Formation Cyber Threat Intelligence : initiation au renseignement sur les menaces

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Cette session de formation de 3 jours propose un panorama complet des fondamentaux de la Threat Intelligence. Des définitions, aux concepts en passant par les différentes méthodologies et les outils, cette formation abordera autant les aspects stratégiques qu'opérationnels et techniques du "renseignement sur les menaces".
Destiné à tout type de profil, consultant, analyste CERT ou SOC, RSSI technique ou non-technique, cette session prendra également la forme de nombreuses mises en situation et de démonstrations.
Les participants comprendront pourquoi et comment une démarche de Threat Intelligence est désormais devenue indispensable pour anticiper et ajuster la cyberdéfense de son organisation face aux cybermenaces d'aujourd'hui et de demain.

Référence	CTI13
Durée	2 jours (14h)
Tarif	à partir de 2 500 €HT

PROCHAINES SESSIONS

Pour connaître les prochaines dates ou organiser un intra-entreprise, contactez-nous, nous vous répondrons sous 72 heures.

Objectifs

| Identifier les différentes facettes de la Threat Intelligence (stratégique, tactique, opérationnelle & technique)
| Appréhender le paysage des cybermenaces d'aujourd'hui
| Connaître les principaux modèles, référentiels, formats et concepts de la Threat Intelligence
| Maîtriser les bases de l'investigation et de l'analyse en Threat Intelligence
| Connaître les principaux outils et sources d'informations
| Identifier les applications concrètes de la Threat Intelligence : détecter (SOC), répondre (CERT/CSIRT) et « chasser » les incidents (hunting)

Public

| Analyste CERT/CSIRT
| Opérateur SOC
| Consultant en cybersécurité
| Responsable d'équipe sécurité souhaitant initier une capacité Threat Intel
| Responsable de la sécurité des systèmes d'information (RSSI)

Prérequis

| Connaissances de base dans le fonctionnement des systèmes d'information (système, réseau) et en sécurité informatique.

Programme de la formation

La menace
Le Renseignement
Le cycle du Renseignement
Les 3 domaines du Renseignement
Sources
Renseignement Appliqué
Outillage
Méthodes d'analyse
Lecture : Draw me like one of your French APTs

OPSEC
Particules élémentaires de la CTI
Exploitation des particules élémentaires en OSINT
Modélisation des modes opératoires adverses
Attribution
Connecting the dots
Lecture : Pyschology of Intelligence Analysis - Richard Heuer
Techniques d'Analyse Structurée
Matrice d'hypothèses comparées (ACH)
Biais cognitifs et erreurs de logique
Techniques de manipulation de l'information
Restitution et Diffusion du Renseignement
Partage du Renseignement Technique

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.