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

Mis à jour le 06/06/2025

S'inscrire

Formation Sécurité des Applications

3 jours (21 heures)

PRÉSENTATION

Notre formation sécurité des applications vous permettra de développer des applications web et mobiles modernes et sécurisées. À l'issue de cette formation, vous maîtriserez les bonnes pratiques nécessaires pour protéger efficacement votre code contre les risques cyber et serez en mesure d'assurer une veille continue et pertinente en cybersécurité.

À travers un tour d'horizon complet intégrant les référentiels internationaux (OWASP, NIST, ANSSI), vous explorerez les principales menaces affectant les applications web et mobiles, tels que les injections SQL, les contrôles d'accès insuffisants ou les failles spécifiques à l'IA, notamment à travers les différents TOP 10 d'OWASP (Web, Mobile, API).

Vous apprendrez à intégrer la sécurité dès la phase de conception (Secure by Design), adopter les meilleures pratiques de développement sécurisé et utiliser efficacement les outils modernes d'analyse (SAST, DAST, SCA). Des ateliers pratiques vous permettront d'appliquer immédiatement ces concepts sur une application fil rouge réaliste, renforçant votre capacité à détecter et corriger rapidement les vulnérabilités.

Enfin, notre formation vous introduira aux principes essentiels du DevSecOps et de la sécurité Cloud, pour une protection continue et efficace de vos applications, dans une démarche proactive et collaborative.

Comme tous nos programmes, cette formation place les exercices pratiques au cœur de votre apprentissage, vous permettant ainsi d'acquérir des compétences opérationnelles immédiatement mobilisables.

OBJECTIFS

- Comprendre les problématiques de la sécurité des applications
- Identifier les principales menaces et vulnérabilités affectant les applications web et mobiles
- Appliquer les bonnes pratiques de sécurité dans le développement d'applications
- Utiliser des outils et techniques pour détecter et corriger les failles de sécurité

- Découvrir les principes de base de la cybersécurité et leur impact sur la sécurité des applications

PUBLIC VISÉ

- Architectes
- Développeurs
- Analystes
- Chefs de projets

Pré-requis

- Posséder une bonne connaissance de la programmation objet et de la programmation d’application Web

Programme de notre Formation Sécurité des applications

Introduction à la sécurité applicative

- Pourquoi la cybersécurité est stratégique ?
- Enjeux et conséquences des failles applicatives
- Coût moyen d’une faille
- Acteurs et motivations : cyber-crime, hacktivisme, espionnage, supply-chain
- Obligations légales (RGPD, NIS2)
- Surfaces d’attaque et notion de « misuse case »
- Triangle de sécurité du modèle CIA : Confidentialité, Intégrité, Disponibilité
- Rôle des normes et des agences gouvernementales (OWASP, ANSSI, NIST, CISA, CERT)
- Cybersecurity Framework 2.0 de NIST : Gouvernance et Supply Chain
- Principe du Secure Development Lifecycle (SDLC)
- Menaces courantes et exemples d'attaques réelles
- Importance de la sensibilisation et de la culture sécurité
- Atelier pratique : Analyse collective d’une application vulnérable afin d’identifier les risques potentiels.

Tour d'horizon des bases de données de vulnérabilités

- USA
  - CVE (Common Vulnerabilities and Exposures) par le MITRE Corporation
  - NVD (National Vulnerability Database) scores CVSS, classifications CWE et produits affectés
  - ExploitDB (Exploit Database) d'OffSec contenant des preuves de concept
  - OSV (Open Source Vulnerabilities) de Google visant sur les vulnérabilités affectant les logiciels open source
- Europe
  - EUVD (European Vulnerability Database), nouveau projet lancé en mai 2025 par l'ENISA
- Autres : VulnDB, Vulners, Zero-Day.cz
- Prédiction et exploitation des failles : EPSS, KEV, LEV

Vulnérabilités Web : OWASP Top 10 (2025)

- Présentation OWASP Top 10 des vulnérabilités web
- A01 Broken Access Control, A02 Cryptographic Failures, A03 Injection, etc.
- Injection (SQL, LDAP, XML)
- Illustrations live : SQLi avec DVWA, XSS dans un micro-service
- Contrôle d'accès défaillant
- Mauvaises configurations de sécurité
- Défaillances cryptographiques
- Erreurs dans la gestion des authentifications et des sessions
- Atelier pratique : Corriger un formulaire non filtré (Input Validation Cheat Sheet).

