Synapsys

Programme mis à jour le 28 octobre 2026

DevSecOps

DESCRIPTION

Intégrez la sécurité à chaque étape de votre chaîne DevOps : de la gestion des secrets à l'analyse de code, en passant par la sécurisation des pipelines CI/CD et des infrastructures as code.

2090€ HT par participant

2 jours (14 heures)

Présentiel ou distanciel

Intra ou inter-entreprise

PROGRAMME DÉTAILLÉ DE LA FORMATION

1 Introduction à DevSecOps

- Culture shift-left, responsabilité partagée
- Risques sécurité liés à l'automatisation
- DevSecOps vs approche traditionnelle de la sécurité

2 Gestion des secrets et des accès

- Gestion des secrets dans les pipelines (Vault, Azure Key Vault, GitHub secrets)
- Rotation des clés, accès conditionnels, RBAC/PIM

3 Analyse de code et de dépendances

- SCA / SAST : GitHub Advanced Security, SonarQube, Snyk, Checkov
- Scanning des containers et images Docker
- Cas pratique : faille dans une dépendance NPM ou NuGet

4 Sécurité des infrastructures et des pipelines

- Security as Code / Policy as Code (OPA, Sentinel)
- Scanner les configurations IaC (Terraform, ARM, Bicep)
- Intégration dans les pipelines : alertes, blocages, reporting

5 Surveillance et remédiation

- Logs et audit trail sécurité
- Intégration avec SIEM (Defender, Sentinel, Splunk)
- Mise en place d'un playbook de remédiation

6 Atelier final : Sécuriser une chaîne DevOps existante

- Détection de vulnérabilités
- Mise en place de contrôles automatisés
- Analyse des risques résiduels

PUBLIC CONCERNÉ

- DevOps intermédiaires ou confirmés,
- Equipes sécurité (SOC, RSSI technique, architecte SSI),
- Développeurs souhaitant intégrer des pratiques sécurisées,
- Ingénieurs cloud, lead DevOps et DSI techniques.

PRÉ-REQUIS

- Une expérience en environnement DevOps est indispensable,
- Connaissance des pipelines CI/CD,
- Pratique de l'IaC (Terraform, ARM ou Bicep),
- Bases en sécurité informatique recommandées.

OBJECTIFS PÉDAGOGIQUES

- **Intégrer la sécurité** dès les premières étapes du cycle de développement (approche shift-left)
- **Identifier les risques** liés aux dépendances, configurations, pipelines et secrets
- **Utiliser les outils** de scanning, d'analyse de code et de policy as code
- **Adopter les bonnes pratiques** de sécurité dans une démarche CI/CD moderne
- **Comprendre les rôles et responsabilités** entre développeurs, DevOps et équipes sécurité