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

Mis à jour le 22/09/2026

S'inscrire

Formation Certification Cisco CCNP Cybersecurity

5 jours (35 heures)

Présentation

La certification Cisco CCNP Cybersecurity valide des compétences avancées dans les opérations de cybersécurité, l'analyse des menaces, le Threat Hunting et la défense contre les attaques au sein d'environnements complexes.

Notre formation Cisco CCNP Cybersecurity vous prépare aux examens 350-201 CBRCOR et 300-220 CBRTHD du parcours de certification retenu. Elle vous permettra de développer les compétences nécessaires pour analyser les risques, détecter les activités malveillantes et conduire des investigations avancées.

Vous apprendrez à exploiter la Threat Intelligence, à modéliser les menaces avec MITRE ATT&CK et à identifier les tactiques, techniques et procédures utilisées par les attaquants. Vous serez également en mesure de construire des hypothèses de Threat Hunting et de rechercher les traces d'une compromission dans les données réseau, endpoints, applications et environnements Cloud.

La formation aborde également les playbooks de réponse aux incidents, l'analyse des attaques avancées, les gaps de détection et l'automatisation des opérations de sécurité. Vous apprendrez à transformer les résultats de vos investigations en nouvelles capacités de détection et en mesures de remédiation adaptées.

À l'issue de cette formation, vous serez capable de conduire une investigation SOC avancée, d'industrialiser vos processus de Threat Hunting et d'améliorer la posture de défense de votre organisation. Vous disposerez également des connaissances nécessaires pour préparer les examens 350-201 CBRCOR et 300-220 CBRTHD permettant d'obtenir la certification Cisco CCNP Cybersecurity dans le parcours retenu.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie Cisco CyberOps Professional (1.2) et ses nouveautés.

Objectifs

- Préparer les examens 350-201 CBRCOR et 300-220 CBRTHD
- Maîtriser les processus avancés d'opérations de cybersécurité et de réponse aux incidents
- Exploiter la Threat Intelligence et les modèles de menace pour analyser les comportements adverses
- Conduire des campagnes de Threat Hunting sur les endpoints, réseaux, applications et environnements Cloud
- Identifier les gaps de détection et renforcer les capacités de surveillance et de défense
- Automatiser et industrialiser les processus d'investigation, de détection et de remédiation

Public visé

- Analystes SOC expérimentés
- Analystes cybersécurité
- Threat Hunters
- Ingénieurs sécurité
- Consultants cybersécurité
- Professionnels préparant la certification Cisco CCNP Cybersecurity

Pré-requis

- Bonne maîtrise des fondamentaux de la cybersécurité et des réseaux TCP/IP
- Expérience pratique de l'analyse des logs, événements et alertes de sécurité
- Connaissances des processus de détection et de réponse aux incidents
- Connaissances des systèmes Windows et Linux et des principales sources de télémétrie de sécurité
- Des notions de Python ou PowerShell sont recommandées pour les exercices d'automatisation et de Threat Hunting
- Une expérience en SOC ou des compétences équivalentes à la CCNA Cybersecurity sont recommandées

Pré-requis techniques

- Ordinateur portable avec 8 Go de RAM minimum et droits d'administration
- Connexion Internet stable pour accéder aux labs et ressources nécessaires à la formation
- Navigateur web récent : Chrome, Firefox ou Edge
- Environnement permettant d'utiliser les outils d'analyse réseau, de logs et les scripts nécessaires aux exercices
- Client SSH et outils fournis ou indiqués par le formateur pour les travaux pratiques

Note : Ambient IT n'est pas propriétaire des certifications Cisco. Ces certifications appartiennent à Cisco Systems, Inc.

Programme de notre formation Certification Cisco CCNP Cybersecurity

[Jour 1 - Matin]

Maîtriser les opérations de cybersécurité et la gestion des risques

- Comprendre les domaines des examens 350-201 CBRCOR et 300-220 CBRTHD
- Analyser les relations entre actifs, vulnérabilités, menaces, impacts et risques
- Comprendre les rôles et responsabilités des équipes SOC et des analystes cybersécurité
- Évaluer la posture de sécurité d'un système ou d'une infrastructure et identifier les écarts de configuration
- Comprendre les politiques, standards et mécanismes de gestion du risque appliqués aux opérations de sécurité
- Atelier pratique : analyser un scénario de compromission et construire une évaluation des risques et des mesures de sécurité associées.

[Jour 1 - Après-midi]

Construire des playbooks et gérer la réponse aux incidents

- Comprendre la structure et les composants d'un playbook de sécurité
- Appliquer les différentes étapes du processus de réponse aux incidents
- Définir les actions de qualification, confinement, éradication, récupération et escalade
- Mettre en œuvre les principes de durcissement, segmentation et réduction de la surface d'attaque
- Utiliser les métriques d'Incident Response pour mesurer et améliorer l'efficacité des opérations
- Atelier pratique : construire et exécuter un playbook de réponse à un incident puis définir les actions de durcissement nécessaires.

