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

Mis à jour le 29/07/2026

S'inscrire

Formation Senior Lead SOC 2 Manager

5 jours (35 heures)

Présentation

Le SOC 2 est devenu un référentiel clé pour démontrer la maîtrise des contrôles de sécurité, de la disponibilité, de la confidentialité et de l'intégrité. Cette formation vous prépare à piloter une démarche audit-ready et production-ready dans des environnements exigeants.

Notre formation Senior Lead SOC 2 Manager vous permet d'aller au-delà de la simple compréhension du référentiel pour structurer une gouvernance opérationnelle, aligner les preuves, et sécuriser les processus de conformité sur la durée.

Vous apprendrez à interpréter les Trust Services Criteria, à organiser la collecte d'évidences, à suivre les écarts de contrôle, à coordonner les parties prenantes et à préparer efficacement les audits internes et externes.

À l'issue de la formation, vous serez en mesure de renforcer un dispositif SOC 2, de prioriser les remédiations, d'industrialiser le suivi des contrôles et de fiabiliser la production des livrables attendus par les auditeurs et les équipes de sécurité.

Cette formation aborde également le monitoring, la gestion des incidents, la traçabilité, la documentation et les bonnes pratiques de pilotage afin de consolider une posture de conformité durable.

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

Objectifs

- Maîtriser les exigences du référentiel SOC 2 et des Trust Services Criteria.
- Structurer une gouvernance de conformité orientée preuves,contrôles et responsabilités.

- Organiser la collecte, la qualification et la conservation des évidences d'audit.
- Analyser les écarts, prioriser les remédiations et suivre les plans d'action.
- Préparer un audit type 1 ou type 2 avec une approche industrialisée.
- Renforcer le pilotage des incidents, du monitoring et de la traçabilité.

Public visé

- Analyste SOC
- Responsable conformité
- Consultant cybersécurité
- Auditeur sécurité
- Responsable GRC

Pré-requis

- Connaissance des fondamentaux de la cybersécurité et des contrôles internes.
- Expérience préalable en SOC,GRC ou en gestion de la conformité.
- Maîtrise des notions de risque, de preuve et de traçabilité.
- Compréhension des environnements cloud,SaaS ou hybrides.
- Lecture opérationnelle de la documentation de sécurité et des procédures d'audit.

Pré-requis techniques

- Ordinateur récent avec navigateur web à jour et espace disque suffisant pour les supports de cours.
- Connexion Wi-Fi ou Ethernet stable pour les échanges, ateliers et démonstrations.
- Suite bureautique installée, notamment Microsoft Excel ou équivalent pour le suivi des contrôles.
- Accès à un lecteur de documents PDF et à un outil de prise de notes pour les livrables de formation.
- Micro et casque recommandés pour les sessions à distance et les travaux collaboratifs.

Programme de notre formation Senior Lead SOC 2 Manager

[Jour 1 - Matin]

Fondations du référentiel

- Positionnement du SOC 2 dans une stratégie de conformité et de confiance.
- Lecture structurée des Trust Services Criteria et de leurs attentes opérationnelles.
- Différences entre Type 1 et Type 2, impacts sur le pilotage et les preuves.
- Rôles du Senior Lead Analyst, des équipes de sécurité et des parties prenantes métier.
- Cartographie initiale des contrôles, des risques et des dépendances documentaires.
- Atelier pratique : construire une première matrice de correspondance entre critères SOC 2 et contrôles existants.

[Jour 1 - Après-midi]

Gouvernance et périmètre

- Définition du périmètre d’audit, des systèmes concernés et des exclusions justifiées.
- Structuration de la gouvernance, du RACI et des circuits de validation.
- Identification des sources de preuve, des référentiels internes et des exigences de conservation.
- Alignement entre objectifs de conformité, contraintes opérationnelles et priorités de remédiation.
- Gestion des dépendances avec les fournisseurs, sous-traitants et environnements cloud.
- Atelier pratique : formaliser un périmètre SOC 2 et un schéma de responsabilités pour une organisation fictive.