Vulnérabilités Mobiles : OWASP Mobile Top 10 (2025)

- Spécificités iOS/Android : stockage local, permissions, reverse engineering
- M1 Improper Credential Usage à M10 Insufficient Cryptography
- Mauvaise gestion des identifiants
- Authentification et autorisation insuffisantes
- Stockage non sécurisé des données sensibles
- Protection insuffisante côté client (reverse engineering)
- Communication non sécurisée avec le backend
- Atelier pratique : Examen d'une application mobile vulnérable pour détecter les principales failles. Analyser une APK avec MobSF et vérifier les exigences MASVS.

Tests et outils d’analyse de sécurité

- SAST : Techniques d'analyse statique, démonstration avec SonarQube
- DAST : Techniques d'analyse dynamique, test en boite noire, simulation d’attaque avec OWASP ZAP
- SCA : Analyse des dépendances, OWASP Dependency-Check et flux CVE
- Présentation d’outils : OWASP ZAP, Burp Suite
- Méthodologie simple de pentesting applicatif
- Gestion et priorisation des vulnérabilités découvertes
- Importance de la journalisation et du monitoring applicatif
- Atelier pratique : Scan rapide de l'application fil rouge et interprétation des résultats.

Sécurité dès la conception (Secure by Design)

- Principes d’architecture sécurisée (Defense-in-depth, principe du moindre privilège)
- Techniques de modélisation des menaces (STRIDE)
- Gestion proactive des risques (identification et priorisation)
- Bonnes pratiques pour le cloisonnement et l'isolation des composants
- Sécurisation des API et microservices
- Cas d'usage des référentiels NIST et ANSSI sur le design sécurisé
- Atelier pratique : Réaliser une modélisation des menaces (threat modeling) sur l’application fil rouge.

Bonnes pratiques de développement sécurisé

- Principes de codage défensif : validation d’entrée, gestion d’erreurs, logging
- Chiffrement : choix des algorithmes, gestion des secrets
- Utilisation adéquate de la cryptographie (chiffrement, hachage)
- Authentification & gestion de sessions robustes (OAuth 2.1, MFA)
- Gestion sécurisée des authentifications et des sessions utilisateurs
- Gestion sécurisée des erreurs et exceptions
- Maintien à jour des bibliothèques et composants tiers
- Protection côté client (CSP, gestion des cookies sécurisés)
- Atelier pratique : Corriger des extraits de code vulnérable issus de l’application fil rouge.

Sécurité des API modernes

- Présentation OWASP API Security Top 10
- Contrôle d’accès sur les endpoints API
- Sécurisation des communications API (JWT, OAuth2)
- Validation stricte des données entrantes
- Gestion sécurisée des clés et secrets API
- Protection contre les attaques de type DoS/API Abuse
- Atelier pratique : Identifier et corriger une vulnérabilité sur une API REST de l’application fil rouge.

Conclusion et Ouverture : le DevSecOps et Sécurité Cloud

- Présentation des principes du DevSecOps
- Intégration continue de la sécurité (SAST/DAST dans CI/CD)
- Sécurisation de la chaîne d’approvisionnement logicielle (SBOM, gestion des dépendances)
- Bonnes pratiques de configuration d’infrastructure (IaC sécurisée)
- Surveillance continue et réponses aux incidents
- Culture sécurité dans les équipes de développement
- Durcissement des images & conteneurs : principe de moindre privilège, signatures
- Sécurisation du pipeline CI/CD : gates SAST / SCA / IaC scan, « shift-left »
- Zéro Trust et contrôle d’identité dans les infrastructures cloud natif

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.