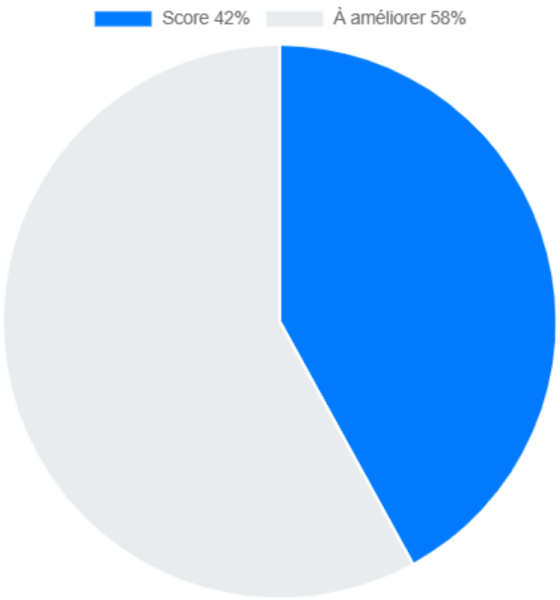
Rapport de Sécurité



Recommandations

Recommandation	Statut	Note
Utilisez des mots de passe complexes et un gestionnaire de mots de passe.	Terminé	
Évitez le partage public, utilisez des permissions spécifiques.	Terminé	
Planifiez des sauvegardes régulières pour prévenir les pertes de données.	Terminé	
Assurez-vous que les données sont chiffrées pour prévenir les interceptions.	En attente	a appliquer des le projet suivant
Utilisez IAM/RBAC pour limiter les privilèges d’accès.	En attente	
Mettez en place des outils de détection d’activités anormales.	En attente	
Sensibilisez à l’usage des services cloud et restreignez les usages non autorisés.	En attente	
Utilisez des outils de gestion centralisée pour avoir une vue d’ensemble.	En attente	
Adoptez une architecture sécurité cloud alignée sur les bonnes pratiques OWASP.	En attente	

Conseils

Conseil
Ø=Ü¡ A c t i v e z l e s a l e r t e s d e c o n n e x i o n s u s p e c t e .

Conseil
Ø=Ý Utilisez un gestionnaire de mots de passe.
Ø=Ý Revoyez régulièrement les autorisations.
Ø=Ü¾ Stockez vos sauvegardes en lieu sûr.
&þ Activez les alertes de connexion suspecte sur votre plateforme cloud.
Ø=Ý Activez l'authentification multifacteur (MFA).
Ø=Þáþ 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.

Failles OWASP

Faille	Description	Lien
Défaillances cryptographiques	Données non chiffrées ou mal protégées.	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/
Configuration de sécurité incorrecte	Paramètres par défaut ou services inutiles activés.	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
Contrôle d'accès inadéquat	Des utilisateurs peuvent accéder à des ressources non autorisées.	https://owasp.org/Top10/A01_2021-Broken_Access_Control/