

Formation DevSecOps, Les fondamentaux

Présentation

Cette formation de 2 jours introduit les fondamentaux du DevSecOps pour des profils débutants.

Elle clarifie les notions clés (DevOps, sécurité applicative, CI/CD) et montre comment intégrer la sécurité dès les premières étapes du cycle de vie logiciel.

Au travers de démonstrations et d'exercices guidés, les participants découvrent les pratiques, outils et réflexes essentiels pour contribuer à une démarche DevSecOps au sein de leur organisation.

Durée : 14,00 heures (2 jours)

Tarif INTRA : [Nous consulter](#)

Objectifs de la formation

- Comprendre les principes clés de DevOps et la place de la sécurité (Shift Left) dans le cycle de vie logiciel.
- Identifier les risques de sécurité courants (OWASP Top 10) et les surfaces d'attaque dans une chaîne de livraison.
- Découvrir les pratiques d'intégration de la sécurité dans l'intégration continue et le déploiement continu (CI/CD).
- Comprendre les rôles, responsabilités et flux de collaboration entre Dev, Sec et Ops.
- Identifier des premières actions concrètes pour amorcer une démarche DevSecOps dans son contexte.

Prérequis

- Connaissances générales en cycle de vie logiciel (Git, build, test manuel).
- Notions basiques de ligne de commande.
- Appétence pour la collaboration inter-métiers.

Public

- Développeurs, testeurs QA, ingénieurs IT/Ops, chefs de projet et Product Owners débutant sur DevSecOps.



- Contextes : équipes IT/numériques d'entreprises, ESN, projets internes, premiers appels d'offres intégrant des exigences de sécurité.
- Expérience attendue : notions de base en développement ou en exploitation ; aucune expérience préalable en sécurité n'est requise.

Programme de la formation

Jour 1 – Comprendre les bases de DevSecOps et le Shift Left

Session du matin :

- Panorama DevOps : concepts, flux de valeur, pipeline CI/CD, culture et collaboration
- Pourquoi DevSecOps ? Principes, bénéfices, menaces actuelles, conformité, introduction au Shift Left
- Surfaces d'attaque et risques : revues OWASP Top 10 (vue débutant) et exemples concrets

Session de l'après-midi :

- Acteurs et responsabilités : Dev, Sec, Ops – modèles de gouvernance et communication
- Exemples de contrôles de sécurité en amont : gestion des secrets, dépendances, SBOM (notion), revue de code
- Démonstration guidée : du commit au build, où insérer des contrôles simples

TP / Exercice :

- Mise en place d'un dépôt d'exemple (GitHub/GitLab), configuration basique du workflow (README, règles simples), identification de 5 risques sur un mini-projet fourni et proposition de parades initiales. Livrable : fiche risques initiale et check-list de contrôles à intégrer

Points clés & takeaways :

- Vision claire du DevSecOps et du Shift Left
- Cartographie initiale des risques et premières actions simples à valeur rapide

Jour 2 – Intégrer des contrôles de sécurité dans une CI/CD débutante

Session du matin :

- Introduction aux contrôles automatisés : SAST (analyse de code), SCA (dépendances), analyse de secrets
- Notions de conteneurisation sécurisée : images, registres, bonnes pratiques de base
- Politique minimale : qualité + sécurité – seuils, rapports, remontées d'alertes

Session de l'après-midi :

- Mise en pratique guidée : ajout d'un job SCA et secrets scanning sur le pipeline de l'exemple
- Lecture et interprétation de rapports – passer d'alertes à des actions concrètes
- Plan d'amorçage DevSecOps : 30-60-90 jours, rôles, quick wins, indicateurs simples

TP / Exercice :

- Extension du pipeline de l'exemple avec un contrôle SCA (dépendances) et un scan de secrets. Correction d'au moins 2 findings simples. Livrable : pipeline mis à jour + rapport synthèse (actions menées, résultats, prochaines étapes)

Points clés & takeaways :

- Savoir où et comment intégrer 2 à 3 contrôles de sécurité simples dans une CI/CD
- Plan d'action initial pour poursuivre la démarche DevSecOps après la formation

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur à travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.