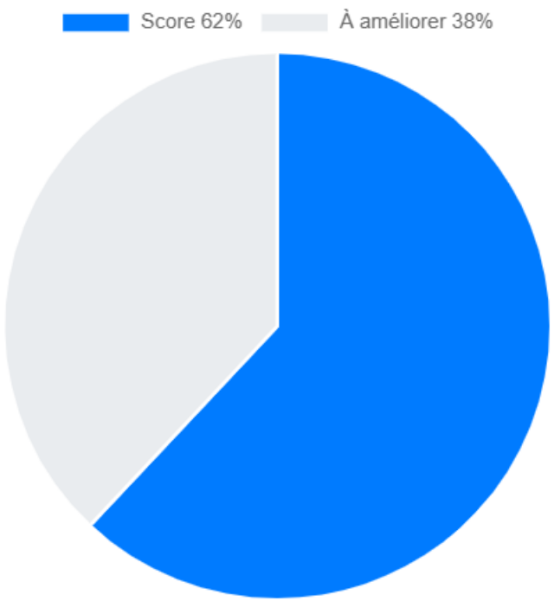
Rapport de Sécurité



Score de Sécurité

Score: 62%

Recommandations

Recommandation	Statut	Note
Faites un audit périodique des accès pour limiter les risques.	En attente	
Utilisez IAM/RBAC pour limiter les privilèges d’accès.	En attente	
Mettez en place des outils de détection d’activités anormales.	En attente	
Protégez vos APIs avec des clés d’accès, authentification et limites de requêtes.	En attente	
Activez les logs pour suivre les accès, erreurs et activités suspectes.	En attente	
Renforcez la console admin avec restriction IP, MFA et journalisation.	En attente	

Conseils Pratiques

Conseil
Activez les alertes de connexion suspecte.
Utilisez un gestionnaire de mots de passe.
Revoyez régulièrement les autorisations.
Stockez vos sauvegardes en lieu sûr.

Conseil
Activez les alertes de connexion suspecte sur votre plateforme cloud.
Utilisez un gestionnaire de mots de passe et activez l’authentification multifacteur (MFA).
Revoyez régulièrement les permissions et rôles dans votre cloud IAM.
Stockez vos sauvegardes dans des zones sécurisées et géographiquement distinctes.
Mettez à jour vos images et conteneurs cloud régulièrement.
Évitez d’exposer des services cloud directement à Internet sans protection.
Chiffrez vos données en transit et au repos dans le cloud.
Effectuez des audits de sécurité et analysez les logs de vos services cloud.
Sécurisez l’accès aux API cloud avec des clés et tokens bien gérés.
Automatisez les correctifs et mises à jour via des pipelines CI/CD sécurisés.

Failles OWASP détectées

Faille	Description	Lien
Contrôle d'accès inadéquat	Des utilisateurs peuvent accéder à des ressources non autorisées.	https://owasp.org/Top10/A01_2021-Broken_Access_Control/
Configuration de sécurité incorrecte	Paramètres par défaut ou services inutiles activés.	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
Insécurité des API	APIs vulnérables sans contrôle ou protection suffisante.	https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_(SSRF)/
Défaillances cryptographiques	Données non chiffrées ou mal protégées.	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/
Identification et authentification non sécurisées	Mauvaise gestion des identifiants et sessions.	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/