Basic of Cyber Attack and Malware Detection

Duration: 3 Days

COURSE OUTLINE

- Types of Malware; such as computer virus, worm, Trojan, backdoor, rootkit, ransomware, Botnet, etc.
- Introduction to Cyber attack using malware – Overview of the primary types of malware, how to create a safe malware analysis environment.
- Basic of Malware detection and analysis techniques and tools.
- Demonstration and Hand-on Exercises for Attack and Malware Detection and Analysis – This section demonstrates how malware works, how to detect the malicious processes and connections. The attendances receive hand-on exercises in order to practice and improve some technical skill for analyzing and responding to incidents.

WHO SHOULD ATTEND

- Network Administrator who are working in the areas of computer and network security
- Incident Response Team Members who regularly respond to complex security incidents/intrusions from APT groups/advanced adversaries
- Digital Forensic Analysts who want to investigate cyber incidences and advanced intrusion attacks.
- Information Security Staffs who are dealing with cyber-attacks and data breach incidents and intrusions
- IT staffs who are interested in the area of cyber security and digital forensics, and need to know how to detect, investigate, remediate, and recover from compromised systems

PREREQUISITES

- General knowledge of computer and network system.
- Be familiar with Windows and Linux OS
- Background in computer network protocols and tools such as Wireshark.
- Some basic of Linux command