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

Mis à jour le 07/10/2025

S'inscrire

Formation certification ISSEP – Information Systems Security Engineering Professional

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

La certification ISSEP (Information Systems Security Engineering Professional) est une spécialisation avancée ISC2 qui valide l'expertise en ingénierie de la sécurité tout au long du cycle de vie système.

Cette formation couvre la traduction des exigences métiers en exigences de sécurité, la modélisation et le design d'architectures robustes, la gestion des risques, ainsi que l'intégration des contrôles dans les réseaux, systèmes, applications, IAM, cloud et la résilience.

Notre formation ISSEP vous donnera les méthodes, les modèles et les outils pour concevoir, documenter et justifier des architectures sécurisées, tout en vous préparant efficacement à l'examen ISSEP (ISC2).

Comme toutes nos formations, celle-ci s'appuie sur la dernière version stable du référentiel et privilégie une approche résolument pratique et opérationnelle.

Objectifs

- Concevoir une architecture de sécurité cohérente, traçable et testable.
- Appliquer standards et frameworks.
- Sécuriser réseaux, systèmes, cloud, applications et données.
- Intégrer cryptographie et IAM dans la conception.
- Déployer résilience (haute disponibilité, continuité, reprise) et conformité continue.
- Se préparer au passage de la certification ISSEP.

Public visé

- Architectes sécurité
- Ingénieurs sécurité senior
- Consultants SSE
- Responsables techniques sécurité
- RSSI

Pré-requis

- Être certifié CISSP
- Solides bases en réseaux, systèmes, IAM, cryptographie et cloud
- Expérience projet sécurité

Programme formation ISSAP - Information Systems Security Engineering Professional

[Jour 1 - Matin]

Ingénierie de la sécurité : rôle et périmètre ISSEP

- Positionnement ISSEP et rôle ingénierie sécurité
- Principes SSE et intégration au SDLC
- Gouvernance, responsabilités et livrables
- Tracer le lien entre besoins et contrôles de sécurité
- Vue d’ensemble du cursus
- Atelier pratique : Rôles, livrables et périmètre SSE.

[Jour 1 - Après-midi]

Référentiels, normes et exigences

- NIST SP 800-160, ISO/IEC 15288, ISO/IEC 27001/27002
- Conformité et exigences sectorielles
- Transformer les objectifs métiers en exigences de sécurité
- Critères d’acceptation et niveaux d’assurance
- Mesure : KPI/KRI
- Atelier pratique : Dériver des exigences mesurables.

Gestion des risques et ingénierie

- Méthodes ISO 27005, EBIOS RM, NIST SP 800-30

- Cartographie menaces/actifs
- Sélection contrôles proportionnés
- Acceptation/transfer/mitigation/évitage
- Amélioration continue PDCA
- Atelier pratique : Élaborer une matrice de risques orientée architecture.

[Jour 2 - Matin]

Modélisation et design d’architecture sécurité

- Vues logique/physique/opérationnelle
- Threat modeling (STRIDE, ATT&CK)
- Patterns zero-trust et segmentation
- SPOF, dépendances et hypothèses de confiance
- Dossier d’architecture (SAD)
- Atelier pratique : Carte de flux et zones de confiance.

[Jour 2 - Après-midi]

Réseaux et périmètres modernes

- Segmentation, IDS/IPS, firewalls, proxys
- VPN, SD-WAN, inspection TLS
- Observabilité et télémétrie
- SOC, SIEM, SOAR
- Hybride et multi-cloud
- Atelier pratique : Design multi-zones sécurisé.

Systèmes, plateformes et supply chain

- Durcissement OS, virtualisation, conteneurs
- SBOM, provenance et signatures
- Secrets, bastions, PAM
- Journaux, immuabilité, récupération
- Intégration SecOps
- Atelier pratique : Infra sécurisée et flux d’admin.

[Jour 3 - Matin]

Cryptographie et gestion des clés

- Symétrique, asymétrique, hachage
- PKI, HSM, rotation et révocation
- Protocoles TLS, IPsec, SSH
- Data at-rest/in-transit/in-use

- Politiques de confiance
- Atelier pratique : Architecture PKI et certificats.

[Jour 3 - Après-midi]

Ingénierie sécurité des applications

- SSDLC et DevSecOps
- Risques OWASP et contrôles
- API/microservices et secrets
- Gates qualité et tests
- Conformité embarquée
- Atelier pratique : Revue d’architecture applicative.

Cloud et responsabilité partagée

- IaaS/PaaS/SaaS et shared-responsibility
- Landing zones et guardrails
- Réseaux/identités/données Cloud
- Policy as code et drift
- Multi-cloud et interco
- Atelier pratique : Blueprint cloud sécurisé.

[Jour 4 - Matin]

Identité et accès

- MFA, authentification et autorisation
- Fédération : SAML, OAuth2, OIDC
- PAM et moindre privilège
- Accès adaptatif et contexte
- Journaux et audit
- Atelier pratique : Architecture IAM complète.

[Jour 4 - Après-midi]

Données : classification et protection

- Classification, labellisation
- Chiffrement, masquage, tokenisation
- Gouvernance et rétention
- Traçabilité et auditabilité
- Vie privée by design/default
- Atelier pratique : Politique de classification.

Résilience et continuité

- Structurer les plans de reprise (PRA/PCA) et les seuils de tolérance (RTO/RPO)
- Plans de réponse et exercices
- Anti-fragilité et secure-by-default
- Amélioration continue et priorisation
- Budget d’erreur et SLO/SLA
- Atelier pratique : Runbook PRA/PCA.

[Jour 5 - Matin]

Sécurité physique et environnementale

- Contrôles physiques et datacenters
- Convergence physique/logique
- Accès, surveillance, preuves
- Contraintes réglementaires
- Intégration au modèle de menaces
- Atelier pratique : Évaluer un site critique.

[Jour 5 - Après-midi]

Conformité projet/produit

- Agile/produit : « shift-left » sécurité
- Critères d’acceptation et gates
- Fournisseurs et tier risk
- Coûts et arbitrages
- Docs d’architecture standardisées
- Atelier pratique : Checklist SSE produit.

Préparation à l’examen ISSEP

- Domaines et pondérations
- QCM + advanced item types
- 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.