+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 22/08/2025

S'inscrire

Formation Threat Intelligence

3 jours (21 heures)

Présentation

Notre formation « Threat Intelligence » vous permettra de comprendre le fonctionnement d'un programme de renseignement cyber, d'identifier les sources pertinentes, de traiter les indicateurs de compromission (IOC) et d'automatiser les processus grâce à l'Intelligence Artificielle.

Vous saurez mettre en place et intégrer une cellule CTI dans un SOC, utiliser les outils d'OSINT, structurer un flux de renseignement, ou encore produire des rapports à destination des analystes, des équipes IT ou des décideurs. L'accent sera mis sur la transformation des données brutes en renseignement exploitable pour la détection, la réponse aux incidents et la prise de décision stratégique.

La Threat Intelligence s'intègre à l'architecture de sécurité existante en renforçant la détection des menaces, la réaction aux incidents et la chasse proactive (threat hunting). Grâce à l'IA, vous pourrez automatiser la veille, prioriser les alertes et améliorer le temps de réponse. Vous apprendrez également à définir une gouvernance CTI (workflow, rôles, responsabilités) afin d'assurer une diffusion efficace et adaptée du renseignement dans l'organisation.

À la suite de notre formation, vous serez en mesure de mettre en place un service de renseignement sur les menaces, d'en exploiter les données dans votre environnement métier, et d'utiliser les outils adaptés (MISP, frameworks MITRE, flux OSINT, etc.).

Objectifs

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

Public visé

- RSSI
- SOC Manager
- Analyste SOC
- Consultant en cybersécurité
- Personne en charge de la sécurité d'un système d'information d'entreprise

Pré-requis

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

Formation Cyber Threat Intelligence (CTI) – Collecte, Analyse & Automatisation OSINT

[Jour 1 - Matin]

Fondamentaux & cadre de la CTI

- Cycle du renseignement : planification ? collecte ? analyse ? diffusion ? retour
- Typologie CTI : stratégique, tactique, opérationnel, technique
- Enjeux organisationnels de la CTI (place dans une stratégie de cybersécurité, relations RSSI/DPO/DIRCOM).
- Cas d’usage par profil cible : RSSI (pilotage), SOC (détection), IR (réponse).
- Menaces, motivations et surfaces d’attaque (APT, cybercrime, hacktivisme…)
- Formats & vocabulaires : IOC/IOA, TTP, MITRE ATT&CK, kill chain, STIX/TAXII (intro)
- Atelier pratique : Analyse d’une cyberattaque récente ? extraction des éléments CTI utiles

[Jour 1 - Après-midi]

Collecte d’informations – Méthodes conventionnelles

- Cartographie des sources : ouvert (sites officiels, CERT, blogs, RSS), communautés sectorielles, rapports éditeurs, logs internes
- Techniques manuelles de veille : plan de requêtes, opérateurs avancés, suivi RSS/newsletters, vérification d’authenticité
- Critères de qualité : fiabilité, fraîcheur, pertinence, biais, couverture sectorielle
- Journal de collecte & traçabilité (chaîne de custody, citation des sources)
- Atelier pratique : Construire un plan de collecte + grille d’évaluation des sources (score qualité)

[Jour 2 - Matin]

Collecter, trier & qualifier (approche conventionnelle)

- Ingestion manuelle multi-formats (CSV/JSON/PDF/web) et normalisation de base
- Nettoyage : dédoublonnage, désambiguïsation d'entités, enrichissements simples (WHOIS, GeoIP, ASN, réputation publique)
- Qualification : scoring de la source & de l'indicateur (confiance, contexte, secteur, temporalité)
- Pré-structuration vers STIX « light » (objets simples : indicator, malware, relationship)
- Atelier pratique : Nettoyer et qualifier un lot d'IOC issus de plusieurs flux

[Jour 2 - Après-midi]

Analyser & corréler (approche conventionnelle)

- Pivoting & liens : domaines ? IP ? hash ? infra, construction de timelines
- Cartographie MITRE ATT&CK & kill chain pour dégager les TTP dominants
- Détection de patterns récurrents (campagnes, fournisseurs d'infra, heures d'activité)
- Restitution : rapport analyste (technique) vs executive brief (décisionnel)
- IA appliquée à la corrélation et à la détection de patterns récurrents (clustering, scoring automatique des IOC avec LLM/ML).
- Démonstration d'un outil open source ou sandbox IA appliqué à la CTI.
- Atelier pratique : Corrélation multi-sources + rédaction d'un one-pager actionnable

[Jour 3 - Matin]

Collecte & analyse augmentées par l'IA (OSINT + corrélation automatisée)

- Pipelines OSINT automatisés : RSS enrichis, crawlers/scrapers conformes, API publiques
- Usage raisonné de l'IA/LLM : classification thématique, déduplication, extraction d'IOC, résumé et corrélation contextuelle (pas d'analyse prédictive)
- Connecteurs STIX/TAXII : packaging & échange normalisés des indicateurs collectés
- Gouvernance & conformité : limites légales, RGPD, TOU, réduction des biais, validation humaine
- Atelier pratique : Monter un mini-pipeline (flux publics) ? extraction, déduplication, résumé & export STIX « light »

[Jour 3 - Après-midi]

Intégration dans un cadre opérationnel

- TIP/MISP : import, déconfliction, scoring, partage contrôlé
- SIEM/SOAR : transformer le renseignement en use cases (règles, alertes, playbooks)
- Threat hunting guidé CTI & enrichissement des investigations IR
- Mesure & pilotage : KPI/KRI CTI (taux de faux positifs, MTTD/MTTR, couverture ATT&CK), boucle d'amélioration
- Mise en place d'un service CTI complet
- Atelier pratique : Concevoir un mini-service CTI (workflow collecte ? validation ? diffusion ? action, matrice RACI, plan de diffusion interne/externe)

Livrables & acquis

- Plan de collecte conventionnelle + grille de scoring des sources
- Jeu d'IOC nettoyés & qualifiés + mini-taxonomie STIX « light »
- Executive one-pager et rapport analyste
- Pipeline OSINT auto (IA collecte + tri + résumé + corrélation) + export STIX
- Use cases SIEM/SOAR, playbook de réponse, KPI de pilotage CTI
- Charte d'usage CTI, matrice RACI et plan de mise en place d'un service CTI (document de synthèse de fin de formation)

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.