SOME Setup

Description

Necessary information will be provided for the effective and sustainable establishment of SOME (Cyber Incident Response Team) structures required to be established in public institutions and critical sectors within a successful project.

Delegates will learn

- SOME principles
- SOME Personnel
- SOME Processes
- Cyber Incident Detection
- SOME Technologies

Outline

SOME principles

- Foundations of SOME installation
- SOMEs in Turkey
- International SOME STANDARDS

SOME Personnel

- Personnel selection criteria
- Trainings to be received by the personnel
- tasks to support SOME

- SOME’s communication channels

SOME Processes

- Basic SOME processes, elaboration of SOME processes
- determination of SOME processes specific to the organization
- control of SOME processes
- Example SOME policies and processes

Cyber Incident Detection

- IOC (Indicators of Compromise event indicators)
- Non-technical cyber event indicators
- Technical event indicators
- Confirmation of event indicators and extraction of false alarms

SOME Technologies

- Technologies required for an effective SOME
- technologies that can be used for cyber incident detection
- integration of SOME technologies, post-incident follow-up

Prerequisites

There are no prerequisites