Threat Hunting

Duration: 3 Days

COURSE DESCRIPTION

This course focuses on the process and technique to analyze and handle cyber-attack evidences This course also covers the technique used to hunt, identify, and recover from a wide range of threats within enterprise networks. This course is suitable for a security analyst who works at Tier 2 and 3 of Security Operation Center.

COURSE OUTLINE

- Introduction to the techniques of cyber attack investigation, and methods of attack analysis
- Threat hunting techniques that will help an investigator in quicker identification of breaches.
- Rapid incident response analysis and breach assessment.
- Incident response and intrusion forensics methodology for threat hunting.
- Step-by-step tactics and procedures to respond to and investigate intrusion cases.
- Discovery of unknown malware on a system.
- Demonstration and Hand-on Exercises.

PREREQUISITES

- Basic of SOC Tier 1: Processes and Tools
- General knowledge of computer and operating system.
- Some experience in computer programming languages.
- Background in Computer Network and Tools such as Wireshark.
- Some basic of Linux command.
- Be familiar with Virtual Machine (VMware or Virtual Box)

WHO SHOULD ATTEND

A system administrator, a security analyst, and a forensic investigator with some background in conducting forensic analysis, network traffic analysis, log analysis, and security assessments. It is also well suited for those managing CIRT / incident response teams, or those in roles that require oversight of forensic analysis and other investigative tasks.

SKILL LEVEL

- Intermediate – Advanced Users / SOC Tier 2 and 3