+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 CSSLP – Certified Secure Software Lifecycle Professional

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

CSSLP est la certification (ISC)² dédiée à la sécurité du cycle de vie logiciel. Elle valide des compétences avancées pour intégrer des bonnes pratiques de sécurité à chaque phase du SDLC : exigences, architecture, codage sécurisé, tests, déploiement, maintenance et supply chain.

Notre formation CSSLP vous prépare de manière opérationnelle à l'examen, en combinant synthèse des 8 domaines, ateliers concrets et simulations de questions, tout en ancrant les réflexes DevSecOps au quotidien.

Vous apprendrez à modéliser les menaces, concevoir des architectures sécurisées, industrialiser les tests de sécurité dans vos pipelines CI/CD et maîtriser la gestion des vulnérabilités et des dépendances.

À l'issue du parcours, vous disposerez d'une vision claire du périmètre CSSLP, d'un plan d'action pragmatique pour vos projets et d'un examen blanc intégralement corrigé afin d'aborder l'examen officiel en confiance.

Comme toutes nos formations, celle-ci s'aligne sur le dernier référentiel de l'examen diffusé par (ISC)² et ses mises à jour.

Objectifs

- Couvrir efficacement les 8 domaines CSSLP et leurs attentes.
- Intégrer la sécurité dans chaque phase du SDLC.
- Concevoir une architecture et un design sécurisés.
- Mettre en œuvre tests et automatisation sécurité dans CI/CD.

- Piloter gestion des risques, vulnérabilités et supply chain.
- Réussir l’examen grâce à un examen blanc commenté.

Public visé

- Développeurs
- DevSecOps
- Lead dev
- SRE
- Testeurs et QA
- Chefs de projet

Pré-requis

- Notion de base en sécurité applicative
- 4 ans d'expérience dans le domaine de la cybersécurité

Programme de formation CSSLP – Certified Secure Software Lifecycle Professional

[Jour 1 - Matin]

Principes fondamentaux de la sécurité logicielle

- Objectifs CIA : Confidentialité, Intégrité, Disponibilité
- Sécurité logicielle vs Sécurité applicative : périmètre et enjeux
- Gouvernance, conformité, gestion des risques dans le SDLC
- Rôles et responsabilités (dev, Sec, QA, SRE, PO)
- Atelier pratique : Analyse d’incident, causes racines et contre-mesures.

[Jour 1 - Après-midi]

Gouvernance et cadre normatif

- Panorama (ISC)² CSSLP et ses 8 domaines
- Référentiels : ISO 27001, NIST SSDF, OWASP SAMM
- Politiques, chartes, risk appetite, comité sécurité
- Conformité : RGPD, PCI-DSS, HIPAA
- Atelier pratique : Cartographier obligations et contrôles pour un produit.

Intégrer la sécurité au SDLC

- Sécurité en Agile, DevSecOps, Waterfall
- Contrôles de sécurité : DoR, DoD et revues intégrées au processus Agile
- Boucles d'amélioration continue, KPIs sécurité
- Collaboration transverse et flux de feedback
- Atelier pratique : Planifier des contrôles sécurité dans un sprint.

[Jour 2 - Matin]

Exigences de sécurité

- Recueil d'exigences fonctionnelles et non fonctionnelles
- Misuse/Abuse cases, critères d'acceptation sécurité
- Traçabilité : matrices, threat statements
- Priorisation par risque et par impact
- Atelier pratique : Cahier des charges sécurité d'un module SaaS.

[Jour 2 - Après-midi]

Architecture et design sécurisés

- Principes : least privilege, defense in depth, SoC
- Modélisation de menaces et surface d'attaque
- Patterns sécurisés (façade, médiateur, sandboxing)
- Microservices, API, cloud : arbitrages sécurité/performance
- Atelier pratique : Concevoir une architecture d'API REST sécurisée.

Gestion des risques

- Identification, classification, hiérarchisation (EBIOS, ISO 27005)
- Plans de traitement : éviter, réduire, transférer, accepter
- Registre des risques, KRI, revue périodique
- Cartographie vulnérabilités et dette de sécurité
- Atelier pratique : Évaluer les risques d'une application existante.

[Jour 3 - Matin]

Développement et codage sécurisé

- Validation entrées/sorties, gestion d'erreurs et exceptions
- Bonnes pratiques OWASP Top 10 : prévention des failles XSS, CSRF, injections, SSRF et XXE
- Gestion sécurisée des secrets, configuration immuable et principes du modèle 12-Factor
- Dépendances et SBOM : versions, signatures
- Atelier pratique : Revue de code et correctifs ciblés.

[Jour 3 - Après-midi]

Identités, sessions et accès

- Authentification, autorisation, MFA, RBAC/ABAC
- Protocoles OAuth2, OIDC, SAML
- Sessions : cookies, SameSite, HSTS, rotation de jetons
- Prévenir élévation de privilèges et usurpation
- Atelier pratique : Sécuriser un flux Login/OAuth d’API.

Données et confidentialité

- Chiffrement symétrique/asymétrique, PKI, gestion de clés
- Hashing et salage, stockage chiffré, KMS
- Données au repos/en transit
- Privacy by Design/Default et minimisation
- Atelier pratique : Protéger un jeu de données sensibles.

[Jour 4 - Matin]

Tests de sécurité

- SAST, DAST, IAST, Fuzzing : usages et limites
- Automatisation dans CI/CD, seuils et quality gates
- Données de test : anonymisation et sensibles
- Traçabilité des défauts et suivi
- Atelier pratique : Pipeline de tests sécurité automatisés.

[Jour 4 - Après-midi]

Déploiement et environnements

- Durcissement containers, K8s, IaC
- Secrets en production, rotation, zero-trust
- Observabilité : logs, métriques, traces, alertes
- Réponse à incident, rollback, post-mortem
- Atelier pratique : Sécuriser un déploiement CI/CD.

Maintenance et vulnérabilités

- Patch management, fenêtres de maintenance
- Suivi des vulnérabilités (CVE), bug bounty et contrôle des dépendances via outils SCA
- Communication post-incident, statut et RCA
- Décommissionnement et effacement sécurisé
- Atelier pratique : Plan de remédiation priorisée.

[Jour 5 - Matin]

Chaîne d’approvisionnement logicielle

- Risques tiers, contrat et clauses sécurité
- SBOM, provenance, signature et intégrité
- Politique open-source : approbation et suivi
- Audits fournisseurs et SLA sécurité
- Atelier pratique : Mini-audit de supply chain.

[Jour 5 - Après-midi]

Révision des 8 domaines et stratégies d’examen

- Synthèse des 8 domaines CSSLP
- Pièges typiques et distracteurs récurrents
- Gestion du temps et techniques d’élimination
- Atelier pratique : Mini-quiz chronométré et débrief.

Examen blanc CSSLP et correction

- Correction détaillée et justifications
- Analyse des erreurs et axes de révision
- Conseils finaux et plan de dernière ligne droite
- 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.