CYBERPORT ACADEMY
Business Unit Of MSC Cyberport Sdn. Bhd.

Certified Cyber Defender Practitioner (CCDP)

Prevent, detect and mitigate threats as they arise in real time.

A Cyber Defender practitioner, often referred to as a Cyber Defense Analyst, plays a crucial role in protecting organizations from cyber threats. These professionals use various cyber defense tools, such as intrusion detection systems (IDS) and firewalls, to monitor and analyze network traffic and system activities. Their primary responsibilities include detecting, identifying, and mitigating potential cyber threats and intrusions.

Cyber Defense Analysts need a strong foundation in cybersecurity principles, network security methodologies, risk management, and intrusion detection techniques. They also require skills in data management, vulnerability assessment, and network traffic analysis

Certified Cyber Defender Practitioner (CCDP)

Duration: 3 days instructor-led course

Course Overview

The Certified Cyber Defender Practitioner 3 days hands-on certification training prepares an organization to create a complete end to end solution for proactively monitor prevent, detect and mitigate threats as they arise in real time. This fast paced and thorough hands-on training will lead the IT-Pro through a well-rounded experience where he/she will be able to set up an deploy state of the art open source and for purchase analysis tools, intrusion detection tools, syslog servers, SIEMs along with integrating them for the entire company to find and, in many cases prevent today's exploits.

Prerequisites

1 year experience in Information Technology @ Information System is required. Some knowledge in Cyber Security is preferred.

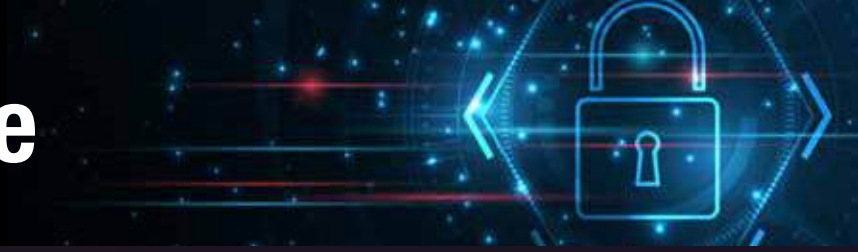
Who Should Attend

Business executives, academicians, government servants, working adults and university students.

Course Methodology

The participants are taught via lectures with various multimedia teaching aids as well as hands-on exercises in the class-room or online setting.

Course Outline



Module 1: Cyber Defense Principles

- Blue Team vs Red Team vs Purple Team
- Defensive Network Architecture Concepts
- Security Operation Center Concepts
- Identifying vulnerabilities
- Detecting threats
- Implementing security measures

Module 2: Digital Forensics & Incident Response

- Creating Digital Forensic Lab
- Digital Forensic & Investigation Tools
- Analyzing packets
- Capture & analyze network activity
- Capture & analyze file

Module 3: Practical Malware Analysis

- msfvenom analysis
- ransomware analysis
- Process monitor configuration
- Sandbox configuration
- Hybrid analysis

Module 4: Traffic Analysis

- Anylizer Tools
- Intercepting traffic
- Website Defacement traffic analysis
- IDS Alerts traffic analysis
- Find the backdoor
- Traffic Analysis with AI (TAAI)

Module 5: Cyber Defense within the Organization

- Deploy & Configuring NGFW
- Deploy & Configuring SIEM
- Deploy & Configuring IPS/IDS
- Cloud Defense System

Module 6: Defeating the Red Team

- System Hardening
- Mitigation
- Deploy & Configuring Defensive System
- Artificial Intelligence Uses in Blue Team Security