

Certified Network Defender (CND)

Kuala Lumpur (Malaysia)

24 - 28 March 2025

UK Traininig

PARTNER



Certified Network Defender (CND)

Code: IT28 From: 24 - 28 March 2025 City: Kuala Lumpur (Malaysia) Fees: 4900 Pound

Introduction

The Certified Network Defender CND course is designed to equip network administrators with the skills necessary to defend their networks from threats. This course offers a comprehensive understanding of network security, focusing on the protection, detection, and response to network attacks. Participants will learn about network defense fundamentals, network security controls, protocols, perimeter appliances, secure IDS configurations, VPNs, firewall configurations, and network traffic signature analysis. By the end of the course, participants will be proficient in designing and implementing network security policies and plans.

Course Objectives

- Understand network defense fundamentals and techniques.
- Implement secure network protocols and controls.
- Configure and manage firewalls, VPNs, and IDS/IPS.
- Conduct network traffic monitoring and analysis.
- Develop and implement network security policies and incident response strategies.

Course Outlines

Day 1: Introduction to Network Security

- Overview of Network Security Concepts.
 - Importance of network security.
 - Types of network threats.
 - Network security policies and procedures.
- Network Defense Essentials.
 - Defense-in-depth strategy.
 - Layered security approach.
 - Network security architecture.
- Security Threats and Vulnerabilities.
 - Common network vulnerabilities.
 - Threat vectors and attack methods.
 - Risk assessment and management.
- Network Security Controls.
 - Physical security controls.
 - Technical security controls.
 - Administrative security controls.
- Introduction to Network Security Tools.
 - Types of security tools.

UK Training
PARTNER



- Tool selection and deployment.
- Overview of network defense technologies.

Day 2: Network Security Protocols and Configuration

- Secure Network Protocols.
 - TCP/IP security fundamentals.
 - Secure communication protocols SSL/TLS, SSH.
 - VPN technologies and protocols.
- Firewall Configuration and Management.
 - Types of firewalls.
 - Firewall architecture and deployment.
 - Configuring firewall rules and policies.
- Intrusion Detection and Prevention Systems IDS/IPS.
 - IDS/IPS concepts and types.
 - Deployment strategies.
 - Configuring and managing IDS/IPS.
- Network Access Control NAC.
 - NAC concepts and technologies.
 - Implementing NAC.
 - Managing access control policies.
- Secure Network Design.
 - Network segmentation and isolation.
 - Designing secure network topologies.
 - Implementing network security zones.

Day 3: Network Traffic Monitoring and Analysis

- Network Traffic Analysis Fundamentals.
 - Importance of traffic analysis.
 - Types of network traffic.
 - Tools for traffic monitoring and analysis.
- Packet Analysis.
 - Understanding packet structure.
 - Capturing and analyzing packets.
 - Identifying malicious traffic.
- Network Performance Monitoring.
 - Monitoring network performance metrics.
 - Identifying performance bottlenecks.
 - Tools for performance monitoring.
- Log Management and Analysis.
 - Importance of log management.
 - Log collection and storage.
 - Analyzing logs for security events.
- Network Anomaly Detection.
 - Understanding network baselines.
 - Detecting deviations from normal behavior.
 - Responding to network anomalies.



Day 4: Incident Response and Handling

- Incident Response Fundamentals.
 - Importance of incident response.
 - Incident response lifecycle.
 - Roles and responsibilities in incident response.
- Incident Detection and Analysis.
 - Detecting security incidents.
 - Analyzing incident data.
 - Identifying the root cause of incidents.
- Incident Containment, Eradication, and Recovery.
 - Containment strategies.
 - Eradicating threats.
 - Recovery procedures and best practices.
- Forensic Investigation Techniques.
 - Introduction to digital forensics.
 - Collecting and preserving evidence.
 - Analyzing forensic data.
- Incident Response Planning.
 - Developing an incident response plan.
 - Conducting incident response drills.
 - Continuous improvement of incident response capabilities.