[Jour 2 - Matin]

Contrôles de sécurité

- Analyse des contrôles liés à l’accès, à l’authentification et au principe du moindre privilège.
- Exigences sur la gestion des changements, les approbations et la séparation des tâches.
- Contrôles de journalisation, de supervision et de conservation des traces.
- Lecture des attentes en matière de confidentialité, d’intégrité et de protection des données.
- Évaluation de la maturité des contrôles et repérage des zones de fragilité.
- Atelier pratique : auditer un jeu de contrôles et qualifier les écarts selon leur criticité.

[Jour 2 - Après-midi]

Evidence et documentation

- Construction d’une stratégie de collecte des évidences fiable et répétable.
- Critères de qualité d’une preuve, traçabilité, horodatage et chaîne de responsabilité.
- Organisation documentaire, nommage, versioning et stockage sécurisé des livrables.
- Préparation des dossiers d’audit pour limiter les demandes complémentaires.
- Gestion des preuves sensibles et des restrictions d’accès aux documents.
- Atelier pratique : constituer un dossier de preuves complet pour un contrôle SOC 2 donné.

[Jour 3 - Matin]

Risk assessment avancé

- Méthodologie d’analyse des risques appliquée au contexte SOC 2.
- Identification des scénarios de défaillance, des impacts et des facteurs aggravants.
- Priorisation des risques selon l’exposition, la vraisemblance et la criticité métier.
- Définition des traitements, des acceptations et des plans de remédiation.
- Suivi des risques résiduels et articulation avec le pilotage de la conformité.
- Atelier pratique : produire une mini cartographie des risques avec plans d’action associés.

[Jour 3 - Après-midi]

Monitoring et détection

- Rôle du monitoring dans la démonstration continue de maîtrise des contrôles.
- Indicateurs utiles pour suivre l'état des contrôles et les dérives de conformité.
- Surveillance des événements de sécurité, corrélation et escalade.
- Articulation entre journalisation, supervision et détection d'anomalies.
- Exploitation des métriques pour alimenter le reporting de conformité.
- Atelier pratique : définir un tableau de bord de pilotage SOC 2 avec indicateurs clés.

[Jour 4 - Matin]

Incidents et réponse

- Organisation d'une capacité de réponse aux incidents alignée sur les exigences d'audit.
- Cycle de vie d'un incident, de la détection à la clôture documentée.
- Procédures de notification, d'escalade et de coordination inter-équipes.
- Capitalisation post-incident, retour d'expérience et amélioration continue.
- Exigences de traçabilité pour les incidents, les décisions et les actions correctives.
- Atelier pratique : simuler le traitement d'un incident et produire la documentation associée.

[Jour 4 - Après-midi]

Remédiation et plans d'action

- Construction d'un plan de remédiation réaliste, mesurable et priorisé.
- Coordination des actions entre sécurité, produit, infrastructure et gouvernance.
- Suivi des jalons, des dépendances et des preuves de correction.
- Gestion des dérogations, des risques acceptés et des arbitrages de direction.
- Préparation des éléments de justification pour les écarts non résolus.
- Atelier pratique : transformer une liste d'écarts en plan d'action pilotable par échéances.

[Jour 5 - Matin]

Préparation d'audit

- Organisation du dossier de préparation pour un audit interne ou externe.
- Anticipation des questions d'audit et des demandes de clarification.
- Techniques de revue croisée des preuves et des contrôles sensibles.
- Gestion des interviews, des démonstrations et des séquences de validation.
- Bonnes pratiques pour sécuriser la cohérence entre récit, preuves et réalité opérationnelle.
- Atelier pratique : conduire une revue d'audit simulée avec grille de préparation et de restitution.

[Jour 5 - Après-midi]

Consolidation et pilotage durable

- Synthèse des acquis et structuration d’un plan de montée en maturité.
- Industrialisation du suivi des contrôles, des preuves et des revues périodiques.
- Intégration de la conformité dans les rituels de pilotage et les comités de sécurité.
- Définition des actions de continuité pour maintenir un dispositif SOC 2 robuste.
- Feuille de route post-formation pour stabiliser la gouvernance et préparer les prochains cycles d’audit.
- Atelier pratique : élaborer une feuille de route SOC 2 sur 90 jours avec priorités, responsables et livrables.

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.