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

Mis à jour le 02/09/2026

S'inscrire

Formation Certification Certified Junior Detection Engineer

Présentation

La Formation Certification Certified Junior Detection Engineer vous prépare à la certification officielle Certified Junior Detection Engineer (CJDE) et aux compétences fondamentales de détection des menaces attendues dans un SOC moderne.

Cette formation de niveau intermédiaire vous permet de consolider les connaissances nécessaires pour concevoir, tester et améliorer des détections exploitables. Vous aborderez les fondamentaux réseau,Windows, Linux, l'analyse des journaux et les méthodes de réponse aux incidents utiles à l'examen CJDE.

Vous apprendrez à créer des règles avec Sigma et YARA, à analyser les données réseau avec Zeek, puis à exploiter les capacités de plateformes SIEM telles que Splunk, Elastic et Graylog. L'objectif est de développer une démarche de détection structurée, contextualisée et mesurable.

Le parcours couvre également l'intégration de la threat intelligence, le réglage des alertes, l'analyse comportementale, les bases de Python et les pratiques Git appliquées à la détection. Les exercices s'appuient sur des scénarios réalistes pour rapprocher la préparation de situations rencontrées en environnement opérationnel.

À l'issue de la formation, vous serez en mesure de vous préparer efficacement à l'examen pratique de la certification Certified Junior Detection Engineer (CJDE). Vous disposerez des repères nécessaires pour analyser une menace, développer une détection, réduire les faux positifs et présenter une démarche de validation cohérente.

Objectifs

- Comprendre les domaines de compétences évalués par la certification Certified Junior Detection Engineer (CJDE).
- Analyser des données réseau, système et applicatives pour identifier des comportements suspects.
- Créer et valider des règles de détection avec Sigma, YARA et des requêtes SIEM.
- Régler les détections afin d'améliorer leur pertinence et de limiter les faux positifs.
- Intégrer la threat intelligence et l'analyse comportementale dans un processus de détection.
- Se préparer aux cas pratiques et au format de l'examen CJDE.

Public visé

- Analyste SOC
- Analyste détection
- Ingénieur détection
- Administrateur SIEM
- Analyste réponse à incident

Pré-requis

- Connaissances fondamentales en cybersécurité et en fonctionnement d'un SOC.
- Maîtrise des notions de base des réseaux TCP/IP, DNS et HTTP.
- Pratique initiale des environnements Windows et Linux.
- Capacité à lire des journaux techniques et à utiliser des requêtes simples.
- Notions de script avec Python ou langage équivalent.

Pré-requis techniques

- Poste sous Windows 10 ou 11, macOS ou distribution Linux récente.
- Processeur double coeur minimum,8 Go de RAM recommandés et espace disque disponible pour les fichiers de travail.
- Navigateur récent Google Chrome, Mozilla Firefox ou Microsoft Edge, avec les mises à jour installées.
- Connexion Internet stable, sans filtrage de sécurité bloquant les plateformes de laboratoire, les téléchargements et les accès aux services de formation.
- Droits d'installation ou accès à un environnement de travail permettant d'utiliser Visual Studio Code et Git.

Programme de notre formation Certified Junior Detection Engineer

[Jour 1 - Matin]

Fondamentaux de la détection et cadrage de la certification

- Positionnement de la certification Certified Junior Detection Engineer (CJDE) et compétences attendues.
- Rôle de l'ingénierie de détection dans un SOC, distinction avec le threat hunting et la réponse à incident.
- Cycle de vie d'une détection, de l'hypothèse de menace au suivi de la qualité.
- Panorama des sources de télémétrie, journaux endpoint, réseau, identité et applications.
- Révision des concepts TCP/IP, DNS, HTTP, routage et services réseau utiles à l'analyse.
- Atelier pratique : cartographier les sources de logs d'un SOC fictif et associer chaque source aux menaces qu'elle peut aider à détecter.

[Jour 1 - Après-midi]

Analyse système et réponse à incident

- Artefacts de sécurité essentiels sous Windows et Linux.
- Lecture des journaux d'authentification, de processus, de services et d'activité système.
- Chaîne d'analyse d'une alerte, qualification, enrichissement, priorisation et escalade.
- Indicateurs de compromission, comportements suspects et éléments de preuve.
- Rappels sur le confinement, la conservation des éléments utiles et le retour d'expérience.
- Atelier pratique : qualifier une alerte d'authentification suspecte à partir de journaux Windows et Linux, puis rédiger les actions de réponse initiales.

