RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

DEVSECOPS

Le **DevSecOps** est une méthodologie qui vise à inclure les pratiques de sécurité dans le processus de développement et de mise en production d'applications. Les bonnes pratiques de sécurité suivantes sont à considérer.

→ **Réaliser et maintenir à jour une cartographie des applications utilisées :** les droits système, les secrets d'installation et de fonctionnement, les matrices de flux, les rôles des développeurs (relecture, validation, droits sur les environnements, etc.), les référents ayant la connaissance globale (technique et métier).

→ **Faire une analyse de risque globale** en prenant en compte les chemins de compromission des postes des développeurs, de la sous-traitance, de la chaîne CI/CD* (*Continuous Integration/Continuous Deployment*) et des technologies utilisées (ex. : *cloud*).

→ **Considérer que les actions réalisées par la CI/CD de production sont des actions d'administration.** Il est recommandé de dédier un poste d'administration pour la CI/CD de production, d'appliquer le principe de moindre privilège, de générer à la demande les jetons (*tokens*), et de journaliser et superviser la CI/CD.

→ **Gérer les secrets de manière sécurisée.** Il est recommandé d'utiliser un gestionnaire de secrets distinct par environnement (ex. : hors production, production). Il convient également de s'assurer de l'absence de secrets en dur dans le code source, dans les journaux d'événements des tâches (*jobs*), ou dans les dépôts de code.

→ **Gérer les dépendances avec rigueur** : les minimiser, les évaluer et appliquer les correctifs de sécurité avant déploiement.

→ **Prévoir des tests de sécurité automatisés dans la CI/CD** : tests de non-régression (pour éviter de nouvelles vulnérabilités), étanchéité entre profils d'utilisateurs, tests d'analyses statique et dynamique, tests de conformité de l'IaC (*Infrastructure as Code*).

→ **Sécuriser le déploiement en production des applications** en maintenant l'intégrité du code source de bout en bout, en signant et vérifiant les signatures des tags de version des artefacts.

→ **Implémenter une authentification multifacteur** pour l'accès aux dépôts et pour la signature des *commits*.

→ **Séparer les infrastructures CI/CD de développement et de production** et **ne pas les exposer directement sur Internet.**

→ **Réinstancier régulièrement l'infrastructure CI/CD** et ne pas y stocker de données persistantes.

→ **Être vigilants sur les besoins en confidentialité** vis-à-vis de l'infrastructure de CI/CD (ex. : localisation, tests du code source en SaaS public).

→ **Imposer des règles de développements sécurisés** dans les équipes.

→ **Appliquer des règles de durcissement sur les OS** hébergeant les applications (cf. https://cyber.gouv.fr/guide-linux).

(*) La chaîne CI/CD comprend plusieurs outils, par exemple : orchestrateur, dépôts de code source, tests automatisés, gestionnaire de secrets, outils de déploiements, artefacts.

V1.0 (02/24)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr