Rapport de Réflexion : Lab 3

Sécurité Cloud & DevSecOps

30 décembre 2025

1 Résumé de l'état initial (Baseline)

Avant toute intervention, les outils d'analyse statique ont révélé une surface d'attaque significative :

Checkov

147 échecs critiques

Semgrep

6 vulnérabilités détectées

2 Actions de remédiation appliquées

Les vulnérabilités ont été corrigées à trois niveaux clés de l'infrastructure :

Terraform Sécurisation de l'infrastructure Cloud.

- Suppression de l'accès public sur les buckets S3.
- Restriction des règles de sécurité (Security Groups) trop permissives.

Kubernetes Durcissement (Hardening) du déploiement.

- Désactivation du mode privilégié et de l'escalade de privilèges.
- Forçage de l'exécution via un utilisateur non-root.
- Épinglage (pinning) des versions d'images pour la reproductibilité.

Dockerfile Optimisation de l'image de base.

- Migration de `ubuntu:latest` vers `ubuntu:22.04`.
- Création et utilisation d'un utilisateur dédié (`appuser`).

3 Comparaison après corrections

L'application des bonnes pratiques a permis une réduction notable des risques :

Outil	Initial	Final	Amélioration
Checkov	147	115	**-32**
Semgrep	6	0	**-6 (100%)**

4 Observations et patterns identifiés

- **Permissivité par défaut :** Les configurations standard privilégient souvent la facilité d'usage au détriment de la sécurité (ex : `0.0.0.0/0`).
- **Violation du moindre privilège :** Utilisation abusive du compte `root` et politiques IAM trop larges.
- **Risque Supply Chain :** L'usage du tag `latest` introduit une imprédictibilité et des failles potentielles non maîtrisées.

5 Stratégies de prévention futures

Recommandations Proactives

1. **Intégration CI/CD :** Automatiser Checkov et Semgrep pour bloquer tout build contenant des vulnérabilités critiques.
2. **Policy as Code :** Déployer *Open Policy Agent* (OPA) pour appliquer des règles de sécurité strictes sur les manifestes Kubernetes.
3. **Hardening des images :** Privilégier des images minimales (Distroless ou Alpine) et scanner régulièrement les dépendances.