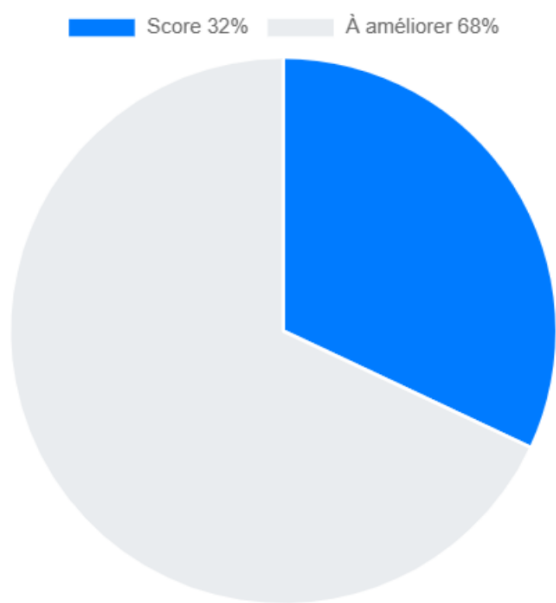


# Rapport de Sécurité



## Recommandations

Recommandation	Statut	Note
Activez la MFA pour renforcer l'accès à vos comptes cloud.	En attente	
Utilisez des mots de passe complexes et un gestionnaire de mots de passe.	En attente	
Évitez le partage public, utilisez des permissions spécifiques.	En attente	
Faites un audit périodique des accès pour limiter les risques.	En attente	
Assurez-vous que les données sont chiffrées pour prévenir les interceptions.	En attente	
Effectuez un audit régulier pour identifier les failles de configuration.	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

Conseil
🔒 Activez les alertes de connexion suspecte.
📝 Utilisez un gestionnaire de mots de passe.
🔄 Revoyez régulièrement les autorisations.
💾 Stockez vos sauvegardes en lieu sûr.
☁️ Activez les alertes de connexion suspecte sur votre plateforme cloud.

## Conseil

Ø=Ý Activez l'authentification multifacteur (MFA).

Ø=Þáp Mettez à jour vos conteneurs régulièrement.

Ø=Þ« Ne jamais exposer les ports inutiles.

Ø=Ý Chiffrez les données en transit et au repos.

Ø=Üñ Sécurisez vos clés et tokens API.

## Faibles OWASP

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