New

Security by Design : Intégrer la sécurité à vos projets informatiques dès leur conception

Anticiper les risques pour renforcer la fiabilité des systèmes

Présentiel ou en classe à distance

3 jours (21 h)

Prix inter : 2.890,00 € HT
Forfait intra : 7.690,00 € HT

Réf.: SR213

La formation **Security by Design** propose une approche méthodique et opérationnelle pour intégrer la **sécurité applicative dès les phases de conception** et tout au long du cycle de vie des applications. Elle permet aux équipes techniques de comprendre comment traduire les principes fondamentaux de sécurité **défense en profondeur, moindre privilège, sécurité par défaut** en mécanismes concrets au niveau de l'architecture, du développement et des pipelines DevSecOps. Les participants apprennent à réaliser un threat modeling structuré (STRIDE, DFD), à **formaliser des exigences de sécurité** exploitables et à identifier les risques liés aux architectures modernes (microservices, API, cloud-native).
Au-delà des concepts, la formation met fortement l'accent sur l'**automatisation de la sécurité** et l'intégration d'outils tels que SAST, DAST, SCA, SonarQube, Trivy, OWASP Dependency-Check au sein des pipelines CI/CD. Les ateliers pratiques permettent d'analyser des architectures existantes, de détecter des antipatterns de sécurité, de corriger des vulnérabilités simples et de définir des indicateurs de pilotage pour mesurer l'efficacité de la démarche.

A qui s'adresse cette formation ?

Pour qui

- Développeurs confirmés, architectes techniques, ingénieurs DevOps / SecOps souhaitant structurer leur démarche Security by Design

Prérequis

- Connaissances générales des architectures applicatives (applications web, API, bases de données)
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Fondamentaux du Security by Design et cadrage sécurité

- Définir le Security by Design et ses enjeux techniques.
- Appliquer les principes clés : défense en profondeur, moindre privilège, sécurité par défaut
- Distinguer Secure by Design et Secure by Default
- Relier Security by Design aux architectures applicatives existantes (monolithes, microservices, cloud-native)
- Introduire la notion de trust boundaries pour préparer la modélisation des menaces

Atelier

Analyser une architecture applicative existante

Identifier les écarts par rapport aux principes du Security by Design

Associer chaque principe à des mécanismes techniques concrets (authentification, chiffrement, validation d'entrée, contrôle d'accès).

2 - Exigences de sécurité et modélisation des menaces

- Formuler des exigences de sécurité non fonctionnelles exploitables
- Identifier les données sensibles et contraintes réglementaires (RGPD, conformité)
- Introduire la modélisation des menaces (STRIDE ou équivalent)
- Utiliser les diagrammes de flux de données (DFD)

Atelier

Reformuler un cahier des charges fonctionnel en exigences de sécurité SMART

Classer les exigences par priorité et impact

Construire un diagramme de flux de données

Identifier les menaces associées à chaque composant

Proposer des mesures de mitigation adaptées

3 - Architecture sécurisée et intégration DevSecOps

- Analyser une architecture applicative sous l'angle sécurité
- Identifier patterns et antipatterns de sécurité
- Intégrer les contrôles de sécurité dans le SDLC.
- Positionner la sécurité dans une démarche DevSecOps
- Illustrer l'intégration avec des outils concrets : GitLab CI/CD, SonarQube, OWASP Dependency-Check, Trivy, etc

Atelier

Examiner une architecture applicative fournie

Identifier les faiblesses de conception

Proposer des améliorations d'architecture sécurisée

4 - Sécurité dans le développement et automatisation

- Appliquer les bonnes pratiques de codage sécurisé (OWASP, CWE)
- Comprendre le rôle et les différences entre outils SAST, DAST et SCA
- Intégrer les contrôles de sécurité automatisés dans les pipelines CI/CD
- Exploiter les résultats de scans pour prioriser et corriger les vulnérabilités

Atelier

Configurer des outils SAST / DAST dans un pipeline CI/CD fictif

Analyser les résultats de scans de sécurité

Corriger un défaut de sécurité simple identifié par les outils

Documenter une matrice de vulnérabilités et hiérarchiser les corrections

5 - Tests de sécurité et validation continue

- Mettre en place des tests unitaires et d'intégration orientés sécurité
- Comprendre les boucles de feedback automatisées
- Introduire les tests de fuzzing et les tests d'intrusion simplifiés
- Faire le lien avec l'OWASP ASVS (Application Security Verification Standard)

Atelier

Ajouter des contrôles de sécurité dans une suite de tests existante

Vérifier le déclenchement automatique des tests dans le pipeline CI/CD

Évaluer la couverture de tests sécurité à partir d'indicateurs quantitatifs

6 - Gouvernance technique et cas intégrateur

- Clarifier les rôles Dev / Sec / Ops dans une démarche Security by Design
- Définir des indicateurs de suivi sécurité (KPIs/KRIs : taux de correction, couverture de tests, MTTR sécurité)
- Identifier les pièges courants et meilleures pratiques de gouvernance technique

Atelier

Élaborer un plan d'action Security by Design pour une équipe technique

Les objectifs de la formation

- Appliquer les principes Security by Design dans une architecture applicative
- Réaliser un threat modeling exploitable. Définir et implémenter des contrôles de sécurité dès la conception
- Intégrer la sécurité dans un pipeline CI/CD
- Mettre en place des tests et outils de sécurité automatisés
- Définir des indicateurs et mécanismes de gouvernance pour suivre l’efficacité de la démarche

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Une découverte et une mise en oeuvre d’outils reconnus
- L'apprentissage par la pratique : les phases théoriques sont complétées d'ateliers favorisant un ancrage durable des acquis
- Une formation animée par des formateurs experts en sécurité applicative et DevSecOps

Dates et villes 2026 - Référence SR213

Dernières places disponibles Session garantie

A distance

du 23 mars au 25 mars	du 15 juil. au 17 juil.	du 2 nov. au 4 nov.
du 20 avr. au 22 avr.	du 21 sept. au 23 sept.	du 14 déc. au 16 déc.

Paris

du 23 mars au 25 mars	du 15 juil. au 17 juil.	du 2 nov. au 4 nov.
du 20 avr. au 22 avr.	du 21 sept. au 23 sept.	du 14 déc. au 16 déc.