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

Mis à jour le 03/03/2026

S'inscrire

Formation Certification Ec-council CTIA™

3 jours (21 heures)

Présentation

La formation EC-Council CTIA™ vous apprend à conduire une investigation de cybermenace de bout en bout : collecte, analyse, corrélation et restitution. Elle s'adresse aux contextes SOC, réponse à incident et chasse aux menaces, pour accélérer la détection et réduire le temps de remédiation.

Vous travaillez sur une démarche structurée : cadrage d'un cas, définition d'hypothèses, acquisition de données (logs, endpoints, réseau) et analyse orientée preuves. L'accent est mis sur la traçabilité, la qualité des indicateurs et la priorisation des actions.

Cette formation privilégie l'approche pratique via ateliers et démos : investigation d'alertes, enrichissement OSINT, cartographie MITRE ATT&CK, et rédaction de rapports. Livrables : playbooks d'investigation, checklists de collecte, modèles de rapport et tableaux de bord d'indicateurs.

Objectifs

- Qualifier une alerte et formuler des hypothèses d'attaque.
- Collecter et préserver des artefacts pertinents (logs, mémoire, disque).
- Corréler des événements multi-sources pour reconstruire une chronologie.
- Enrichir et valider des IOC/TTP avec des sources de threat intel.
- Produire un rapport actionnable et des recommandations de remédiation.

Public visé

- Analystes SOC (N1 à N3)
- Équipes CERT/CSIRT et réponse à incident
- Administrateurs sécurité / ingénieurs sécurité
- Auditeurs techniques souhaitant renforcer l'investigation

Pré-requis

- Notions de réseaux TCP/IP, DNS, HTTP/TLS
- Compréhension des journaux Windows et Linux
- Bases de sécurité : authentification, privilèges, malware
- Lecture de commandes et scripts simples (PowerShell/Bash)

Pré-requis techniques

- PC avec 16 Go RAM recommandés (8 Go minimum) et 40 Go d’espace libre
- OS : Windows 10/11 ou Linux récent (ou Windows avec WSL2)
- Outils : navigateur moderne, terminal, éditeur de texte, Wireshark, Sysinternals
- Accès admin local pour installer des outils et exécuter des captures

Programme de notre formation Ec-council CTIA

[Jour 1 - Matin]

Fondamentaux CTIA et cadre d’une investigation

- Rôles et responsabilités de l’analyste en Threat Intelligence (CTI vs SOC vs DFIR)
- Cycle du renseignement : planification, collecte, traitement, analyse, diffusion
- Typologie des menaces : cybercriminels, APT, hacktivisme, insider
- Définir le périmètre : objectifs, contraintes, niveaux de classification, règles d’engagement
- Atelier pratique : Formaliser une demande CTI (PIR) et un plan de collecte.

[Jour 1 - Après-midi]

Collecte OSINT et hygiène opérationnelle

- Sources OSINT : moteurs, réseaux sociaux, dépôts de code, registres, forums, paste sites
- Techniques de recherche : opérateurs avancés, pivoting, enrichissement par recoupement
- Gestion des identités et cloisonnement : comptes dédiés, navigation isolée, traces et métadonnées
- Validation et fiabilité : biais, corroboration, horodatage, conservation des preuves
- Atelier pratique : Construire une checklist OSINT et collecter des artefacts sur une cible fictive.

[Jour 2 - Matin]

Analyse des indicateurs et normalisation (IOC/TTP)

- Différencier IOC, IOA et TTP et choisir le bon niveau de granularité
- Extraction d’artefacts : domaines, URLs, IP, hashes, certificats, user-agents, patterns
- Enrichissement : WHOIS/DNS, ASN, réputation, passive DNS, relations infrastructurelles
- Déduplication, scoring et priorisation : pertinence, fraîcheur, impact, confiance
- Atelier pratique : Enrichir une liste d’IOC et produire une synthèse exploitable.

[Jour 2 - Après-midi]

Modélisation de l’adversaire et attribution

- Cartographier les TTP avec MITRE ATT&CK (tactiques, techniques, sous-techniques)
- Construire un profil d’acteur : motivations, capacités, secteurs ciblés, géographies, outillage
- Attribution : niveaux de preuve, limites, faux drapeaux, hypothèses et incertitudes
- Production d’un dossier : chronologie, infrastructure, malware, campagnes, recommandations
- Atelier pratique : Mapper une campagne à ATT&CK et rédiger une note d’attribution argumentée.

[Jour 3 - Matin]

Industrialisation CTI et partage (STIX/TAXII)

- Structurer l’information : objets, relations et bonnes pratiques de description
- Introduction à STIX 2.x : indicators, malware, threat-actor, intrusion-set, sightings
- Transport et diffusion via TAXII : collections, abonnements, contrôle d’accès
- Intégration dans l’écosystème : TIP, SIEM, SOAR, EDR (cas d’usage et limites)
- Atelier pratique : Modéliser une campagne en STIX et préparer un paquet de partage.

[Jour 3 - Après-midi]

Restitution, détection et plan d’action

- Formats de livrables : bulletin, alerte, rapport stratégique, fiche acteur, executive summary
- Traduire CTI en détection : règles SIEM, requêtes, watchlists, YARA/Suricata (principes)
- Mesurer l’efficacité : KPI/KRI, couverture ATT&CK, taux de faux positifs, retours des équipes
- Gouvernance : gestion des sources, cycle de vie des IOC, rétention, conformité et confidentialité
- Atelier pratique : Produire un rapport CTI complet et un plan de détection priorisé.

FAQ – QUESTIONS / RÉPONSES

Dans quelle langue la formation CTIA™ vous est enseignée ?

La formation est en français.

L’examen est-il compris dans le prix de la formation ?

Oui, le prix de la certification est inclus au coût de la formation ($450 à titre indicatif). Vous pourrez passer l'examen à la fin de la session.

Comment se déroule l'examen pour la certification CTIA™ ?

L'examen consiste en un QCM basé sur la performance composé de 50 **questions** maximum.

Il s'effectue en ligne dans un centre d'examen agréé Pearson Vue.

Cet examen dure **120 minutes**, les langues disponibles sont l'anglais

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.