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

Mis à jour le 06/04/2025

S'inscrire

Formation découverte du DevSecOps

1 jour (7 heures)

PRÉSENTATION

Notre formation Découverte du SecOps offre aux architectes, développeurs et experts sécurité une vision partagée des enjeux, leur permettant de parler le même langage et d'initier une démarche structurée.

Notre programme de formation vous permettra de vous familiariser avec les concepts et les compétences nécessaires pour identifier et adresser efficacement les vulnérabilités, depuis la conception logicielle jusqu'aux opérations en production.

Des démonstrations et des retours d'expérience viendront illustrer comment une culture SecOps solide permet aux architectes, développeurs et équipes de sécurité de parler le même langage et collaborer de manière fluide.

À l'issue de cette formation, vous aurez une vue claire sur les possibilités offertes par le SecOps dans votre entreprise.

OBJECTIFS

- Acquérir un socle commun de connaissances sur les concepts clés de la sécurité opérationnelle (SecOps) et ses liens avec DevOps (DevSecOps)
- Comprendre les enjeux et les contraintes de la sécurité dans le cycle de vie des applications et des infrastructures
- Évaluer l'opportunité et la pertinence d'adopter une démarche SecOps / DevSecOps au sein de l'organisation

PUBLIC VISÉ

- Architectes logiciels
- Équipe Cybersécurité

- Développeurs référents
- Éventuellement, Ops/Administrateurs système intéressés par l’aspect sécurité

Prérequis

- Connaissances de base en développement et/ou architecture logicielle
- Sensibilité à la cybersécurité (pas besoin d’être expert)

Programme de notre formation découverte du DevSecOps

Introduction à la Sécurité Opérationnelle (SecOps)

- Contexte et définitions
- De DevOps à SecOps : pourquoi la sécurité est-elle désormais au cœur de l’opérationnel ?
- Différences et complémentarités entre SecOps et DevSecOps
- Enjeux et tendances actuelles
- Multiplication des cybermenaces et complexité grandissante des systèmes
- Évolution des responsabilités et nécessité de la collaboration

Fondamentaux de la Sécurité dans la Chaîne de Valeur

- Cycle de vie d’une application et points de contrôle (de la conception à la production)
- Principales vulnérabilités (OWASP Top 10, erreurs de configuration, etc.) et méthodologies de détection
- Risques liés à l’infrastructure : configuration, réseau, conteneurs, virtualisation, cloud
- Contraintes réglementaires : RGPD, ISO 27001, etc. (selon le contexte de l’organisme)
- Comprendre les grands concepts de risques et de vulnérabilités pour un langage commun

Les Piliers du SecOps

- Culture et organisation
- Collaboration entre équipes : partage de responsabilités, décloisonnement des silos
- Intégration des équipes Sec et Ops tout au long du cycle de livraison
- Automatisation et outils
- Supervision et monitoring de la sécurité (SIEM, SOC, etc)
- Gestion des vulnérabilités
- Identity and Access Management (IAM)
- Processus de gestion des incidents
- Détection, réaction et remédiation
- Retours d’expérience et amélioration continue
- Identifier comment intégrer la sécurité dans l’opérationnel (process, culture, outils)

Panorama DevSecOps

- Qu’est-ce que DevSecOps ?
- Comment et pourquoi “shifter” la sécurité à gauche
- Exemples de pipelines sécurisés
- Pratiques et outils clés
- SAST, DAST, IAST, Container Security, IaC Security
- Outils de CI/CD intégrant des contrôles de sécurité
- Retours d’expérience
- Cas concrets d’entreprises ayant mis en place une démarche DevSecOps (succès, échecs, leçons apprises)
- Continuité entre SecOps et DevOps
- Importance du “Shift Left”

Étude de Cas / Synthèse

- Mise en situation : discussion ouverte autour d’un cas d’usage concret (par exemple, un projet interne existant)
- Questions/Réponses : forum ouvert pour clarifier les points clés
- Synthèse : reprise des concepts majeurs et conseils pour amorcer la démarche en interne

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.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l'État.
© Ambient IT 2015-2025. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg