

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

About Cyber-Warfare: Types and Strategies

Cyber Threat Intelligence Requirements

Other Key CTI Requirements

Overview of Essential Tools: 7 Must Have Tools

The Cyber Kill Chain

The 7 Phases of the Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command and Control

Actions on Objectives

The Cyber Intelligence Cycle

Tactical, Operational and Strategic CTI

Overview of the Threat Intelligence Cycle

Planning and Direction

Collection

Processing

Analysis

Dissemination

Putting it All Together

Threat Intelligence Collection and Reporting

Overview of Collection and Reporting

Aggregation

Normalization and Parsing

Collecting Threat Intelligence

Strategic Threat Intelligence Collection

Operational Threat Intelligence Collection

Tactical Threat Intelligence Collection

Threat Intelligence Gathering Components

More on Collection

Overview of Data Sources

Choosing a Data Source: Devices, IP, Phishing and More

Categories of Threat Information

Cyber Threat Statistics and Reporting

Collecting CTI Information: Passive, Active and Hybrid Collection

Open Source Intelligence

Human Intelligence

Signals Intelligence

Imagery Intelligence

Measurement and Signatures Intelligence

Threat Analysis

Components of Cyber Threat Information Analysis

Analyzing CTI

Strategic Threat Intelligence Analysis

Operational Threat Intelligence Analysis

Tactical Threat Intelligence Analysis

Technical Threat Intelligence Analysis

CTI Evaluation

Developing Action Plans for Future Attack Prevention

CTI Program and Partners

Planning a CTI Program

Components of a Successful CTI Program

Recommendations

Overview of Operational Components

Implementation of a Threat Intelligence Program

CTI Partners

Primary Use Cases

Best Practices and Challenges