Gouvernance

# Cyber Threat Intelligence - Niveau 2

3 jours (21h00) | ★★★★½ 4,6/5 | SEC-CTI2 | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel



*Document mis à jour le 09/12/2023*

## Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Décrire les techniques, tactiques, procédures et infrastructures courantes de la CTI (Cyber Threat Intelligence) de manière approfondie
- Utiliser STIX et TAXII pour représenter les informations sur les menaces
- Développer OpenCTI pour optimiser les flux de travail CTI
- Mettre en place MISP pour collecter, enrichir et partager les informations sur les menaces
- Créer des événements MISP pour documenter les indicateurs de menace
- Intégrer MISP avec d'autres outils de sécurité et collaborer entre organisations
- Appliquer l'automatisation de la CTI avec l'API MISP
- Explorer des études de cas avancées pour une meilleure application des connaissances.

## Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

## Prérequis

Avoir suivi le cours SEC-CTI "Cyber Threat Intelligence - Niveau 1" ou avoir les connaissances équivalentes. Comprendre les concepts fondamentaux de la Cybersécurité et des indicateurs de menace. Etre familié avec MISP, STIX et TAXII à un niveau introductif et avoir une connaissance de base en langage de progammation Python. Avoir également des compétences informatiques de base et être à l'aise avec l'utilisation d'ordinateurs et de logiciels.

## Public concerné

Professionnels de la sécurité informatique, analystes en Cybersécurité, gestionnaires de la sécurité, experts en sécurité.

## Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

# Programme

## Jour 1 - Matin

- Rétrospective sur les bases de la CTI
- Techniques, tactiques, procédures et infrastructures courantes (TTP, APT, IOC, OTX...)
- Standards de gestion des vulnérabilités
- Compréhension de la structure et du format de STIX pour la représentation des informations sur les menaces
- Utilisation de TAXII pour l'échange automatisé d'indicateurs de menace entre les organisations
- Exemples d'implémentation de STIX et TAXII dans le domaine de la CTI

## Jour 1 - Après-midi

- Utilisation d'OpenCTI
- Intégration de STIX, TAXII et OpenCTI dans les flux de travail de CTI

## Jour 2 - Matin

- Présentation et installation de MISP (Malware Information Sharing Platform) et de son rôle dans la CTI
- MISP pour la collecte, l'enrichissement et le partage des informations
- Création d'événements MISP

## Jour 2 - Après-midi

- Intégration de MISP avec d'autres outils de sécurité
- MISP pour la collaboration et le partage d'informations entre les organisations
- Pivot dans les IoC

### *Exemple de travaux pratiques (à titre indicatif)*

- *Atelier pratique d'échange d'informations sur les menaces en utilisant MISP*

## Jour 3 - Matin

- Introduction à l'automatisation de la CTI avec MISP
- Utilisation de l'API MISP pour l'automatisation de la collecte et de la distribution d'informations sur les menaces
- Développement de scripts pour l'intégration avec MISP

## Jour 3 - Après-midi

- Etude de cas avancée
- Corrigé
- Explorer les tendances émergentes et les nouveaux défis de la CTI
- Bilan du cours et réflexion sur la manière d'appliquer les connaissances acquises
- Récapitulatif et perspectives

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

## Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

## Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

## Modalités et délais d'accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.