
Programme de Formation

Cyber Threat Intelligence (CTI) : Principes et Pratique

Organisation

Durée : 14 heures

Mode d'organisation : Présentiel

Contenu pédagogique



Public visé

Analystes SOC, responsables de la sécurité des systèmes d'information (RSSI), consultants en cybersécurité, ou toute personne impliquée dans la veille, l'analyse et la gestion des menaces informatiques.



Objectifs pédagogiques

- Décrire les concepts fondamentaux de la Cyber Threat Intelligence (CTI).
- Utiliser la terminologie et la nomenclature propre à la CTI.
- Identifier les types de menaces et les modes d'attaques courants.
- Manipuler des outils OSINT et CTI pour collecter et analyser des informations.
- Produire un premier rapport d'analyse CTI structuré.



Description

Jour 1

Matin : Introduction aux bases de la CTI

Définir la Cyber Threat Intelligence : rôle et importance.

Terminologie essentielle : TTP, IOC, APT, OPSEC.

Présentation des standards de vulnérabilités.

Découverte d'outils de gestion de l'information : MindMap, Obsidian, Notion.

Après-midi : Collecte et analyse d'informations ouvertes (OSINT)

Principes et outils OSINT appliqués à la CTI.

Outils pratiques : OTX AlienVault, Maltego, Shodan, Kaspersky Threat Data Feeds.

Mise en pratique : recherches ciblées et analyse de sources publiques.

Jour 2

Matin : Méthodologie d'analyse CTI et outils avancés

Introduction à la méthodologie MITRE ATT&CK.

Techniques de cartographie des attaques et visualisation TTP.

Découverte de MISP et OpenCTI : plateformes de partage d'indicateurs de compromission (IoC).

Après-midi : Production d'un rapport CTI et exercices pratiques

Exemples de rapports d'analyse de menaces.

Atelier pratique : élaboration d'un mini-rapport CTI à partir d'une enquête simulée.

Rétrospective : bonnes pratiques et pistes d'approfondissement.



Prérequis

Avoir des connaissances de base en cybersécurité.



Modalités pédagogiques

- Notre approche pédagogique repose sur une alternance entre apports théoriques opérationnels et mises en pratique directement issues du contexte professionnel des participants.
- Chaque thème traité s'appuie sur des études de cas concrets et des exercices pratiques, conçus spécifiquement à partir des situations réelles rencontrées dans l'environnement professionnel des stagiaires.
- Nos méthodes favorisent l'adaptation aux besoins de chaque participant afin d'optimiser leur engagement et leur apprentissage.
- L'animation privilégie une pédagogie active, favorisant les échanges, l'analyse réflexive des pratiques et une adaptation continue aux réalités professionnelles des participants.



Moyens et supports pédagogiques

- Des supports pédagogiques numériques adaptés au contexte professionnel sont remis aux participants.
- Dispositifs pédagogiques variés sont mobilisés tout au long de la formation (études de cas, exercices pratiques, travaux en sous-groupes, mises en situation, jeux pédagogiques) favorisant l'apprentissage actif, collaboratif et l'appropriation des contenus.



Modalités d'évaluation et de suivi

- Un QCM est réalisé en début et en fin de formation afin d'évaluer l'évolution des connaissances.
- Le suivi des stagiaires est assuré tout au long de la formation à travers des ateliers pratiques, des mises en situation et des échanges permettant d'évaluer leur participation et leur progression.

Une attestation individuelle de formation sera remise à chaque participant à l'issue de la formation.



Informations sur l'accessibilité

Si vous êtes en situation de handicap, ou si vous rencontrez une difficulté pouvant impacter votre participation à la formation, n'hésitez pas à nous contacter. Nous étudierons ensemble les aménagements ou adaptations pédagogiques, matérielles ou organisationnelles à mettre en place pour vous accompagner dans les meilleures conditions.