[Jour 2 - Matin]

Réseau et télémétrie de sécurité

- Analyse des flux réseau, des sessions, des protocoles et des métadonnées.
- Utilisation de Wireshark et tcpdump pour examiner le trafic suspect.
- Repérage des anomalies DNS, des connexions sortantes inhabituelles et des communications de commande et contrôle.
- Compréhension des logs de pare-feu, proxy, IDS et équipements réseau.
- Construction d'hypothèses de détection à partir de techniques d'attaque observables sur le réseau.
- Atelier pratique : analyser une capture réseau pour identifier une activité suspecte, extraire les indicateurs pertinents et définir une logique de détection.

[Jour 2 - Après-midi]

Détection réseau avec Zeek

- Architecture et objectifs de Zeek dans une stratégie de détection réseau.
- Lecture des principaux journaux Zeek, connexions, DNS, HTTP, SSL et fichiers.
- Corrélation des événements réseau pour construire un scénario d'investigation.
- Identification de comportements liés à l'exfiltration, au scan, au beaconing et aux téléchargements suspects.
- Principes de création, de test et d'ajustement d'une détection fondée sur la télémétrie réseau.
- Atelier pratique : exploiter des logs Zeek pour détecter un schéma de beaconing et documenter les critères de réglage de la détection.

[Jour 3 - Matin]

Règles Sigma et détection portable

- Principes de la détection déclarative avec Sigma et structure d'une règle.
- Choix des champs, opérateurs, conditions et métadonnées pour une détection maintenable.
- Traduction d'un scénario de menace en logique de détection basée sur les événements.
- Bonnes pratiques de versionnement, de documentation et de validation d'une règle.
- Limites des règles génériques et adaptation au contexte de collecte de l'organisation.
- Atelier pratique : écrire une règle Sigma de détection d'exécution suspecte, la tester sur des événements fournis et améliorer ses conditions.

[Jour 3 - Après-midi]

YARA et analyse orientée malware

- Objectifs de YARA pour l'identification de fichiers et de familles de malwares.
- Syntaxe des règles, chaînes, conditions, modificateurs et bonnes pratiques de lisibilité.
- Différence entre indicateurs statiques, signatures fragiles et comportements détectables.
- Exploitation d'artefacts de fichiers pour enrichir une investigation et une détection.
- Validation des règles YARA, maîtrise des faux positifs et documentation des limites.
- Atelier pratique : concevoir une règle YARA à partir d'échantillons inoffensifs et d'artefacts fournis, puis évaluer sa précision.

[Jour 4 - Matin]

SIEM, requêtes et réglage des alertes

- Fonctions d'un SIEM dans la centralisation, la recherche et la corrélation des événements.
- Approches de requêtage dans Splunk, Elastic et Graylog.
- Construction d'une détection à partir d'une requête, d'un seuil ou d'une séquence d'événements.
- Mesure de la qualité, taux de faux positifs, couverture, criticité et exploitabilité des alertes.
- Méthode de tuning, exceptions justifiées, listes d'autorisation et conservation de la visibilité.
- Atelier pratique : créer une requête de détection dans un SIEM, analyser les résultats et la régler pour réduire les alertes non pertinentes.

[Jour 4 - Après-midi]

Threat intelligence et détection comportementale

- Différences entre renseignement stratégique, opérationnel et tactique.
- Évaluation de la fiabilité, de la fraîcheur et de la pertinence des indicateurs de compromission.
- Intégration de la threat intelligence dans les recherches, les règles et les investigations.

- Approche comportementale, lignes de base, anomalies et détections résistantes aux changements d'indicateurs.
- Apports et limites de l'IA dans les flux de travail de détection et de priorisation.
- Atelier pratique : enrichir un cas de compromission avec des indicateurs et concevoir une détection comportementale complémentaire.

[Jour 5 - Matin]

Detection as Code et industrialisation

- Principes de Detection as Code pour rendre les règles traçables, réutilisables et contrôlées.
- Utilisation de Git, commits, branches et revues de code appliqués aux contenus de détection.
- Organisation d'un dépôt de règles, conventions de nommage et gestion des métadonnées.
- Stratégie de tests, jeux de données de validation et contrôle des régressions.
- Préparation du déploiement, suivi post-déploiement et amélioration continue des détections.
- Atelier pratique : versionner une règle Sigma dans un dépôt Git, documenter son objectif et préparer un plan de test avant déploiement.

[Jour 5 - Après-midi]

Révision et préparation à l'examen pratique

- Révision transversale des domaines couverts par la certification Certified Junior Detection Engineer (CJDE).
- Analyse de scénarios de type examen, collecte des éléments, priorisation et justification technique.
- Méthode de gestion du temps pour une évaluation pratique longue durée.
- Vérification des livrables, clarté des conclusions, traçabilité des décisions et qualité de la documentation.
- Identification des axes de révision individuels, des erreurs fréquentes et des réflexes à adopter avant l'examen.
- Atelier pratique : réaliser une mise en situation de synthèse combinant analyse de logs, création de règle, réglage et restitution d'un cas de détection.

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.