Mise en place d'outillage DevSecOps

Assigné

FR

LM **Laurent MATHIEU**
créé : 19/…

En tant qu'administrateur système DevOps, vous repartez du pipeline CI/CD mis en place lors du bref 8 pour l'application de vote en ligne.

Suite à un incident de sécurité lié à une faille applicative non détectée lors d'une release précédente, le RSSI est soucieux de la vélocité accrue des déploiements aux outils CI/CD. En effet, ces déploiements fréquents et rapides ne laissent pas suffisamment de temps pour effectuer les tests de sécurité nécessaires.

Le RSSI souhaiterait donc évaluer puis mettre en place une approche DevSecOps afin de palier à cette limite des méthodes traditionnelles de sécurité dans un environnement DevOps. Il a donc demandé aux équipes DevOps et SRE d'évaluer l'automatisation des tests de sécurité à l'intérieur même du pipeline CI/CD.

Référentiels

Administra
Cloud

Contexte du projet

Les outils suivants sont préconisés par l'équipe sécurité afin d'automatiser les tests de sécurité dans le pipeline CI/CD :

Static application security testing

- SonarQube

Software composition analysis

- OWASP Dependency-Check
- Clair https://github.com/quay/clair
- Trivy https://github.com/aquasecurity/trivy
- Grype https://github.com/anchore/grype

Dynamic application security testing

- OWASP Zap

Afin de mener à bien ces objectifs, vous allez devoir implémenter les éléments suivants à partir de votre pipeline CI/CD existant :

- Les tests doivent être réalisés dans un environnement de test temporairement créé par le pipeline CI/CD lors de la phase de 'Test'. Cet environnement est différent de l'environnement de

production de la phase ‘Deploy’. Vous devez utiliser deux outils différents de deux catégories différentes à partir des outils recommandés par l’équipe sécurité. Vous allez devoir analyser les différentes options proposées par l’équipe sécurité et documenter sur quelles bases vous avez choisi vos deux outils sélectionnés. Le déploiement en production sera automatique si les tests de sécurité du pipeline passent avec succès. Le déploiement devra être interrompu si l’un des outils remonte une ou plusieurs alertes. Un membre désigné de votre équipe, ainsi qu’un membre de l’équipe sécurité auront l’autorité pour pouvoir continuer le déploiement malgré l’alerte l’ayant interrompu (contrôle paritaire). Vos instructeurs prendront le rôle des membres de l’équipe sécurité. Des métriques et/ou tableaux de bord doivent être collectes afin d’avoir des statistiques sur les tests de sécurité. Le format est libre.

- Vous devez utiliser deux outils différents de deux catégories différentes à partir des outils recommandés par l’équipe sécurité. Vous allez devoir analyser les différentes options proposées par l’équipe sécurité et documenter sur quelles bases vous avez choisi vos deux outils sélectionnés.
- Le déploiement en production sera automatique si les tests de sécurité du pipeline passent avec succès.
- Le déploiement devra être interrompu si l’un des outils remonte une ou plusieurs alertes. Un membre désigné de

votre équipe, ainsi qu'un membre de l'équipe sécurité auront l'autorité pour pouvoir continuer le déploiement malgré l'alerte l'ayant interrompu (contrôle paritaire). Vos instructeurs prendront le rôle des membres de l'équipe sécurité.

Travail complémentaire :
Des métriques et/ou tableaux de bord doivent être collectes afin d'avoir des statistiques sur les tests de sécurité. Le format est libre.

- Implémentez les autres outils de tests de sécurité automatisés et intégrez-les dans le pipeline CI/CD.

Modalités pédagogiques

Travail individuel

Modalités d'évaluation

A definir.

Livrables

1/ Analyser les différents outils de tests de sécurité automatisés et expliquer des avantages et inconvénients de chacun (minimum 1000 mots).

2/ Configuration du pipeline CI/CD avec les outils de tests de sécurité automatisés (fichiers de configuration et/ou impressions d’écrans avec explications).

3/ À la fin de la semaine de formation (vendredi), vous réaliserez une démonstration en 10 minutes du bon fonctionnement des outils.

Critères de performance

A definir.