

Threat Intelligence

Durée: 3 Jours Réf de cours: GKTHREAT Version: 1.0

Résumé:

Cette formation Threat Intelligence (CTI) vous permettra de comprendre pourquoi et comment mettre en place dans votre organisation des services de renseignement sur les menaces afin d'anticiper et de répondre aux cyber-attaques.

Mise à jour : 16.12.2025

Public visé:

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

Objectifs pédagogiques:

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

Pré-requis:

Prérequis :

- | | |
|---|--|
| ■ Connaissances de base dans le fonctionnement des systèmes d'information et en cyber sécurité. | |
|---|--|
-

Contenu:

Jour 1 – Fondamentaux de la CTI et gestion des données	Jour 2 – Collecte, IA et détection intelligente	LAB 6 : Jeu de données ? pipeline de traitement
Démarrage de la formation	Module 3 : IOC/TTP et plateformes CTI	Jour 3 – NLP ; intégration CTI en entreprise
■ Présentation des enjeux, tour de table des participants, identification des attentes, présentation du déroulé pédagogique et des modalités d'évaluation.	■ IOC vs TTP, plateformes : OpenCTI, MISP, MITRE ATT&CK	Module 6 : NLP pour la détection de phishing
Module 1 Introduction à la CTI	■ Intégration entre outils	■ Emails suspects, headers, tokens
■ Définitions, objectifs, sources d'information, OPSEC	LAB 3 : Installation d'OpenCTI ; MISP + corrélation IOC ? TTP	■ Classification de texte et scoring
■ Menaces : typologies, APT, cycles d'attaque	Module 4 : Introduction à l'IA pour la cybersécurité	■ Études de cas réels
■ Sources : OSINT, forums, darknet, honeypots	■ Détection basée ML vs règles, tendances	LAB 7 : Script Python NLP de détection d'un mail de phishing
■ Éthique, cycle de vie du renseignement	■ Biais, pertinence, qualité des données	Module 7 : Architecture CTI d'entreprise
LAB 1 : QCM + étude de sources IOC publiques	LAB 4 : QCM IA + démonstration sur détection réseau	■ Acteurs CTI (SOC, analyste, RSSI)
Module 2 : Structuration de la veille	Module 5 : Détection par IA supervisée/non supervisée	■ Intégration : SIEM, alerting, playbooks
Présentation d'outils : MindMap, Obsidian, Notion	■ KNN, SVM, clustering, arbre de décision	■ Rôles, processus, indicateurs de pilotage
■ Structuration des données CTI et taxonomie	■ Prétraitement, vectorisation, features	LAB 8 : Atelier : construction d'une architecture cible CTI
LAB 2 : Installation, collecte et annotation IOC dans un outil de prise de notes	LAB 5 : Modélisation simple sur base IOC	■ Clôture de la formation

Méthodes pédagogiques :

Démarche pédagogique Alternance entre apports théoriques, démonstrations techniques, et labs pratiques encadrés Études de cas réels (APT, phishing, IOC) Apprentissage basé sur la mise en œuvre directe d'outils CTI et de scripts d'intelligence artificielle Utilisation de supports numériques interactifs, QCM, échanges guidés, quiz collectifs

Répartition Théorie / Pratique 40 % Théorie : (concepts, méthodes, architecture CTI, IA appliquée, NLP) 60 % Pratique : (labs d'installation, configuration, analyse IOC/TTP, scripts Python NLP/ML, tests d'intégration OpenCTI/MISP)

Méthodes pédagogiques

La formation repose sur une alternance entre apports théoriques (40%) et travaux pratiques (60 %)

L'animation participative via des outils collaboratifs, partages d'écran, analyses d'études de cas, exercices collaboratifs et activités de groupe simulant des contextes réels.

Accès à un espace de partage sécurisé contenant : Le support de cours officiel au format électronique Les QCM d'entraînement Les fichiers d'exercices et corrigés Les modèles de documents utilisés dans les travaux pratiques

Matériel fourni : Support de cours au format électronique Documentation synthétique utilisable en contexte professionnel après la formation

Suivi qualité et évaluation

Avant la formation : Questionnaire de positionnement / diagnostic envoyé aux participants afin de recueillir les attentes, le niveau initial et détecter d'éventuels besoins spécifiques (techniques, pédagogiques ou liés à l'accessibilité)

Pendant la formation : Évaluation à chaud en fin de première journée pour recueillir les ressentis immédiats et ajuster l'animation pédagogique si besoin Quiz, exercices, cas pratiques Mises en situation Échanges pédagogiques avec le formateur

À l'issue de la formation : Questionnaire de satisfaction à chaud (participant + formateur) Une attestation de suivi de fin de formation sera délivrée à chaque participant

Suivi d'exécution : Une feuille d'émargement est signée numériquement chaque demi-journée par les participants et le formateur En distanciel, la traçabilité de la présence est assurée via l'outil collaboratif (statistiques de connexions synchrones) et les échanges interactifs

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur