+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 CCNA Cybersecurity

5 jours (35 heures)

Présentation

La certification Cisco CCNA Cybersecurity valide les compétences nécessaires pour surveiller les systèmes, analyser les menaces et participer à la détection et à la réponse aux incidents au sein d'un Security Operations Center (SOC).

Cette formation Cisco CCNA Cybersecurity vous permettra de développer les compétences opérationnelles attendues d'un analyste cybersécurité. Vous apprendrez à identifier les principales menaces, à analyser les systèmes Windows et Linux et à exploiter les données réseau et endpoint pour détecter les signes d'une compromission.

Vous serez en mesure d'analyser les logs, flux NetFlow, captures réseau et alertes de sécurité, de corréler différentes sources de télémétrie et d'utiliser MITRE ATT&CK pour comprendre les techniques employées par les attaquants.

La formation aborde également les technologies SIEM, SOAR et XDR, l'analyse des intrusions réseau, le Threat Hunting et la construction de playbooks SOC. Vous apprendrez à qualifier les alertes, réduire les faux positifs et reconstruire la chronologie d'un incident à partir des données disponibles.

À l'issue de cette formation, vous serez capable de participer à une investigation SOC, de conduire les premières étapes d'une réponse à incident et d'appliquer les politiques et procédures nécessaires aux opérations de sécurité. Vous disposerez également des connaissances nécessaires pour préparer l'examen 200-201 CCNACBR permettant d'obtenir la certification Cisco CCNA Cybersecurity.

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

Objectifs

- Comprendre les fondamentaux de la cybersécurité et le fonctionnement d'un SOC
- Analyser les systèmes, logs, flux réseau et événements afin d'identifier les signes d'une compromission
- Maîtriser les principes du Network Security Monitoring et de l'analyse des intrusions
- Exploiter les technologies SIEM, SOAR et XDR pour corréler les événements et faciliter les investigations
- Mettre en œuvre les principes de réponse aux incidents, Threat Hunting et playbooks SOC
- Préparer l'examen 200-201 CCNACBR de la certification Cisco CCNA Cybersecurity

Public visé

- Analystes cybersécurité juniors
- Analystes SOC N1 / N2
- Techniciens sécurité
- Administrateurs systèmes et réseaux souhaitant évoluer vers la cybersécurité
- Professionnels souhaitant développer des compétences en opérations de sécurité

Pré-requis

- Connaissances fondamentales des réseaux TCP/IP, ports et protocoles courants
- Notions générales de cybersécurité et des principales menaces informatiques
- Connaissances de base des systèmes Windows et Linux recommandées
- Aucune certification Cisco préalable n'est obligatoire

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

Programme de notre formation Certification Cisco CCNA Cybersecurity (200-201 CCNACBR)

[Jour 1 - Matin]

Comprendre les fondamentaux de la cybersécurité

- Comprendre les notions de menace, vulnérabilité, exploit et risque
- Identifier les principaux acteurs de la menace et leurs motivations
- Comprendre les principes de confidentialité, intégrité et disponibilité du modèle CIA
- Appliquer les principes de défense en profondeur et de contrôle des accès
- Comprendre le rôle d'un analyste cybersécurité et l'organisation d'un SOC
- Atelier pratique : analyser un scénario de compromission et identifier les menaces, vulnérabilités et contrôles de sécurité associés.

[Jour 1 - Après-midi]

Analyser les réseaux et protocoles pour la cybersécurité

- Revoir les modèles OSI et TCP/IP, les ports et les principaux services réseau
- Analyser les protocoles Ethernet, IP, TCP et UDP dans un contexte de sécurité
- Comprendre le fonctionnement de DNS, DHCP, HTTP/HTTPS et SMTP
- Identifier le rôle du routage, des VLAN, du NAT et de la segmentation réseau
- Comprendre le 5-tuple et son utilisation pour identifier et corréler les communications réseau
- Atelier pratique : examiner une capture réseau avec Wireshark et identifier les protocoles, flux et comportements suspects.

