Gouvernance

Cyber Threat Intelligence - Niveau 1

3 jours (21h00) | ★★★★★ 5/5 | SEC-CTI | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 28/05/2024.

Objectifs de formation

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

- Décrire les concepts de base de la CTI (Cyber Threat Intelligence)
- Utiliser les termes de la nomenclature de la CTI
- Identifier les différentes menaces et les différents types d'attaques
- Décrire les outils et les méthodes pour vous protéger contre les attaques.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, 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 certains 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 des connaissances de base en informatique et en réseaux. Avoir également des connaissances des systèmes d'exploitation Windows et Linux, et des concepts de cybersécurité tels que les menaces, les vulnérabilités et les attaques.

Public concerné

Professionnels de la cybersécurité, analystes de sécurité, ingénieurs système et étudiants en cybersécurité souhaitant développer leurs compétences en CTI.

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

- Introduction aux bases de la CTI (Cyber Threat Intelligence)
- Nomenclature utilisée dans le domaine de la CTI
- Techniques, tactiques, procédures et infrastructures courantes (TTP, ATP, IOC...)
- APT vs OPSEC
- Standards de gestion des vulnérabilités
- Présentation des outils de gestion des informations
  - MindMap
  - Notion
  - Start.me
  - Feed RSS...

Jour 1 - Après-midi

- Introduction à l'OSINT (Open-Source Intelligence) et à ses bases
- Utilisation d'outils tels qu'OTX AlienVault, Kaspersky Threat Data Feeds, Shodan...

Exemples de travaux pratiques (à titre indicatif)

- *Exercices pratiques utilisant Maltego*

Jour 2 - Matin

- Présentation de la méthodologie de MITRE TTP (Techniques, Tactics, Procedures)
- Démonstration d'un outil de visualisation de TTP : unprotect.it

Exemples de travaux pratiques (à titre indicatif)

- *Exercices pratiques utilisant les TTP de MITRE*

Jour 2 - Après-midi

- Introduction à Munin
- Présentation d'OpenCTI et de ses fonctionnalités
- Utilisation et prise en main d'OpenCTI

Jour 3 - Matin

- Présentation d'exemples de rapports CTI
- Rédaction d'un rapport sur les résultats de l'enquête

Exemples de travaux pratiques (à titre indicatif)

- *Enquête sur un groupe de cybercriminels et recherche d'indicateurs de compromission (IOC) liés à un malware*

Jour 3 - Après-midi

- Correction des rapports
- Rétrospective sur le cours

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.