LOG Collection And Management

Description

Providing cyber incident detection and post-incident review skills by using records (logs) that can be obtained from the organization network and systems.

Delegates will learn

- ◦ Types of Records Generated on the Network
- ◦ Establishment of Record Collection and Retention Structure
- ◦ Processing of Records
- ◦ Use of Records

Outline

Types of Records Generated on the Network

- Introduction to the world of records
- Server-generated records
- Client (Windows and Linux) records
- Records of network devices
- Records of security devices

Establishment of Record Collection and Retention Structure

- Determination of the systems that generate records on the network
- methods that can be used to collect records
- classification of records according to their importance

- Installation of record collection structure
- Keeping the collected records

Processing of Records

- Record processing tools
- Techniques that can be used to process records
- Converting recording data into useful information
- Record review tools
- Record review methods

Use of Records

- Records occurring in cyber incidents
- cyber attack detection via Records
- attacker detection within the network with Records
- malware detection with Records
- use of post-cyber incident records

Prerequisites

There are no prerequisites