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

Mis à jour le 08/10/2025

S'inscrire

Formation certification ISSAP - Information Systems Security Architecture Professional

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

La certification ISSAP (ISC2) valide une expertise avancée en architecture de sécurité : gouvernance, modélisation, réseaux et systèmes, IAM, cryptographie, cloud et résilience. Elle s'adresse aux profils confirmés qui conçoivent, évaluent et pilotent des architectures sécurisées alignées sur la stratégie d'entreprise.

Notre formation ISSAP couvre les domaines officiels et traduit les exigences réglementaires et techniques en architectures concrètes : modèles, contrôles, preuves et exploitation.

Vous apprendrez à documenter, justifier et faire évoluer vos choix dans des environnements hybrides et multi-cloud.

À l'issue, vous serez en capacité de concevoir et auditer des architectures de cybersécurité complexes, de guider les projets critiques et de vous préparer efficacement à l'examen ISSAP.

Comme toutes nos formations, ce programme s'appuie sur la dernière version stable des ressources ISC2 et privilégie une approche pratique et opérationnelle.

Objectifs

- Concevoir une architecture de cybersécurité cohérente et traçable.
- Appliquer standards et frameworks (ISO/NIST, TOGAF, SABSA).
- Sécu réseaux, systèmes, cloud et applications.
- Intégrer cryptographie et IAM dans la conception.
- Développer des architectures résilientes et conformes.
- Se préparer au passage de la certification ISSAP.

Public visé

- Architectes sécurité
- Ingénieurs sécurité senior
- **R**esponsables techniques sécurité
- RSSI
- Professionnels souhaitant monter en expertise

Pré-requis

- Être certifié CISSP
- Expérience confirmée en architecture de sécurité
- Bases solides en réseaux, systèmes, IAM, crypto, cloud

Programme de formation ISSAP – Information Systems Security Architecture Professional

[Jour 1 - Matin]

Fondamentaux de l’architecture de sécurité

- Positionnement ISSAP, lien avec l’architecture SI et la cybersécurité
- Rôle et périmètre de l’architecte sécurité
- Vue d’ensemble des domaines ISSAP
- Alignement sécurité vs stratégie d’entreprise
- Livrables et gouvernance d’architecture
- Atelier pratique : Cartographier rôles et responsabilités d’un architecte sécurité.

[Jour 1 - Après-midi]

Cadres et méthodes d’architecture

- Référentiels : TOGAF, SABSA, Zachman
- Méthode orientée risque et conformité
- Artefacts d’architecture (vues, modèles, glossaire)
- Traçabilité exigences - contrôles
- Gouvernance et cohérence multi-projets
- Atelier pratique : Carte d’architecture sécurité de haut niveau.

Gouvernance, risque et conformité

- Politiques, standards, normes (ISO, NIST)
- Cadres réglementaires clés (RGPD, sectoriels)
- Processus décisionnel et accountability
- Mesure de maturité et KPI/KRI
- Intégration GRC dans l’architecture
- Atelier pratique : Mini-policy et critères d’acceptation sécurité.

[Jour 2 - Matin]

Modélisation d’architecture de sécurité

- Principes de conception et patterns
- Vues logique / physique / opérationnelle
- Menaces et hypothèses de confiance
- Modèles Zero-Trust et segmentation
- End-to-end et defense-in-depth
- Atelier pratique : Modéliser une zone sensible.

[Jour 2 - Après-midi]

Réseaux et périmètres modernes

- Segmentation, IDS/IPS, firewalls, proxys
- VPN, SD-WAN, filtrage, inspection TLS
- Réseaux hybrides et multi-cloud
- Contrôles réseau vs exigences métiers
- Observabilité et supervision
- Atelier pratique : Design d’un réseau sécurisé multi-zones.

Infrastructures et systèmes

- Durcissement OS/virtualisation/conteneurs
- Plan de contrôle, secrets, bastions
- Sécurité plateformes et workloads
- Chaîne d’approvisionnement
- Intégration aux opérations
- Atelier pratique : Schéma d’infra sécurisée avec bastion et logs.

[Jour 3 - Matin]

Cryptographie et gestion des clés

- Concepts appliqués (symétrique, asymétrique, hachage)
- PKI, certificats, HSM, rotation
- Protocoles : TLS, IPsec, SSH

- Data-at-rest / in-transit / in-use
- Modèles de confiance et délégation
- Atelier pratique : Architecture PKI et politique de certificats.

[Jour 3 - Après-midi]

Sécurité applicative et SDLC

- Intégration sécurité au SDLC / DevSecOps
- API, microservices, secrets management
- Menaces OWASP et contrôles d’architecture
- Revues d’architecture et gates
- Qualité, tests et conformité
- Atelier pratique : Évaluer l’architecture d’une appli web.

Cloud et responsabilité partagée

- Modèles IaaS/PaaS/SaaS et shared-responsibility
- Atterrissage sécurisé (landing zones)
- Réseaux, identités et données dans le Cloud
- Multi-cloud et interco
- Guardrails et policy as code
- Atelier pratique : Blueprint d’architecture Cloud sécurisée.

[Jour 4 - Matin]

Gestion des identités et des accès

- Fédération : SAML, OAuth2, OIDC
- Gestion des accès : comptes privilégiés, authentification forte et droits utilisateurs
- Contexte, risque et accès adaptatif
- Intégration IAM vers SI et SaaS
- Logs, audit et conformité
- Atelier pratique : Concevoir une architecture IAM de bout en bout.

[Jour 4 - Après-midi]

Données et gouvernance

- Classification, rétention, cycle de vie
- Chiffrement, masquage, tokenisation
- Data mesh / data lake : exigences sécurité
- Traçabilité, preuves et audits
- Vie privée et principes RGPD
- Atelier pratique : Politique de classification et contrôles associés.

Résilience, continuité et crise

- HA, PRA/PCA, dépendances critiques
- Plans de réponse et exercices
- Anti-fragilité et « secure-by-default »
- Plans d’amélioration continue
- Budget d’erreur et SLO
- Atelier pratique : Runbook PRA/PCA et tests périodiques.

[Jour 5 - Matin]

Sécurité physique et environnementale

- Contrôles physiques & datacenters
- Convergence physique/logique
- Normes et conformité locale
- Surveillance, accès, preuves
- Intégration au modèle de menaces
- Atelier pratique : Évaluer un site critique (zones & contrôles).

[Jour 5 - Après-midi]

Architecture sécurisée orientée projets

- Agile/DevSecOps : « shift-left »
- Critères d’acceptation sécurité et gates
- Docs d’architecture : vues et standards
- Fournisseurs et tier risk
- Coûts, priorisation et arbitrages
- Atelier pratique : Checklist d’architecture sécurité pour un produit.

Préparation à l’examen ISSAP

- Structure de l’examen
- Plan de révision
- QCM types, pièges et gestion du temps
- Ressources officielles ISC2
- 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.