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

Mis à jour le 13/05/2026

S'inscrire

Formation Certification Cisco CCNP Cybersecurity : Concentration

5 jours (35 heures)

Présentation

Cisco CCNP Cybersecurity : Concentration est une certification avancée permettant de valider une expertise spécialisée en forensic réseau, réponse à incident et investigation de cybermenaces avec l'examen 300-215 CBRFIR.

Notre formation Certification Cisco CCNP Cybersecurity : Concentration vous permettra de maîtriser les compétences attendues pour l'examen 300-215 CBRFIR.

Vous apprendrez à analyser des incidents de sécurité, exploiter les journaux, identifier les indicateurs de compromission, conduire des investigations réseau et structurer une réponse à incident efficace.

Vous serez en mesure de qualifier une alerte, collecter les preuves, interpréter les traces techniques, reconstruire une chronologie d'attaque et proposer des mesures de confinement et de remédiation.

Grâce à une approche orientée cas concrets, forensic, analyse de logs et ateliers pratiques, cette formation vous préparera aux exigences opérationnelles des environnements SOC et Incident Response.

À l'issue de la formation, vous serez prêt à passer l'examen 300-215 CBRFIR, dédié à la cybersécurité, au forensic et à la réponse aux incidents.

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

Objectifs

- Préparer l’examen 300-215 CBRFIR.
- Maîtriser les fondamentaux du forensic réseau.
- Analyser les incidents de sécurité et indicateurs de compromission.
- Structurer une démarche de réponse à incident.
- Exploiter les logs, traces réseau et preuves numériques.

Public visé

- Analystes SOC
- Ingénieurs cybersécurité
- Administrateurs sécurité réseau
- Consultants réponse à incident
- Professionnels préparant la certification CCNP Cybersecurity Concentration

Pré-requis

- Connaissances solides en réseaux TCP/IP
- Notions en cybersécurité opérationnelle
- Expérience avec l’analyse de logs et d’événements sécurité
- Connaissances de base en réponse à incident et investigation

Pré-requis techniques

- Ordinateur portable avec 8 Go de RAM minimum et droits d’administration.
- Connexion Internet stable pour accéder aux labs et ressources Cisco.
- Navigateur web récent : Chrome, Firefox ou Edge.
- Client SSH et lecteur PDF installés.

Programme de formation Certification Cisco CCNP Cybersecurity : Concentration

[Jour 1 - Matin]

Introduction aux spécialisations CCNP Cybersecurity

- Comprendre le parcours CCNP Cybersecurity et les examens de concentration
- Identifier les spécialisations : Firepower, ISE, VPN, SOC, Automation
- Analyser les objectifs techniques des examens Cisco
- Positionner les compétences attendues en environnement SOC et sécurité réseau
- Comprendre les architectures Cisco Security avancées
- Atelier pratique : Cartographie d’une architecture Cisco Security.

[Jour 1 - Après-Midi]

Architecture Zero Trust et segmentation avancée

- Comprendre les principes Zero Trust
- Mettre en œuvre une segmentation réseau avancée
- Contrôler les flux east-west et north-south
- Analyser les risques liés aux accès latéraux
- Appliquer les politiques de microsegmentation
- Atelier pratique : Création d’une politique Zero Trust.

Sécurité des accès et contrôle d’identité

- Comprendre les mécanismes AAA et NAC
- Configurer les politiques d’accès basées sur l’identité
- Analyser les flux d’authentification sécurisée
- Mettre en œuvre le contrôle d’accès dynamique
- Comprendre les usages de Cisco ISE
- Atelier pratique : Construction d’une politique d’accès réseau.

[Jour 2 - Matin]

Firewall nouvelle génération et inspection avancée

- Comprendre le fonctionnement des NGFW
- Analyser les politiques d’inspection applicative
- Configurer les mécanismes IPS et filtrage avancé
- Superviser les journaux et événements de sécurité
- Optimiser les politiques de sécurité Cisco
- Atelier pratique : Analyse et optimisation d’une politique firewall.

