New

Threat Intelligence

Anticiper les attaques grâce à l'analyse des données de cybermenace

Présentiel ou en classe à distance

3 jours (21 h)

Prix inter : 2.890,00 € HT
Forfait intra : 7.690,00 € HT

Réf.: MG230

Threat Intelligence offre une approche complète et opérationnelle du **renseignement sur les menaces cyber**, indispensable aux organisations confrontées à des attaques toujours plus ciblées et sophistiquées. Elle permet de comprendre les fondamentaux de la CTI, le **cycle du renseignement**, les typologies de menaces (APT, cybercriminels, hacktivistes, insiders) ainsi que l'utilisation du framework **MITRE ATT&CK** pour analyser les tactiques, techniques et procédures des attaquants. Les participants apprennent à exploiter efficacement des sources internes (SIEM, EDR, pare-feux) et externes (OSINT, CERT, ISAC, dark web), à structurer les indicateurs (IOC, IOA, TTP) et à utiliser des formats normalisés comme STIX/TAXII pour professionnaliser leur démarche de veille et d'analyse.

A qui s'adresse cette formation ?

Pour qui

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

Prérequis

- Connaissances de base dans le fonctionnement des systèmes d'information et en cyber sécurité
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Introduction à la Cyber Threat Intelligence

- Définition et objectifs de la CTI
- Enjeux métiers : anticipation, détection, réduction de risque
- Le cycle du renseignement : direction, collecte, traitement, analyse, diffusion
- Typologie des CTI : stratégique, tactique, opérationnelle, technique
- Cadre légal et éthique : usage des données, RGPD, confidentialité
- Responsabilité sociétale et CTI : enjeux éthiques, transparence et souveraineté des données

Atelier

Élaboration d'un cycle de renseignement personnalisé selon le métier du stagiaire

2 - Typologie des menaces et acteurs malveillants

- Menaces ciblées vs opportunistes
- Panorama des acteurs : APT, hacktivistes, cybercriminels, insiders
- TTP (Tactics, Techniques, Procedures) et MITRE ATT&CK
- Étude de cas : analyse d'un rapport APT (ex : APT29, LockBit)
- Corrélation entre groupe, tactiques, cibles, secteur d'activité

Atelier

Mapping d’un groupe APT sur le MITRE ATT&CK et extraction des techniques clés

3 - Collecte et enrichissement de la donnée CTI

- Sources internes : SIEM, EDR, pare-feux, honeypots
- Sources externes : OSINT, ISAC, CERT, plateformes CTI, darkweb
- Outils de collecte : MISP, TheHive, OpenCTI, ThreatFox
- Types d’indicateurs : IOCs (hash, IP, domaine), IOAs, TTPs
- Normalisation et format : STIX, TAXII, JSON, YAML

Atelier

mise en oeuvre d’une collecte manuelle et automatisée d’indicateurs de compromission (IOCs) à partir de sources publiques, puis parsing et structuration des données obtenues selon des formats normalisés

4 - Automatiser la CTI avec l’IA et les outils spécialisés

- IA pour résumer, classer, corréler des rapports et bulletins de menace
- Extraction d’entités et résumé avec LLM (ChatGPT, Claude, etc.)
- Enrichissement automatisé d’IOCs (Virustotal API, AbuseIPDB, WHOIS)
- Interconnexion Cortex ↔ MISP ↔ TheHive
- Alertes et corrélations automatiques dans un SIEM avec règles Sigma + CTI

Atelier

Utilisation d’un LLM pour résumer et corréler un rapport de menace. Automatiser l’enrichissement d’une liste d’IOCs à l’aide de sources externes et d’outils spécialisés

5 - Transformer les données CTI en renseignement exploitable

- Qualification : contexte, fiabilité, vérifiabilité des sources
- Attributions : pièges et méthodes (analyse indirecte, pivot, infrastructures)
- Analyse comportementale : MITRE, Kill Chain, Diamond Model
- Visualisation et structuration du renseignement (graphes, liens, narratifs)
- Production de livrables : fiche IOC, rapport analytique, alerte synthétique

Atelier

Construction d’un rapport CTI court à destination d’un SOC Manager avec recommandations concrètes

6 - Intégrer la CTI dans l’organisation

- Positionnement d’une cellule CTI ou analyste CTI dans un SOC/CERT
- Flux CTI entrants / sortants : playbooks, enrichissement SIEM, contribution à MISP
- Intégration dans les processus de détection, réponse à incident, gestion de crise
- Veille structurée : abonnements, plateformes, automatisation de la collecte
- Étude de cas : intégration CTI dans une détection de ransomware ciblé

Atelier

Mise en situation d’un incident ciblé, avec analyse de l’apport du renseignement CTI dans les processus de réaction et d’investigation

Les objectifs de la formation

- 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

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- L'apprentissage par la pratique : les phases théoriques sont complétées d'ateliers favorisant un ancrage durable des acquis
- Les nombreux retours d'expérience et conseils des consultants spécialistes du sujet
- Utilisation d'environnements proches du contexte professionnel

Dates et villes 2026 - Référence MG230

Dernières places disponibles Session garantie

A distance

du 20 avr. au 22 avr.	du 21 sept. au 23 sept.	du 14 déc. au 16 déc.
du 15 juin au 17 juin	du 26 oct. au 28 oct.	

Rennes

du 20 avr. au 22 avr.	du 21 sept. au 23 sept.	du 14 déc. au 16 déc.

Paris

du 20 avr. au 22 avr.	du 21 sept. au 23 sept.	du 14 déc. au 16 déc.
du 15 juin au 17 juin	du 26 oct. au 28 oct.	

Lyon

du 20 avr. au 22 avr.	du 21 sept. au 23 sept.	du 14 déc. au 16 déc.

Nantes

du 20 avr. au 22 avr.	du 21 sept. au 23 sept.	du 14 déc. au 16 déc.

Toulouse

du 15 juin au 17 juin	du 26 oct. au 28 oct.

Strasbourg

du 15 juin au 17 juin	du 26 oct. au 28 oct.

Sophia Antipolis

du 15 juin au 17 juin	du 26 oct. au 28 oct.

Rouen

du 15 juin au 17 juin	du 26 oct. au 28 oct.

Aix-en-Provence

du 15 juin au 17 juin	du 26 oct. au 28 oct.

Lille

du 15 juin au 17 juin	du 26 oct. au 28 oct.