Date de publication : 13/02/2025

Formation : CTI (Cyber Threat Intelligence), niveau 1

Formation pratique - 3j - 21h00 - Réf. CYI
Prix : 2210 € H.T.

4,6 / 5

Cette formation pratique permet de de fournir aux professionnels de la cybersécurité une introduction complète aux principes fondamentaux du renseignement sur les menaces. Elle couvre les concepts clés, les méthodologies de collecte et d'analyse des menaces, ainsi que l'utilisation d'outils adaptés.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Comprendre les concepts fondamentaux du Cyber Threat Intelligence et son rôle dans la cybersécurité
- Identifier les sources de renseignement et maîtriser les techniques de collecte des menaces
- Utiliser des outils de renseignement sur les menaces pour une meilleure détection et prévention des attaques

Public concerné

Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux, auditeurs et pentesters.

Prérequis

Bonnes connaissances de TCP/IP et de la sécurité des réseaux d'entreprise. Ou connaissances équivalentes à celles apportées par le cours "Sécurité systèmes et réseaux, niveau 1" (réf. FRW).

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

Méthodes et moyens pédagogiques

Travaux pratiques

De nombreux outils seront déployés par les participants.

PARTICIPANTS

Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux, auditeurs et pentesters.

PRÉREQUIS

Bonnes connaissances de TCP/IP et de la sécurité des réseaux d'entreprise. Ou connaissances équivalentes à celles apportées par le cours "Sécurité systèmes et réseaux, niveau 1" (réf. FRW).

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1 OSINT et CTI

- Principe de l'investigation et de la source ouverte (OSINT).
- Types de sources : médias, réseaux sociaux, bases de données en ligne, etc.
- Éthique de l'investigation : respect de la vie privée, des droits de l'homme, de la légalité.
- 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 (menace persistante avancée) vs OPSEC (La sécurité opérationnelle).
- Utilisation d'outils tels qu'OTX AlienVault, Kaspersky Threat Data Feeds, Shodan, etc.

2 Outils et techniques de la CTI

- Outils de collecte et d'analyse des menaces (MISP, OpenCTI, VirusTotal, etc.).
- Méthodologie d'investigation des cybermenaces.
- Identification et analyse des indicateurs de compromission (IOC).
- Tactiques, techniques et procédures (TTP) des attaquants avec MITRE.
- Détection et prévention des menaces à travers la CTI.
- Utilisation de MISP pour la gestion des IOC.

3 MISP, OpenCTI

- MISP et ses fonctionnalités.
- OpenCTI et de ses fonctionnalités.
- Configuration et prise en main des plateformes.
- Gestion des menaces avec MISP et OpenCTI.

4 Exploitation et communication du renseignement

- Transformation des données en renseignement exploitable.
- Partage et échange d'informations (standards STIX/TAXII).
- Elaboration d'un rapport de renseignement CTI.
- Réponse à une attaque en utilisant la CTI.

Dates et lieux

CLASSE À DISTANCE
2026 : 17 juin, 28 sep., 14 déc.

PARIS LA DÉFENSE
2026 : 10 juin, 21 sep., 14 déc.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

- Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
- Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.