[Jour 2 - Après-Midi]

VPN avancés et connectivité sécurisée

- Mettre en œuvre des architectures VPN sécurisées
- Comprendre les mécanismes IPsec et SSL VPN
- Diagnostiquer les incidents de tunnelisation
- Sécuriser les accès distants utilisateurs
- Optimiser les performances et la haute disponibilité VPN
- Atelier pratique : Dépannage d’une infrastructure VPN.

Sécurité web et protection du contenu

- Identifier les menaces web et applicatives
- Mettre en œuvre les politiques de filtrage URL

- Analyser les comportements suspects dans les flux HTTP/HTTPS
- Comprendre les mécanismes de sandboxing
- Bloquer les contenus malveillants et exfiltrations
- Atelier pratique : Analyse d’un incident web avancé.

[Jour 3 - Matin]

Sécurité email et lutte contre le phishing

- Comprendre les attaques email modernes
- Mettre en œuvre les protections SPF, DKIM et DMARC
- Analyser les campagnes de phishing et spear phishing
- Configurer des politiques de quarantaine
- Identifier les comportements suspects dans les emails
- Atelier pratique : Investigation d’un email malveillant.

[Jour 3 - Après-Midi]

Détection des menaces et analyse SOC

- Comprendre les workflows d’un SOC
- Analyser les logs et événements de sécurité
- Corréler les alertes dans un environnement SIEM
- Identifier les indicateurs de compromission
- Prioriser et qualifier les incidents
- Atelier pratique : Investigation SOC sur logs réseau.

Protection endpoint et EDR

- Comprendre les mécanismes EDR et Endpoint Security
- Analyser les comportements suspects sur postes clients
- Détecter les activités malveillantes et ransomwares
- Réagir aux alertes endpoint critiques
- Mettre en œuvre des stratégies de confinement
- Atelier pratique : Analyse d’une compromission endpoint.

[Jour 4 - Matin]

Cloud Security et environnements hybrides

- Comprendre les enjeux de la sécurité cloud
- Identifier les risques liés aux environnements hybrides
- Sécuriser les connexions entre datacenter et cloud
- Mettre en œuvre des politiques de visibilité cloud
- Analyser les modèles de responsabilité partagée

- Atelier pratique : Analyse d’une architecture cloud sécurisée.

[Jour 4 - Après-Midi]

Automatisation et APIs Cisco Security

- Comprendre les principes d’automatisation sécurité
- Exploiter les APIs Cisco pour les opérations sécurité
- Automatiser les contrôles et vérifications
- Créer des workflows d’orchestration sécurité
- Identifier les risques liés aux accès API
- Atelier pratique : Automatisation d’une tâche sécurité Cisco.

Réponse à incident et forensic réseau

- Comprendre les méthodologies de réponse à incident
- Collecter et préserver les preuves numériques
- Analyser les traces réseau et journaux système
- Mettre en œuvre des actions de confinement
- Documenter et formaliser un incident sécurité
- Atelier pratique : Investigation forensic simplifiée.

[Jour 5 - Matin]

Hardening, conformité et gouvernance sécurité

- Appliquer les bonnes pratiques de hardening
- Comprendre les référentiels de conformité sécurité
- Mettre en œuvre des politiques de gouvernance
- Analyser les écarts et risques de conformité
- Construire des recommandations de sécurisation
- Atelier pratique : Audit de conformité sécurité.

[Jour 5 - Après-Midi]

Optimisation des performances et troubleshooting sécurité

- Diagnostiquer les incidents sécurité complexes
- Analyser les problèmes de performance réseau liés à la sécurité
- Identifier les erreurs de configuration fréquentes
- Mettre en œuvre des méthodologies de troubleshooting
- Optimiser les politiques et équipements Cisco Security
- Atelier pratique : Résolution d’incidents multi-technologies.

Préparation finale à la certification Cisco CCNP Cybersecurity Concentration

- Réviser les domaines techniques clés de l’examen choisi
- Analyser les attentes Cisco sur les scénarios avancés
- Identifier les pièges fréquents de certification
- Optimiser sa gestion du temps pendant l’examen
- Consolider les connaissances via cas pratiques et quiz
- Atelier pratique : Passage de l'examen blanc + correction.

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.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l’État.
© Ambient IT 2015-2026. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg