Threat Intelligence

Durée: 3 Jours Réf de cours: GKTHREAT Version: 1.0 Méthodes d'apprentissage: Intra-entreprise & sur-mesure

Résumé:

Cette formation Threat Intelligence (CTI) vous permettre 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
- 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

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

Démarrage de la formation

- Présentation des enjeux, tour de table des participants, identification des attentes, présentation du déroulé pédagogique et des modalités d'évaluation.

Module 1 Introduction à la CTI

- Définitions, objectifs, sources d'information, OPSEC
- Menaces : typologies, APT, cycles d'attaque
- Sources : OSINT, forums, darknet, honeypots
- Éthique, cycle de vie du renseignement

LAB 1 : QCM + étude de sources IOC publiques

Module 2 : Structuration de la veille

Présentation d'outils : MindMap, Obsidian, Notion

- Structuration des données CTI et taxonomie

LAB 2 : Installation, collecte et annotation IOC dans un outil de prise de notes

Jour 2 – Collecte, IA et détection intelligente

Module 3 : IOC/TTP et plateformes CTI

- IOC vs TTP, plateformes : OpenCTI, MISP, MITRE ATT;CK
- Intégration entre outils

LAB 3 : Installation d'OpenCTI ; MISP + corrélation IOC ? TTP

Module 4 : Introduction à l'IA pour la cybersécurité

- Détection basée ML vs règles, tendances
- Biais, pertinence, qualité des données

LAB 4 : QCM IA + démonstration sur détection réseau

Module 5 : Détection par IA supervisée/non supervisée

- KNN, SVM, clustering, arbre de décision
- Prétraitement, vectorisation, features

LAB 5 : Modélisation simple sur base IOC

LAB 6 : Jeu de données ? pipeline de traitement

Jour 3 – NLP ; intégration CTI en entreprise

Module 6 : NLP pour la détection de phishing

- Emails suspects, headers, tokens
- Classification de texte et scoring
- Études de cas réels

LAB 7 : Script Python NLP de détection d'un mail de phishing

Module 7 : Architecture CTI d'entreprise

- Acteurs CTI (SOC, analyste, RSSI)
- Intégration : SIEM, alerting, playbooks
- Rôles, processus, indicateurs de pilotage

LAB 8 : Atelier : construction d'une architecture cible CTI

- Clôture de la formation

Méthodes pédagogiques :

Démarche pédagogiqueAlternance 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 / Pratique40 % 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'entraînementLes fichiers d'exercices et corrigésLes 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 besoinQuiz, exercices, cas pratiquesMises en situationÉchanges 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