Basic of Security Operation Center : Process and Tools

Duration: 3 Days

COURSE DESCRIPTION

This course covers the areas of security operations center including Network Security Monitoring, SOC team and operation, design of SOC, SOC processes, and SOC tools. This course introduces how to setup SIEM tools and used them in the operation. This course is suitable for a security analyst who works at Tier 1 of Security Operation Center.

COURSE OUTLINE

- Learn how to design and work with network security monitoring devices.
- Address various underlying principles and techniques for detecting and responding to current and emerging computer security threats.
- Learn how to setup and use SIEM tools to monitor and detect cyber-attacks.
- Learn how to monitor and response various types of incidents in cyber-attacks.
- Learn how to detect network intrusion attempts.

PREREQUISITES

- General knowledge of computer and operating system.
- 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

- Beginner to Intermediate Users

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th