Date de publication : 13/02/2025

Formation : CTI (Cyber Threat Intelligence), niveau 2

Formation pratique - 3j - 21h00 - Réf. CYJ
Prix : 2460 € H.T.

Ce programme de formation avancée en Cyber Threat Intelligence (CTI) vise à approfondir les connaissances des professionnels en cybersécurité souhaitant maîtriser les méthodologies avancées d'analyse des cybermenaces (techniques de collecte, de corrélation et d'exploitation du renseignement sur les menaces).

Objectifs pédagogiques

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

- Analyser et corréler des indicateurs de compromission (IOC) et des tactiques, techniques et procédures (TTP)
- Développer OpenCTI pour optimiser les flux de travail CTI
- Utiliser STIX et TAXII pour représenter les informations sur les menaces
- Maîtriser les techniques avancées de collecte et d'évaluation des renseignements sur les cybermenaces

Public concerné

Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux, analystes CTI, experts en SOC, auditeurs et pentesters.

Prérequis

Connaissances équivalentes à celles apportées par le cours "CTI (Cyber Threat Intelligence), niveau 1" (réf. CYI).

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, analystes CTI, experts en SOC, auditeurs et pentesters.

PRÉREQUIS

Connaissances équivalentes à celles apportées par le cours "CTI (Cyber Threat Intelligence), niveau 1" (réf. CYI).

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 La CTI (Cyber Threat Intelligence)

- Rappel des fondamentaux de la CTI.
- Modèles de renseignement en cybersécurité (Pyramid of Pain, Diamond Model, Cyber Kill Chain, ATT&CK Framework).
- Analyse avancée d'une campagne d'attaque.

2 Analyse et corrélation des menaces

- Techniques d'analyse approfondie des cybermenaces.
- Utilisation avancée des outils CTI (MISP, OpenCTI, Threat Intelligence Platforms).
- Investigation d'un groupe APT.
- Méthodologie de corrélation et de mise en contexte des IOC et TTP.
- Élaboration d'indicateurs de menace exploitables.

3 Exploitation et intégration du renseignement dans les opérations

- Intégration du renseignement CTI dans les SOC et CSIRT.
- Automatisation et orchestration du renseignement CTI.
- Réponse à un incident basé sur des données CTI.
- Stratégies de communication et partage d'informations (STIX/TAXII, ISACs).
- Gestion de crise et prise de décision.

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.

Dates et lieux

CLASSE À DISTANCE
2026 : 10 juin, 21 sep., 14 déc.

PARIS LA DÉFENSE
2026 : 3 juin, 14 sep., 7 déc.