L'AKADÉMIE DU DIGITAL · TRAINING PROGRAMME Qualiopi certification being prepared

DevSecOps

FOR-DEV-M4-A · Development, DevOps & Data

Intégrer la sécurité tout au long de la chaîne de développement et de déploiement

DURATION
28 heures — 4 jours

PRICE
1?960 € HT

AUDIENCE
Schools & training centres

ACCESS
Access within 2 working days after validation of needs and prerequisites.

Tarif établi sur la base de 28h à 70 € HT/h. Parcours dédié aux écoles et centres de formation, établi sur devis ; tarif indicatif et négociable selon le volume et le contexte.

Le module alterne séquences théoriques et ateliers pratiques tout au long de chaque journée. Il prolonge la chaîne DevOps en y intégrant la sécurité (« shift left ») : culture DevSecOps, vulnérabilités applicatives, sécurité du code et des dépendances, sécurité du pipeline et des conteneurs, tests dynamiques et gestion des vulnérabilités. Le fil rouge des ateliers est GitLab CI.

Learning objectives

- Comprendre la philosophie DevSecOps : « shift left », la sécurité comme responsabilité de tous
- Identifier les principales vulnérabilités applicatives (sensibilisation OWASP Top 10)
- Intégrer des contrôles de sécurité automatisés dans un pipeline CI/CD (SAST, DAST, SCA)
- Gérer les secrets, les dépendances et la sécurité des conteneurs et des images
- Mettre en place une démarche de tests de sécurité et de gestion des vulnérabilités
- Connaître les bases de la conformité, de la traçabilité et de la réponse aux incidents

Target audience

- Étudiants et apprenants des écoles et centres de formation partenaires
- Développeurs et profils DevOps souhaitant intégrer la sécurité à leur pratique
- Profils techniques visant des fonctions DevSecOps / sécurité applicative

Prerequisites

La maîtrise des bases DevOps et CI/CD est requise (module « DevOps & CI/CD » fortement recommandé), ainsi qu'une aisance avec Git, Docker et un pipeline. Des notions de développement web facilitent la compréhension des vulnérabilités. Ces éléments sont validés par un formulaire en ligne et / ou un entretien préalable.

- Maîtriser les bases DevOps et CI/CD (module DevOps & CI/CD conseillé).

- Être à l'aise avec Git, Docker et un pipeline d'intégration.
- Avoir des notions de développement web (un atout pour les vulnérabilités).
- Disposer d'une autonomie technique et d'une sensibilité aux enjeux de sécurité.

Programme

Jour 1 — Culture DevSecOps & menaces applicatives

Du DevOps au DevSecOps	1h15	« Shift left », sécurité partagée, ce que le DevSecOps change ; cadre défensif et éthique. Exposé interactif, schéma de la chaîne sécurisée, rappel du cadre éthique.	Questions orales ; QCM sur la culture DevSecOps.
Surface d'attaque	2h15	Cartographier la surface d'attaque d'une application. TP guidé, application de test, grille d'analyse.	Cartographie de la surface d'attaque validée.
Panorama des vulnérabilités (OWASP)	1h00	Sensibilisation à l'OWASP Top 10 et aux vulnérabilités courantes. Exposé, exemples illustrés, références OWASP.	QCM sur l'OWASP Top 10.
Repérer des vulnérabilités	2h30	Identifier des vulnérabilités sur une application volontairement vulnérable. TP sur environnement de test dédié, repérage encadré, débriefing.	Vulnérabilités identifiées validées.

Jour 2 — Sécurité du code & des dépendances

Analyse statique (SAST)	1h15	Principes du SAST, revue de code orientée sécurité. Exposé, exemples de findings, bonnes pratiques.	Questions orales ; QCM.
Intégrer un outil SAST	2h15	Mettre en place un SAST et interpréter les résultats. TP guidé, outil SAST, analyse des rapports.	Analyse SAST validée.
Dépendances (SCA) & secrets	1h00	Sécurité des dépendances et gestion des secrets. Exposé, exemples de CVE, bonnes pratiques de gestion des secrets.	QCM sur SCA et secrets.
Dépendances & secrets	2h30	Détecter des dépendances vulnérables et sécuriser des secrets. TP, scanner de dépendances, coffre à secrets.	Détection et sécurisation validées.

Jour 3 — Sécurité dans le pipeline & les conteneurs

Sécurité dans la CI/CD	1h15	Security gates, automatisation des contrôles de sécurité. Exposé, schéma de pipeline sécurisé, exemples.	Questions orales ; QCM.
Sécuriser le pipeline (GitLab CI)	2h15	Ajouter des contrôles de sécurité automatisés au pipeline. TP guidé GitLab CI, étapes de sécurité, accompagnement.	Contrôles de sécurité intégrés validés.
Sécurité des conteneurs & images	1h00	Scan d'images, durcissement, bonnes pratiques. Exposé, exemples de vulnérabilités d'images.	QCM sur la sécurité des conteneurs.
Scanner & durcir une image	2h30	Scanner et durcir une image de conteneur. TP, scanner d'images, remédiation, revue collective.	Image durcie validée.

Jour 4 — Tests dynamiques, conformité, réponse & projet

Tests dynamiques (DAST) & vulnérabilités	1h00	Principes du DAST, gestion et priorisation des vulnérabilités. Exposé, exemples de scans, méthode de priorisation.	QCM sur le DAST.
Scan DAST & priorisation	2h00	Lancer un scan DAST et prioriser les correctifs. TP, outil DAST sur environnement de test, plan de remédiation.	Scan DAST et priorisation validés.
Conformité & réponse aux incidents	1h00	Conformité, traçabilité, logs de sécurité, bases de la réponse aux incidents. Exposé, exemples, bonnes pratiques de traçabilité.	QCM sur conformité et réponse.
Chaîne CI/CD sécurisée & restitution	2h30	Sécuriser une chaîne CI/CD de bout en bout et présenter. TP de synthèse, présentations, revue collective, QCM final, enquête de satisfaction.	Évaluation sommative : pipeline sécurisé + QCM final.

Teaching methods and resources

In-person training at our premises or yours, in small groups. A mix of theory, hands-on workshops and practical scenarios.

Required equipment :

16 Go de Ram recommandés

- Les stagiaires doivent disposer d'un PC avec le Wifi et 16 Go de RAM recommandés.
- Effectif adapté au format école / centre de formation.
- Parcours dédié aux écoles et centres de formation, établi sur devis.

Assessment methods

Learning outcomes are assessed during and at the end of the training; an attendance certificate is given to every learner.

Accessibility

Training accessible to people with disabilities. Contact us before registering so we can study the adjustments needed.

Funding

Quote or training agreement on request. Qualiopi certification is being prepared: eligibility for OPCO funding will open once it is obtained.

Certification audit planned for T1 2027. No OPCO eligibility before it is obtained.