

Formation Threat Intelligence

Présentation

Cette formation certifiante vous plonge au cœur de la Cyber Threat Intelligence (CTI) pour anticiper, analyser et contrer les menaces cyber. Elle combine fondamentaux, collecte d'indicateurs, IA appliquée et intégration organisationnelle, à travers des études de cas réalistes. À l'issue du parcours, les participants sauront structurer un dispositif CTI opérationnel au sein de leur organisation.

Durée : 21,00 heures (3 jours)

Tarif INTRA : [Nous consulter](#)

Objectifs de la formation

À l'issue de la formation, le stagiaire sera capable de mettre en place un service de renseignement sur les menaces de cyber-attaques grâce à la CTI (Cyber Threat Intelligence)

- Comprendre les fondamentaux de la CTI (Cyber Threat Intelligence)
- Savoir collecter et analyser les informations sur les menaces
- Utiliser l'intelligence artificielle (IA) pour automatiser la collecte, l'analyse et la corrélation d'informations liées aux menaces
- Transformer les données en données exploitables
- Intégrer les outils et méthodes de la CTI dans le processus de sécurité de son organisation

Prérequis

Connaissances de base dans le fonctionnement des systèmes d'information et en cybersécurité.

Public

RSSI, SOC Manager, Analystes SOC, Consultant en cybersécurité ou toute personne en charge de la sécurité d'un système d'information d'entreprise

Programme de la formation



Jour 1. Fondamentaux de la CTI et cycle du renseignement

- Présentation générale de la CTI (Cyber Threat Intelligence)
- Terminologie, périmètre et typologie de la CTI
- Cadres de renseignement : stratégique, opérationnel, tactique, technique
- Présentation du cycle de vie de la CTI : exigences, collecte, traitement, analyse, diffusion, rétroaction

Sources de renseignement & collecte de données

- Classification des sources : OSINT, HUMINT, SIGINT, TECHINT
- Évaluation des sources et des données : pertinence, fiabilité, exactitude
- Respect de l'éthique, de la conformité et de la légalité

Étude de cas : Comment structurer une campagne de collecte orientée menace APT

Jour 2. Analyse des menaces, données exploitables & IA

- Types d'indicateurs (IoC) : IP, domaine, hash, artefacts réseau
- Cartographie des TTP via MITRE ATT&CK
- Acteurs de menace : typologie, motivations, capacités
- Techniques de corrélation et enrichissement

Exercices : Identifier et corréler des IoC extraits de rapports de compromission

Intelligence Artificielle appliquée à la CTI

- Introduction à l'IA dans la cybersécurité : concepts de base
- Apprentissage supervisé / non supervisé appliqué à la détection de menaces
- Corrélation automatisée via modèles prédictifs

Atelier pratique (mise en œuvre d'un mini-algorithme ou démonstration simplifiée) :
Détecter des comportements suspects par approche IA

Jour 3 : Intégration organisationnelle & cas complet

- Architecture d'un programme CTI au sein d'un SOC ou d'un CERT
- Rôles et responsabilités (analyste, RSSI, cellule de veille)
- Flux de renseignement et points d'intégration dans la réponse à incident
- Outils et normes de partage (STIX/TAXII, MISP - en présentation conceptuelle)

Exercice : Concevoir un processus d'intégration CTI dans une organisation type

Conclusion : cas pratique complet d'une détection initiale à l'enrichissement, à l'analyse, jusqu'au rapport final - réalisation en sous-groupe avec restitution orale

- Simulation de scénario ou campagne de phishing ciblée
- Production d'un rapport de Threat Intelligence structuré
- Débrief : Recommandations, décisions de sécurité, lessons learned

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation (*évaluation en ligne dans l'extranet apprenant*)

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.