MINISTRY OF DIGITAL

CyberGuru
CYBER SECURITY PROFESSIONAL DEVELOPMENT

CyberSecurity MALAYSIA

INCIDENT HANDLING – HANDS-ON SCENARIO AND MALWARE ANALYSIS

Level: Specialization | **Duration:** 4 days

Pre-Requisites

Due to the nature of the training will require each participant to prepare a specific environment as the following:

1. Each participant will be given a set of Virtual Machine (VM) image containing complete tools for the training.
2. Each player is encouraged to have host machine at least 8GB of RAM and dual core processors.
3. The use of Windows operating system is recommended due to the training material are covering Windows malware only.
4. Each participant required to install VMware Workstation of VMware Fusion in order to run the given VM image. Trainer will not spend much time on setting up and troubleshoot the environment.
5. Reserved at least 200GB of hard disk space on your host machine for the VM image to run and to copy the given material.
6. Each participant must have administrator privilege on their own machine.

Modules

Day 1: Incident Handling – Hands-on Scenario

1. **Scenario 1: Email**
   - Malicious email
   - Phishing email
   - Harassing email
2. **Scenario 2: Intrusion**
   - Web Defacement
3. **Scenario 3: Social Media**
   - Impersonation/Fake Profile
4. **Scenario 4: DDoS Analysis**
   - Classification of incident
   - Verify if the DDoS continues or has stopped
   - Identify victim's ISP
   - Log analysis

Day 2: Introduction to Tools for Malware Analysis

1. **Tools for basic information gathering**
   - Including hashes, timestamp, etc.
2. **Monitoring tools for Windows malware**
3. **Understanding file formats and identifying file contents**
   - Covering packer, malware persistence, DNS, etc.
4. **Online malware sandbox analysis**

Day 3: Malware Analysis on Real Malware Samples

1. **Analyzing and observing the following malware:**
   - Computer Worm
   - Rogue AV / Fake AV
   - Ransomware
   - Trojan Horses
   - Crypto-mining malware
   - Router malware (Mirai)
   - Parasitic file infector
   - Browser based malware
   - Rootkits
   - File-less infection
   - Botnet / Backdoor
   - Macro Viruses
   - Keyloggers

Day 4: Practical Malware Analysis

1. **Preparing technical report**
2. **Threat Hunting Challenge in grouping**

For additional information, please visit www.cyberguru.my. You can also contact us at training@cybersecurity.my or call at 03 8992 6850

CyberSecurity Malaysia,
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia

Tel: +603 8800 7999 **Fax:** +603 8008 7000
Email: info@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
Website: www.cybersecurity.my