iTrainAsia™

Cyber-Security

Cyber-Security protects companies' services, operations, and data from the ever-increasing risk and heavy cost of cybercrime.

Cybercrime costs $600 billion in 2018, with attacks from malware, Distributed Denial-of-Service (DDoS), and web-based attacks due to rise by another 13% in 2019. In the face of this, it is essential that network and IT professionals learn and improve the techniques to combat cybercrime. This is critical to protect their companies' from disruptions in services, operations, or data theft.

According to a study by Accenture Cost of Cybercrime in 2019, cybercrime is expected to cost USD5.2 trillion over the next 5 years, from 2019 to 2023. The top 5 affected industries are: Banking, Utilities, Software Companies, Automotive, and Insurance, with an average per-company cost of USD13 million in the forms of business disruption, information loss, revenue loss and equipment damage.

Visit **itrainasia.com** to register and turn overleaf for more course information

Certified Cyber-Security Specialist

Duration: 5 Days | HRDF Claimable!

Course Overview

The Certified Cyber-Security Specialist training focuses on creating information security individuals who are trained in protecting, detecting and responding to threats on the network.

Information security individuals are usually familiar with network components, traffic, performance and utilization, network topology, location of each system, security policy, etc. This training will prepare students with the fundamental understanding of the true construct of data transfer, network technologies, software technologies so that they understand how networks operate, understand what software automating is and how to analyse the subject material.

In addition, network defense fundamentals, application of network security controls, protocols, perimeter appliances, secure IDS, VPN and firewall configuration, intricacies of network traffic signature, analysis and vulnerability scanning are also covered which will help information security individuals design greater network security policies and successful incident response plans.

Prerequisites

This training does not impose any prerequisites, however, we recommend that candidates have at least 1 year of IT administration experience.

Who Should Attend

- Anyone starting a career in Information Security / Cyber-Security.
- IT professionals wanting to transition their career into Cyber-Security.
- Anyone needing a robust introduction to Cyber-Security.
- Anyone planning to work in a position that requires Cyber-Security knowledge.
- Anyone with Information Security / Cyber-Security responsibilities.
- Anyone who has learned “on the job” but who would benefit from a formal presentation to consolidate their knowledge.
- Professionals familiar with basic IT and Information Security concepts and who need to round out their knowledge.

Learning Outcomes

Upon completion of this course, you will be able to:

- Analyze and establish security requirements for your systems/networks.
- Defend systems against unauthorized access, modification and/or destruction.
- Configure and support security tools such as firewalls, anti-virus software, patch management systems, etc.
- Define access privileges, control structures and resources.
- Perform vulnerability testing, risk analyses and security assessments.
- Identify abnormalities and report violations.
- Oversee and monitor routine security administration.
- Develop and update business continuity and disaster recovery protocols.

Course Outline

Day 1

Cyber-Security Essentials

- Cyber-Security: The New Frontier
- Cyber-Security & Cybercrime
- Cyber-Security Management
- Introduction to Cyber Terrorism
- Internet Radicalization
- Terrorist Use of the Internet
- Cyber Terrorism Framework
- Case Studies

Day 2

Understanding Current Threats Landscape

- CIS Top 20 Critical Controls
- Cyber Range
- Next Gen-Firewalls

New Age Threats

- Viruses & Worms
- Malware
- Zero Day Attacks
- Vulnerability Exploits
- Phishing / Social Engineering
- Cyber Espionage / Data Theft

Day 3

Reconnaissance

- Port Scan
- Web-Based Recon & Information Gathering
- Command Line Query

Vulnerability Management

- Host Scanning
- Web Application Scanning
- CVE
- Defending Against CVE Vulnerability Attacks

Day 4

Monitoring & Defending Against Advanced Attacks

- Splunk - A SIEM Monitoring Tool
- Defending Against IP Layer DDOS Attacks
- Defending Against Transport Layer DDOS Attacks
- Defending Against Application Layer DDOS Attacks
- Defending Against Botnet & C&C

Advanced Security Operations

- Malware Blocking
- Data Leak Prevention (DLP) / Data Filtering
- File Blocking
- URL Filtering
- Evasion Tactics

Day 5

Introduction to Security Incident & Incident Handling

- Security Incident, Processes & Framework
- Incident Handling
- Security Incident Priority
- Handling Intrusion Incident
- Handling Malware Incident
- Handling Phishing Incident
- Handling Spam Incident

Log Analysis

- Introduction to Log Analysis
- Log Management
- Log Visualization
- Log Analysis
- Hands-On

Testimonials

Hear what Our Students Have to Say

This is a training that we are waiting for so long.

MOHD AZMI SHAFAI, CIMB Bank

The course is beneficial for people who wants to know more about Cyber Security and have more knowledge on prevention on the attacks learned.

Yap Yoong Kian, Mah Sing Group Berhad

Companies Who Learned From Us

Trusted by Public, Private and Education Sectors

MAH SING GROUP
A Premier Lifestyle Developer

REDtone

arvato
BERTELSMANN
Arvato Systems

TENAGA NASIONAL BERHAD
(200866-W)

8 Marina View, Asia Square Tower 1
Level 07-04, Singapore 018960

www.itrainasia.com

info@itrainasia.com