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

Mis à jour le 19/03/2026

S'inscrire

Formation Certification SailPoint Identity Security Leader

3 jours (21 heures)

Présentation

La certification SailPoint Identity Security Leader valide votre capacité à piloter une stratégie Identity Security et à aligner les enjeux risque, conformité et efficacité opérationnelle. Elle s'adresse aux contextes de gouvernance des accès, de réduction des privilèges et d'industrialisation des processus d'identité.

Cette formation vous prépare de façon structurée aux attendus du credential : concepts clés d'IGA, responsabilités d'un leader Identity, et articulation entre politiques, processus et contrôles. L'objectif est de savoir expliquer, prioriser et défendre des choix d'architecture et de gouvernance (joiner/mover/leaver, recertifications, SoD, RBAC/ABAC) auprès des parties prenantes.

L'approche est résolument pratique : ateliers de cadrage, études de cas, démos guidées et quiz type examen. Vous repartez avec des livrables réutilisables : trame de roadmap, matrice risques/contrôles, RACI, et checklist de préparation à l'évaluation.

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

Objectifs

- Expliquer les fondamentaux de l'Identity Security et de l'IGA.
- Cartographier les parties prenantes, rôles et responsabilités (RACI).
- Définir une stratégie de gouvernance : JML, recertifications, SoD, rôles.
- Prioriser une roadmap et des indicateurs (KPI/KRI) orientés risque.
- Se préparer à l'évaluation via questions types et scénarios.

Public visé

- Responsables IAM / IGA
- RSSI, GRC, Risk Managers

Pré-requis

- Notions de gestion des identités et des accès (IAM/SSO/MFA)
- Compréhension des enjeux conformité et audit (ex. ISO 27001, SOX, RGPD)
- Connaissances de base en modèles d’autorisations (RBAC, privilèges)
- Expérience de coordination entre IT, sécurité et métiers

Pré-requis techniques

- PC/Mac avec 8 Go RAM minimum (16 Go recommandé)
- Windows 10/11, macOS ou Linux, navigateur récent (Chrome/Edge/Firefox)
- Suite bureautique pour ateliers (notes, tableaux, schémas)
- Accès à un outil de visioconférence et audio fonctionnel si distanciel

Programme de notre formation Certification SailPoint Identity Security Leader Credential

[Jour 1 - Matin]

Fondamentaux de l’Identity Security et positionnement SailPoint

- Clarifier les objectifs IAM vs IGA : identité, accès, gouvernance, conformité
- Cartographier les risques : comptes orphelins, sur-provisionnement, privilèges excessifs, shadow IT
- Comprendre les concepts clés : joiner/mover/leaver, rôles, politiques, attestations
- Identifier les parties prenantes : IT, sécurité, RH, audit, métiers et responsabilités
- Atelier pratique : Construire une cartographie des risques et des acteurs pour un SI type.

[Jour 1 - Après-midi]

Architecture SailPoint et capacités de gouvernance

- Positionner les briques : sources d’identité, applications, connecteurs, workflows, gouvernance
- Définir le modèle d’identité : attributs, corrélation, qualité de données et référentiels
- Comprendre provisioning vs access request vs certification
- Introduire les contrôles : SoD, politiques d’accès, exceptions et compensations
- Atelier pratique : Décrire une architecture cible SailPoint et ses flux

[Jour 2 - Matin]

Gouvernance des accès : rôles, politiques et séparation des tâches

- Construire une stratégie de role model : business roles, IT roles, entitlements
- Mettre en place des politiques : règles d'éligibilité, garde-fous, exceptions et approbations
- Définir et exploiter la SoD : conflits, règles, remédiation et traçabilité
- Mesurer la maturité : indicateurs de couverture rôles, taux d'exceptions, dérives d'accès
- Atelier pratique : Concevoir un mini-modèle de rôles et une règle SoD pour un cas métier.

[Jour 2 - Après-midi]

Cycle de vie des identités et automatisation (JML)

- Décliner les scénarios Joiner/Mover/Leaver et leurs déclencheurs (RH, ITSM, événements)
- Définir les règles de provisioning : droits par défaut, droits conditionnels, révocation
- Gérer les comptes techniques et non-humains : ownership, rotation, contrôles
- Intégrer les processus : demandes d'accès, approbations, escalades, SLA
- Atelier pratique : Rédiger un workflow JML cible avec étapes, contrôles et points d'audit.

[Jour 3 - Matin]

Attestations, audit et reporting de conformité

- Structurer une campagne de certification : périmètre, population, fréquence, responsables
- Définir les décisions et preuves : conserver, révoquer, déléguer, commenter, justifier
- Optimiser l'efficacité : segmentation, priorisation par risque, échantillonnage, relances
- Préparer l'audit : pistes d'audit, journalisation, rapports et contrôles compensatoires
- Atelier pratique : Concevoir une campagne d'attestation orientée risque et ses livrables d'audit.

[Jour 3 - Après-midi]

Leadership, stratégie de déploiement et préparation à la certification

- Définir une feuille de route : quick wins, lots, dépendances, critères de succès
- Gérer l'adoption : communication, formation, RACI, gouvernance produit et run
- Mettre en place les KPI : réduction du sur-provisionnement, délais JML, taux de révocation, conformité
- Se préparer à l'examen : thèmes clés, pièges fréquents, méthode de réponse et gestion du temps
- Atelier pratique : Simulation d'examen (questions scénarisées) et plan d'action personnel de révision.

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.