Formation **DevSecOps : pratiques et outils**

Cette formation DevSecOps offre une immersion complète dans les pratiques et outils de sécurité intégrés dans le cycle de développement logiciel (SDLC). En combinant la sécurité dès les premières étapes de développement, les participants apprennent à bâtir une chaîne CI/CD sécurisée et à appliquer les bonnes pratiques de sécurité dans des environnements conteneurisés et Kubernetes. Le programme couvre des outils de premier plan tels que SonarQube, OWASP ZAP, Snyk, Vault, ainsi que des scanneurs de vulnérabilités comme Trivy et Clair, permettant aux professionnels de détecter et corriger les vulnérabilités de manière proactive. Les participants acquièrent également des compétences en gestion des secrets, en sécurité des images et des conteneurs, en observabilité et en surveillance, afin de renforcer la sécurité des applications dans un cadre DevSecOps moderne.

Durée
3 jours

Objectifs pédagogiques

- Comprendre et appliquer les principes du DevSecOps
- Mettre en place une chaîne d'intégration continue sécurisée et automatisée
- Sécuriser les environnements d'exécution conteneurisés
- Intégrer Kubernetes dans la démarche DevSecOps

Public
Développeurs, ingénieurs DevOps, architectes Cloud, administrateurs systèmes, et responsables sécurité

Prérequis
Une connaissance de base en développement logiciel et en administration de systèmes, avec une familiarité avec les concepts de CI/CD.
Une expérience pratique avec Docker et Kubernetes est également recommandée.

Programme de formation

Phase d'inclusion

Introduction au DevSecOps

Fondamentaux du DevSecOps: Gouvernance, Conformité, Gestion des risques
Outillage DevSecOps: SonarQube, OWASP ZAP, Snyk, Clair, Trivy, Checkov, Vault)

Sécurisation d'une chaine CI/CD

Mise en œuvre d'une chaîne CI/CD avec Gitlab
Gestion des secrets
Analyse statique de code
Vérification de la conformité
Tests automatisés
Vulnérabilités dans le code source
Analyse SBOM et vulnérabilités dans les dépendances

Sécurisation des environnements conteneurisés

Introduction à la sécurité des conteneurs
Fondamentaux des conteneurs Linux
Bonnes pratiques pour la gestion des conteneurs (Docker, OCI, Podman)
Utilisation de scanneurs de vulnérabilités (Clair, Trivy)
Sécuriser l'exécution des conteneurs
Utilisation de SELinux, AppArmor, Seccomp, Capabilities
Observabilité et sécurité des conteneurs
Utilisation de Falco pour la détection d'anomalies
Utilisation de Prometheus et Grafana pour la surveillance
Gestion des secrets
Utilisation de Vault pour la gestion des secrets

Intégration de Kubernetes dans la démarche DevSecOps

Fondamentaux de Kubernetes
Sécurité du cluster Kubernetes
Audit de sécurité et de conformité (CIS Benchmarks, kube-bench et kubesec)
Gestion des identités et des accès (RBAC)
Sécurité des déploiements
Définition d'une chaîne CI/CD pour Kubernetes
Gestion des secrets
Gestion des images avec des registres sécurisés
Tests de sécurité avec scanners de vulnérabilité