TEPC05 : Certified CyberSecurity Specialist (CCSS) (อบรมเชิงปฏิบัติการพร้อมได้รับประกาศนียบัตรในระดับสากล)

Description :

Program Certified by iTrain Asia Pte Ltd

ท่ามกลางยุคที่ธุรกิจและเศรษฐกิจของโลกถูกขับเคลื่อนด้วยเทคโนโลยี และทักษะด้าน Cybersecurity เป็นที่ต้องการในองค์กร แต่บุคลากรที่มีทักษะทางด้าน Security กำลังขาดแคลน แล้วคุณพร้อมหรือยังที่จะเป็น Certified CyberSecurity Specialist? หลักสูตรสำหรับผู้สนใจทำงานด้าน Cybersecurity

เมื่อผู้เรียนได้ผ่านการเรียน และทดสอบความรู้และความสามารถตามกำหนดเกณฑ์ของหลักสูตร จะได้รับ E-Certificate และ Digital Badge ในระดับสากล

Instructor :

Mr.Mohd Hamizi Jamaludin

Cyber security Instructor

Training Date : **22-26 April 2024**

fee : **37,000 ฿** (ราคายังไม่รวม Vat 7%)

Days & Duration : **5 Day(s) | 30 Hour(s)**

Time : **09:00:00 - 16:00:00**

Language : **English**

Venue : **Online by Zoom**

Type : **Online**

Category : **Professional Certification Program**

Objectives :

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.

Target Group :

Prerequisite:

- 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.

Benefits :

Course Outline :

DAY 1

Cyber-Security Essentials:

- Cyber-Security: The New Frontier
- Cyber-Security & Cybercrime
- 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 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 and C&C

Advanced Security Operations:

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

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

Payment Condition :

Payment can be made by:

1. **Cash or Credit Card or Bank Cheque payable to**
   สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ or National Science and Technology Development Agency
   (a post-dated cheque is not accepted) on the first day of the service or within the last day of the service.

2. **Account transfer and send the proof of the payment** (the deposit slip) via email ttd@swpark.or.th

   - **ธนาคารกรุงเทพ** สาขาอุทยานวิทยาศาสตร์
     Saving Account Number: **080-0-00001-0**
     Account Name: **สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ**

   - **ธนาคารกรุงไทย** สาขาตลาดไท
     Saving Account Number: **152-1-32668-1**
     Account Name: **สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ**

Notes:

- Withholding tax (3%) is exempt.
- Should you need to withdraw, you must send the notice of the withdrawal in writing no later than 7 working days before the commencement date. The cancellation less than 7 days will be subject to a fine of 40% of the fee.
- Software Park Thailand reserves the rights to cancel courses due to unforeseen circumstances.

Contact Person :

For more information, contact our course coordinator on:

เสกสรรค์ สังสุข (อิฐ)
Mr. Seksun Sungsook
: +662 583 9992 Ext. **81421**
: +6681 913 1828
: seksun.sun@nstda.or.th
SOFTWARE PARK THAILAND

You are encouraged to use the course schedule as a guide to plan your training. The schedule is accessible at www.swpark.or.th for more information.