Maîtriser la cryptographie et les contrôles de sécurité

- Comparer le chiffrement symétrique et asymétrique et leurs principaux cas d'usage
- Comprendre les fonctions de hachage, signatures numériques et mécanismes d'intégrité
- Comprendre le fonctionnement des certificats, de la PKI et de TLS
- Identifier le rôle des pare-feu, IDS/IPS, proxys et solutions de protection des endpoints
- Comprendre les mécanismes d'authentification, d'autorisation et de contrôle d'accès
- Atelier pratique : analyser une communication TLS et interpréter les informations d'un certificat numérique.

[Jour 2 - Matin]

Analyser la sécurité des systèmes et des endpoints

- Identifier les principaux composants et mécanismes de sécurité des systèmes Windows et Linux
- Analyser les processus, services, utilisateurs, fichiers et connexions réseau d'un endpoint
- Comprendre les mécanismes de journalisation et les événements utiles aux investigations
- Identifier les signes de compromission et les comportements anormaux sur un système
- Comprendre le rôle des solutions antivirus, EDR et endpoint security
- Atelier pratique : analyser les événements et processus d'un endpoint afin d'identifier les traces d'une compromission simulée.

[Jour 2 - Après-midi]

Comprendre les menaces et le comportement des attaquants

- Identifier les principales catégories de malwares et leurs mécanismes d'infection et de persistance
- Comprendre les techniques de phishing, social engineering et attaques renforcées par l'IA générative
- Identifier les caractéristiques des Advanced Persistent Threats (APT)
- Utiliser les indicateurs de compromission : adresses IP, domaines, URL, hashes et artefacts
- Cartographier le comportement des attaquants avec MITRE ATT&CK et les modèles de cycle d'attaque
- Atelier pratique : analyser un scénario d'attaque et cartographier les techniques observées avec MITRE ATT&CK.

Collecter et exploiter les données de sécurité

- Comprendre les principes du Network Security Monitoring (NSM)
- Identifier les principales sources de télémétrie : logs, événements, alertes, captures réseau et flux
- Comprendre et exploiter les données NetFlow pour analyser les communications
- Collecter et interpréter les journaux système, applicatifs, réseau et sécurité
- Comprendre la collecte, la normalisation, l'enrichissement et la conservation des données dans un SOC
- Atelier pratique : exploiter plusieurs sources de télémétrie pour identifier une activité réseau anormale.

[Jour 3 - Matin]

Analyser les intrusions et le trafic réseau

- Identifier les principales attaques TCP/IP et leurs traces dans le trafic réseau
- Analyser les comportements suspects sur DNS, HTTP/HTTPS et autres protocoles applicatifs
- Comprendre le fonctionnement et l'exploitation des alertes IDS/IPS
- Interpréter les timestamps, sessions et métadonnées d'une capture réseau
- Utiliser les techniques de network forensics pour reconstruire une activité malveillante
- Atelier pratique : reconstruire les différentes étapes d'une intrusion à partir d'une capture PCAP.

[Jour 3 - Après-midi]

Détecter les attaques web et les activités malveillantes

- Comprendre le fonctionnement des applications web et les principaux vecteurs d'attaque
- Identifier les traces d'attaques contre HTTP, DNS et les navigateurs
- Reconnaître les communications de Command & Control (C2) et les comportements de beaconing
- Identifier les signes d'exfiltration, de mouvement latéral et d'escalade de privilèges
- Corréler les données réseau et endpoint pour qualifier une activité malveillante
- Atelier pratique : analyser des traces réseau et endpoint pour identifier le scénario d'une attaque web suivie d'une compromission.

