SETC Training Corporate Logo

IT Security Training: Cyber Threat Intelligence (CYBERT, 4 jours)

Description

The training course Cyber Threat Intelligence (IT Security Training) is a complete exploration of the principles and application of implementing a Cyber Threat Intelligence program within your organization. Starting with the anatomy of an attack and the indications of compromise, the course explores the cyber kill chain together with the cyber intelligence cycle, data collection and analysis as well as threat analysis and the use of networks and partners.

Tarifs

- Tarification: $3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

Cyber Threat Intelligence Basics

- Types of Cyber Threat Intelligence
- Key Features of Threat Intelligence Services
- Benefits of Cyber Threat Intelligence
- Leverage Network Intelligence to Identify Infected Devices
- The Cyber Threat Intelligence (CTI) Cycle
- Advantages of CTI
- Benefits of Strategic CTI
- Overview of APT Groups

Indicators of Compromise

- The Nature of Advanced Persistent Threats (APTs)
- Unusual Outbound Network Traffic
- Anomalies in Privileged User Account Activity
- Geographical Irregularities
- Other Login Red Flags
- Surges in Data Read Volumes
- Large HTML Response Sizes
- Large Number of Requests for the Same File
- Mismatched Port-Application Traffic
- Suspicious Registry Changes
- DNS Request Anomalies
- Unexpected Patching of Systems
- Mobile Device Profile Changes
- Bundles of Data in the Wrong Place
- Web Traffic with Superhuman Behavior
- Signs of DDoS Activity

CTI: Adoption and Users

- Key Characteristics of CTIs
- The CTI Process: An Overview
- Key Considerations: Process Oriented, Risk Adjusted and Adversary Based
- Ensuring Protection and Prevention
- Cyber Threat Sharing and Situational Awareness
- Information Sensitivity and Legal Requirements