[Jour 2 - Matin]

Exploiter la Threat Intelligence et modéliser les menaces

- Collecter et exploiter les indicateurs de compromission issus de différentes sources
- Comprendre le fonctionnement d'une Threat Intelligence Platform (TIP) et le cycle de vie du renseignement
- Interpréter les rapports de Threat Intelligence et identifier les tactiques, techniques et procédures
- Modéliser les menaces avec MITRE ATT&CK, MITRE CAPEC, TaHiTI et PASTA
- Construire et prioriser des hypothèses de Threat Hunting à partir des renseignements disponibles
- Atelier pratique : enrichir des indicateurs de compromission puis modéliser un scénario d'attaque avec MITRE ATT&CK.

[Jour 2 - Après-midi]

Analyser les Threat Actors et attribuer les activités malveillantes

- Identifier les tactiques, techniques et procédures (TTP) à partir des données de sécurité
- Analyser les caractéristiques des Advanced Persistent Threats et des différentes catégories d'acteurs

- Différencier les comportements d'un acteur malveillant et ceux d'un test d'intrusion autorisé
- Utiliser la Pyramid of Pain pour sélectionner les artefacts utiles à la détection et à l'investigation
- Corréler les informations techniques et contextuelles afin d'améliorer l'attribution d'une activité suspecte
- Atelier pratique : analyser plusieurs traces de compromission et déterminer les TTP et le profil probable de l'acteur impliqué.

[Jour 3 - Matin]

Mettre en œuvre les techniques avancées de Threat Hunting

- Construire une démarche de Threat Hunting structurée à partir d'une hypothèse de recherche
- Utiliser Python et PowerShell pour enrichir les capacités d'analyse et de détection
- Rechercher les menaces non détectées à partir des artefacts présents sur les endpoints
- Identifier les communications Command & Control (C2) et les comportements réseau suspects
- Exploiter les logs, sessions, protocoles et données réseau afin de confirmer ou invalider une hypothèse
- Atelier pratique : conduire une campagne de Threat Hunting à partir de données endpoint et réseau puis documenter les résultats.

[Jour 3 - Après-midi]

Rechercher les menaces dans le Cloud, les applications et l'IoT

- Conduire une démarche de Threat Hunting dans un environnement Cloud
- Identifier les spécificités des workloads et applications cloud-native lors des investigations
- Analyser les applications et le code afin d'identifier les comportements ou vulnérabilités exploitables
- Comprendre les méthodes d'analyse des applications et systèmes utilisés par les équipements IoT
- Corréler les données Cloud, applicatives, endpoint et réseau pour rechercher des activités malveillantes
- Atelier pratique : rechercher les traces d'une activité malveillante dans un environnement Cloud et applicatif simulé.

[Jour 4 - Matin]

Analyser les attaques avancées et renforcer la détection

- Comprendre les principes des attaques résidentes en mémoire et identifier les artefacts exploitables
- Interpréter les résultats d'outils spécialisés tels que Volatility lors d'une investigation
- Comprendre les principes du reverse engineering appliqués à l'identification d'une compromission
- Identifier les menaces non détectées, vulnérabilités et erreurs de configuration à l'origine des gaps de détection
- Construire des signatures et recommander de nouvelles capacités de surveillance et de détection

- Atelier pratique : analyser des artefacts mémoire, identifier les indicateurs d'une attaque et proposer de nouvelles règles de détection.

[Jour 4 - Après-midi]

Industrialiser et automatiser les opérations de Threat Hunting

- Appliquer le Threat Hunting Maturity Model pour évaluer et faire évoluer les capacités d'une organisation
- Structurer les étapes de collecte, analyse, investigation, validation et remédiation d'une campagne de chasse
- Construire des runbooks et playbooks permettant de standardiser les opérations du SOC
- Automatiser la collecte, l'enrichissement et la qualification des données de sécurité
- Comprendre les usages de l'IA, du Machine Learning et du SecDevOps dans l'automatisation des opérations de cybersécurité
- Atelier pratique : construire un workflow automatisé de Threat Hunting intégrant enrichissement, qualification et validation humaine.

[Jour 5 - Matin]

Conduire une investigation SOC et remédier aux menaces

- Qualifier un incident à partir de logs, télémétrie, données endpoint et trafic réseau
- Construire une chronologie et identifier les différentes étapes d'une compromission
- Identifier les TTP, les gaps de détection et les éléments utiles à l'attribution de l'attaque
- Définir les mesures de confinement, contre-mesures et actions de remédiation adaptées
- Transformer les résultats de l'investigation en recommandations de détection et d'amélioration de la posture de défense
- Atelier pratique : conduire une investigation SOC complète depuis la détection initiale jusqu'à la construction d'un plan de remédiation priorisé.

[Jour 5 - Après-midi]

Préparer les examens CBRCOR et CBRTHD

- Revoir les domaines du référentiel 350-201 CBRCOR v1.1
- Revoir les domaines du référentiel 300-220 CBRTHD v1.0
- Identifier les différences entre les compétences Core et la spécialisation Threat Hunting and Defending
- Réviser les méthodes, modèles, outils et processus attendus lors des deux examens
- Définir une stratégie de gestion du temps pour les examens de 120 minutes et 90 minutes
- Atelier pratique : réaliser un examen blanc couvrant CBRCOR et CBRTHD, analyser les résultats et construire un plan de révision personnalisé.

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.