

Formation Cyber Threat Intelligence (CTI) – Fondamentaux

Réf. SF34465

Formez-vous aux principes du renseignement sur les menaces grâce à notre formation de référence !

3 j Durée	2 550 € HT Inter / participant	6 150 € HT Intra (≤12 pers.)	0 Sessions à venir
--------------	-----------------------------------	---------------------------------	-----------------------

Objectifs pédagogiques

- ✓ Expliquer le rôle de la CTI et ses principaux cas d'usage (stratégique, opérationnel, tactique/technique)
- ✓ Structurer une analyse en s'appuyant sur des référentiels usuels du marché
- ✓ Cadrer un besoin CTI et sélectionner des sources pertinentes
- ✓ Formaliser et communiquer un renseignement actionnable (note, rapport, briefing) et identifier les modalités de partage
- ✓ Collecter, trier et enrichir des informations de menace en appliquant des principes de validation

Public visé & prérequis

Public viséArchitectes, Auditeurs, Responsables de la sécurité des systèmes d'information (RSSI)

PrérequisConnaissances de base en TCP/IP, sécurité des réseaux et concepts de défense (journalisation, IOC/alerting). Une première exposition aux opérations SOC/IR est un plus.

Programme détaillé

Panorama CTI et cadre de travail

Vocabulaire et périmètre CTI (niveaux de renseignement, acteurs, cas d'usage)
Cycle de vie du renseignement et critères de qualité (fraîcheur, fiabilité, pertinence)
Bonnes pratiques : éthique, conformité, sécurité opérationnelle (OPSEC) et limites de la collecte

Cadrage : définir un besoin de renseignement

Traduire un enjeu métier/sécurité en questions CTI
Priorisation, périmètre, hypothèses, "collection plan" (principes)
Indicateurs de succès et intégration dans les processus existants (SOC/IR/RSSI)

Collecte & qualification des informations (sources et méthodes)

Typologies de sources (publiques/OSINT, communautaires, internes, fournisseurs)
Qualification : fiabilité de la source, validation croisée, gestion des biais
Notions de collecte outillée et d'automatisation (selon contexte)

Analyse & contextualisation de la menace

Structurer l'analyse : éléments observables, hypothèses, contexte, impact
Mise en perspective via des référentiels (ex. MITRE ATT&CK / Kill Chain)
De l'information au renseignement : recommandations et actions possibles (détection, prévention, priorisation)

Industrialisation, partage et communication

Principes d'outillage CTI (TIP / référentiel d'artefacts / gestion du cycle de vie) — exemples possibles selon besoin (MISP, OpenCTI ou équivalent)
Notions de structuration/échange (STIX/TAXII) et gouvernance de diffusion
Production d'un livrable : note de synthèse, rapport, briefing (format et message adaptés aux audiences)

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Cybersécurité et Protection des Données : 4,9/5 — 13 avis

William B. — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Ils nous font confiance

Cette année notre filière Cybersécurité et Protection des Données a accompagné plus de 69 entreprises dont :

AVEM MÉTROPOLE DE LYON ACTIMAGE CONSULTING SAS ADISTA ADVENTIEL AIGA ALCYOR ALDORIA ALSTOM ALTEN SA +59 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com