policy
 - Remote-Access Policy
 - Information-Protection Policy
 - Firewall-Management Policy
 - Special-Access Policy
 - Network-Connection Policy
 - Business-Partner Policy
 - Email Security Policy
 - Passwords Policy
 - Physical Security Policy
 - Information System Security Policy
 - Bring Your Own Devices (BYOD) Policy
 - Software/Application Security Policy
 - Data Backup Policy



Asia Masters Center

- Confidential Data Policy
- Data Classification Policy
- Internet Usage Policies
- Server Policy
- Wireless Network Policy
- Incidence Response Plan (IRP)
- User Access Control Policy
- Switch Security Policy
- Intrusion Detection and Prevention (IDS/IPS) Policy
- Personal Device Usage Policy
- Encryption Policy
- Router Policy
- Security Policy Training and Awareness
- ISO Information Security Standards
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Information Security Acts: Sarbanes Oxley Act (SOX)
- Information Security Acts: Gramm-Leach-Bliley Act (GLBA)
- Information Security Acts: The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)
- Other Information Security Acts and Laws
- Module 5: Physical Security
 - Physical Security
 - Access Control Authentication Techniques
 - Physical Security Controls
 - Other Physical Security Measures
 - Workplace Security
 - Personnel Security: Managing Staff Hiring and Leaving Process



Asia Masters Center

- Laptop Security Tool: EXO5
- Environmental Controls
- Physical Security: Awareness /Training
- Physical Security Checklists
- Module 6: Host Security
 - Host Security
 - OS Security
 - Linux Security
 - Securing Network Servers
 - Hardening Routers and Switches
 - Application/software Security
 - Data Security
 - Virtualization Security
- Module 7: Secure Firewall Configuration and Management
 - Firewalls and Concerns
 - What Firewalls Does?
 - What should you not Ignore?: Firewall Limitations
 - How Does a Firewall Work?
 - Firewall Rules
 - Types of Firewalls
 - Firewall Technologies
 - Firewall Topologies
 - Firewall Rule Set & Policies
 - Firewall Implementation
 - Firewall Administration
 - Firewall Logging and Auditing
 - Firewall Anti-evasion Techniques
 - Why Firewalls are Bypassed?
 - Full Data Traffic Normalization



Asia Masters Center

- Data Stream-based Inspection
- Vulnerability-based Detection and Blocking
- Firewall Security Recommendations and Best Practices
- Firewall Security Auditing Tools
- Module 8: Secure IDS Configuration and Management
 - Intrusions and IDPS
 - IDS
 - Types of IDS Implementation
 - IDS Deployment Strategies
 - Types of IDS Alerts
 - IPS
 - IDPS Product Selection Considerations
 - IDS Counterparts
- Module 9: Secure VPN Configuration and Management
 - Understanding Virtual Private Network (VPN)
 - How VPN works?
 - Why to Establish VPN ?
 - VPN Components
 - VPN Concentrators
 - Types of VPN
 - VPN Categories
 - Selecting Appropriate VPN
 - VPN Core Functions
 - VPN Technologies
 - VPN Topologies
 - Common VPN Flaws
 - VPN Security
 - Quality Of Service and Performance in VPNs

➤ **Module 10: Wireless Network Defense**

- Wireless Terminologies
- Wireless Networks
- Wireless Standard
- Wireless Topologies
- Typical Use of Wireless Networks
- Components of Wireless Network
- WEP (Wired Equivalent Privacy) Encryption
- WPA (Wi-Fi Protected Access) Encryption
- WPA2 Encryption
- WEP vs. WPA vs. WPA2
- Wi-Fi Authentication Method
- Wi-Fi Authentication Process Using a Centralized Authentication Server
- Wireless Network Threats
- Bluetooth Threats
- Wireless Network Security
- Wi-Fi Discovery Tools
- Locating Rogue Access points
- Protecting from Denial-of-Service Attacks: Interference
- Assessing Wireless Network Security
- Wi-Fi Security Auditing Tool: AirMagnet WiFi Analyzer
- WPA Security Assessment Tool
- Wi-Fi Vulnerability Scanning Tools
- Deploying Wireless IDS (WIDS) and Wireless IPS (WIPS)
- WIPS Tool
- Configuring Security on Wireless Routers
- Additional Wireless Network Security Guidelines



Asia Masters Center

- Module 11: Network Traffic Monitoring and Analysis
 - Network Traffic Monitoring and Analysis(Introduction)
 - Network Monitoring: Positioning your Machine at Appropriate Location
 - Network Traffic Signatures
 - Packet Sniffer: Wireshark
 - Detecting OS Fingerprinting Attempts
 - Detecting PING Sweep Attempt
 - Detecting ARP Sweep/ ARP Scan Attempt
 - Detecting TCP Scan Attempt
 - Detecting SYN/FIN DDOS Attempt
 - Detecting UDP Scan Attempt
 - Detecting Password Cracking Attempts
 - Detecting FTP Password Cracking Attempts
 - Detecting Sniffing (MITM) Attempts
 - Detecting the Mac Flooding Attempt
 - Detecting the ARP Poisoning Attempt
 - Additional Packet Sniffing Tools
 - Network Monitoring and Analysis
 - Bandwidth Monitoring
- Module 12: Network Risk and Vulnerability Management
 - What is Risk?
 - Risk Levels
 - Risk Matrix
 - Key Risk Indicators(KRI)
 - Risk Management Phase
 - Enterprise Network Risk Management
 - Vulnerability Management



Asia Masters Center

➤ Module 13: Data Backup and Recovery

- Introduction to Data Backup
- RAID (Redundant Array Of Independent Disks) Technology
- Storage Area Network (SAN)
- Network Attached Storage (NAS)
- Selecting Appropriate Backup Method
- Choosing the Right Location for Backup
- Backup Types
- Conducting Recovery Drill Test
- Data Recovery
- Windows Data Recovery Tool
- RAID Data Recovery Services
- SAN Data Recovery Software
- NAS Data Recovery Services

➤ Module 14: Network Incident Response and Management

- Incident Handling and Response
- Incident Response Team Members: Roles and Responsibilities
- First Responder
- Incident Handling and Response Process
- Overview of IH&R Process Flow

➤ **The Feature Of Asia Master Training And Development Center**

- we pick up the customer from the airport to the hotel.
- we give the participant training bag includes all the necessary tools for the course.
- Working within groups to achieve the best results.
- All our courses are confirmed and we do not postpone or cancel the courses regardless of the number of participants in the course.



Asia Masters Center

- We can assist you in booking hotels at discounted prices if you wish to book through us.
- We offer the certificate from Asia Masters Center for Training and Administrative Development.

➔ The Cost Of The Training Program Includes The Following:

- 1) Scientific article on flash memory.
- 2) Training Room.
- 3) Training.
- 4) Coffee break.
- 5) The training bag includes all the tools for the course.

Price (USD)

Communicate with the training department
to know the participation fees

➤ **There are offers and discounts for groups**

The details of the bank account

Bank name: CIMB Bank Berhad

Account name: Asia Masters Center SDN. BHD

Bank account number: 80-0733590-5

Swift code: CIBBMYKL

IBAN: Null