Exploiter SIEM, SOAR et XDR dans un SOC

- Comprendre l'architecture et le rôle d'un SIEM dans les opérations de sécurité
- Créer et interpréter des règles de corrélation et des alertes de sécurité
- Comprendre le rôle du SOAR dans l'orchestration et l'automatisation des réponses
- Utiliser les principes de Run Book Automation pour standardiser les opérations du SOC
- Comprendre le rôle d'une plateforme XDR et le positionnement de Cisco XDR dans l'investigation
- Atelier pratique : corréler plusieurs événements dans un SIEM et déclencher un scénario de réponse automatisée.

[Jour 4 - Matin]

Corréler les événements et conduire une investigation

- Construire une chronologie d'incident à partir de logs, PCAP, alertes et données endpoint
- Identifier les relations entre événements et distinguer cause, conséquence et bruit opérationnel
- Qualifier une alerte et déterminer sa criticité et son impact potentiel
- Réduire les faux positifs et améliorer la pertinence des investigations
- Documenter les preuves, hypothèses et conclusions d'une investigation SOC
- Atelier pratique : corréler plusieurs sources de données afin de reconstruire la chronologie complète d'un incident.

[Jour 4 - Après-midi]

Gérer la réponse aux incidents et les activités du CSIRT

- Comprendre le cycle de réponse aux incidents et les recommandations du NIST SP 800-61 Rev.3
- Identifier les rôles et responsabilités d'un CSIRT et des différents intervenants
- Mettre en œuvre les phases de détection, analyse, confinement, éradication et récupération
- Préserver les éléments nécessaires aux investigations et à la traçabilité des incidents
- Organiser la communication, l'escalade et le reporting pendant un incident de sécurité
- Atelier pratique : conduire une réponse à incident depuis la qualification de l'alerte jusqu'au plan de récupération.

Construire et exploiter des playbooks SOC

- Comprendre le rôle des playbooks et runbooks dans la standardisation des opérations de sécurité
- Définir les étapes de qualification, investigation, escalade et réponse selon le type d'incident
- Associer les sources de données et outils nécessaires à chaque procédure
- Définir les critères d'escalade et les responsabilités des différents niveaux du SOC
- Mesurer l'efficacité des procédures et organiser leur amélioration continue
- Atelier pratique : construire un playbook SOC pour traiter un scénario de compromission et définir les actions d'escalade associées.

[Jour 5 - Matin]

Mettre en œuvre une démarche de Threat Hunting

- Comprendre les objectifs et les principes du Threat Hunting
- Construire une hypothèse de recherche à partir d'indicateurs, comportements ou renseignements sur les menaces
- Exploiter les données réseau, endpoint et SIEM pour rechercher des traces de compromission
- Utiliser MITRE ATT&CK pour orienter et structurer les investigations
- Transformer les résultats d'une chasse en nouvelles règles et capacités de détection
- Atelier pratique : conduire une session de Threat Hunting à partir d'une hypothèse de compromission et documenter les résultats.

[Jour 5 - Après-midi]

Appliquer les politiques, procédures et bonnes pratiques de sécurité

- Comprendre le rôle des politiques, standards, procédures et guidelines dans les opérations de cybersécurité
- Identifier les responsabilités liées à la gouvernance, au risque et à la conformité
- Comprendre la gestion des vulnérabilités et la priorisation des mesures de remédiation
- Appliquer les principes du NIST Cybersecurity Framework aux opérations de sécurité
- Documenter les incidents, investigations et actions afin d'améliorer les processus du SOC
- Atelier pratique : analyser un incident et produire les recommandations de sécurité et mises à jour procédurales associées.

Préparer la certification Cisco CCNA Cybersecurity

- Revoir les cinq domaines du référentiel 200-201 CCNACBR v1.2
- Réviser les concepts de Security Concepts, Security Monitoring et Host-Based Analysis
- Réviser les compétences de Network Intrusion Analysis et Security Policies and Procedures
- Identifier les domaines nécessitant des révisions complémentaires avant le passage de l'examen
- Appliquer une stratégie de gestion du temps adaptée aux 120 minutes de l'examen
- Atelier pratique : réaliser un examen blanc CCNACBR, 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.