Day 5: Network Security Policy and Risk Management

- Network Security Policy Development.
 - Importance of security policies.
 - Developing comprehensive security policies.
 - Implementing and enforcing policies.
- Risk Management and Assessment.
 - Understanding risk management concepts.
 - Conducting risk assessments.
 - Mitigating network security risks.
- Business Continuity and Disaster Recovery.
 - Importance of business continuity planning.
 - Developing disaster recovery plans.
 - Implementing and testing recovery procedures.
- Security Awareness and Training.
 - Importance of security awareness.
 - Developing security awareness programs.
 - Training employees on network security best practices.
- Continuous Security Improvement.
 - Monitoring and reviewing security measures.
 - Implementing security updates and patches.
 - Staying informed about emerging threats and technologies.



Blackbird Training Cities

Europe



Copenhagen (Denmark)



Sarajevo (Bosnia and Herzegovina)



Málaga (Spain)



Cascais (Portugal)



Glasgow (Scotland)



Edinburgh (UK)



Oslo (Norway)



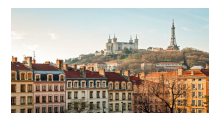
Annecy (France)



Bordeaux (France)



Birmingham (UK)



Lyon (France)



Moscow (Russia)



Stockholm (Sweden)
(Netherlands)



Podgorica (Montenegro)



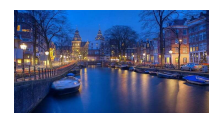
Batumi (Georgia)



London (UK)



Istanbul (Turkey)



Amsterdam



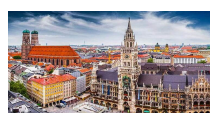
Düsseldorf (Germany)



Paris (France)



Barcelona (Spain)



Munich (Germany)



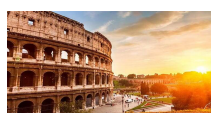
Geneva (Switzerland)



Prague (Czech)



Vienna (Austria)



Rome (Italy)



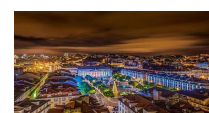
Brussels (Belgium)



Madrid (Spain)



Berlin (Germany)



Lisbon (Portugal)



Zurich (Switzerland)



Manchester (UK)

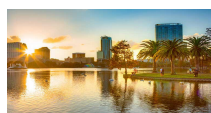


Milan (Italy)

USA & Canada



Los Angeles (USA)



Orlando (USA)



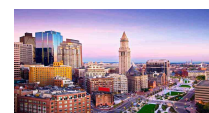
Online



Phoenix (USA)



Texas (USA)



Boston (USA)



Washington (USA)



Miami (USA)



New York (USA)



Seattle (USA)



Toronto (Canada)



Blackbird Training Cities

Asia



Baku (Azerbaijan)



Maldives (Maldives)



Manila (Philippines)



Bali (Indonesia)



Bangkok (Thailand)



Beijing (China)



Singapore (Singapore)
(Kuwait)



Sydney (Australia)



Tokyo (Japan)



Dubai (UAE)



Kuala Lumpur (Malaysia)



Kuwait City



Jakarta (Indonesia)



Amman (Jordan)

Africa



Kigali (Rwanda)



Cape Town (South Africa)



Accra (Ghana)



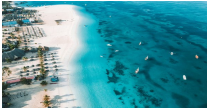
Lagos (Nigeria)



Marrakesh (Morocco)



Nairobi (Kenya)



Zanzibar (Tanzania)



Tangier (Morocco)



Cairo (Egypt)



Sharm El-Sheikh (Egypt)



Casablanca (Morocco)



Tunis (Tunisia)



Blackbird Training Clients



UK Training
PARTNER



Blackbird Training Categories

Management & Admin

Professional Skills
Finance, Accounting, Budgeting
Media & Public Relations
Project Management
Human Resources
Audit & Quality Assurance
Marketing, Sales, Customer Service
Secretary & Admin
Supply Chain & Logistics
Management & Leadership
Agile and Elevation

Technical Courses

Hospital Management
Public Sector
Special Workshops
Oil & Gas Engineering
Telecom Engineering
IT & IT Engineering
Health & Safety
Law and Contract Management
Customs & Safety
Aviation
C-Suite Training



BLACKBIRD
FOR TRAINING



International House 185 Tower Bridge
Road London SE1 2UF United Kingdom



+44 7401 1773 35
+44 7480 775526



Sales@blackbird-training.com



www.blackbird-training.com

