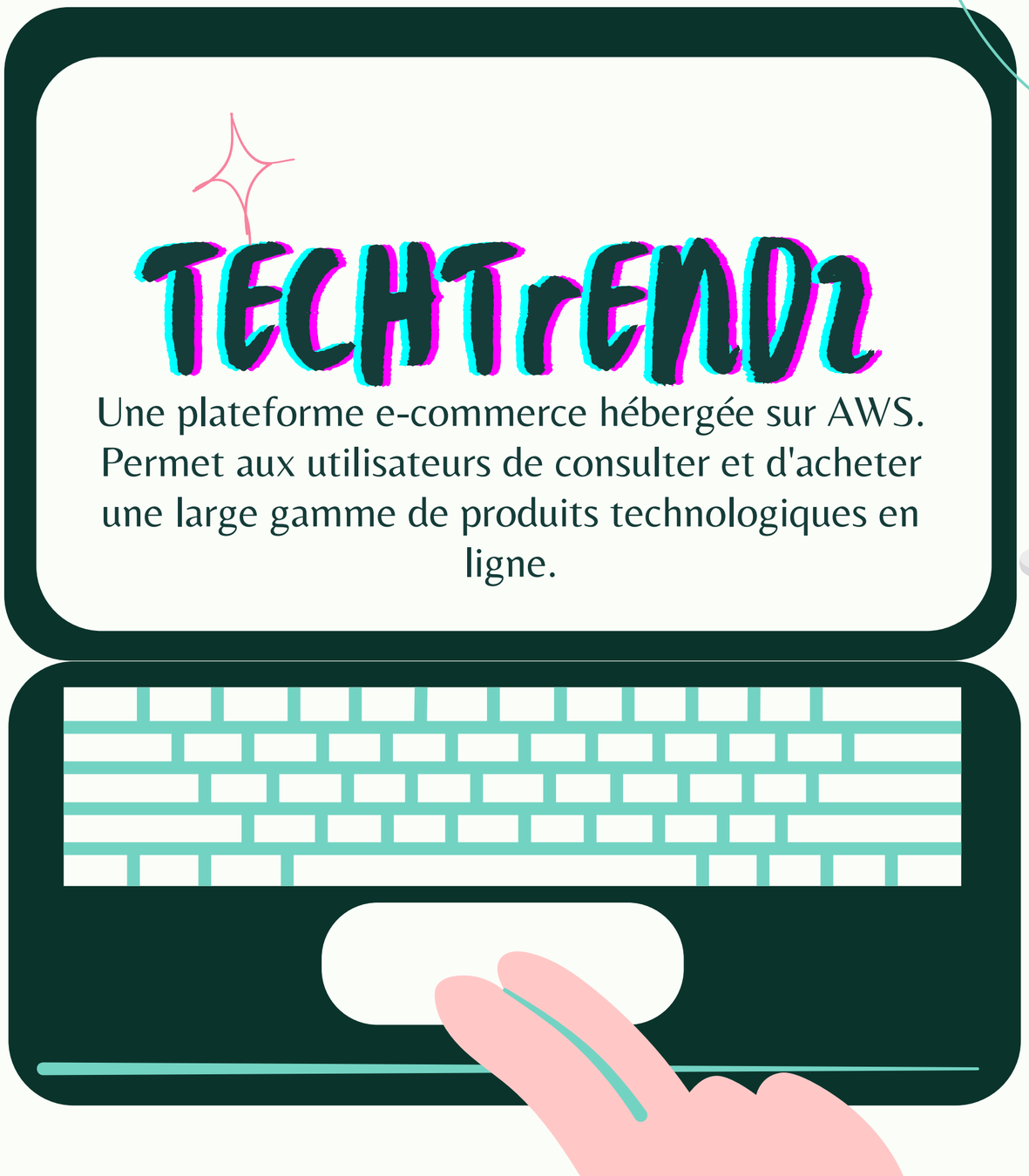
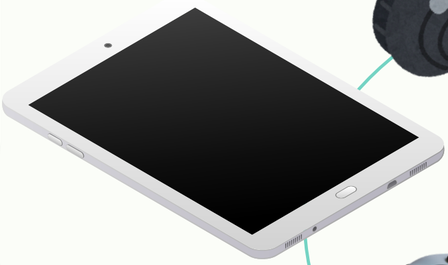
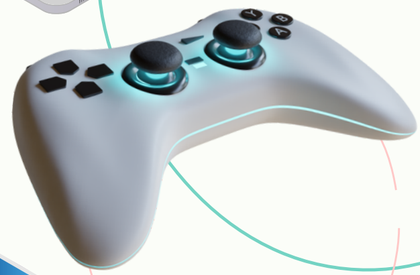
eFrei
PARIS PANTHÉON-ASSAS UNIVERSITÉ

TECHTrENDz

Une plateforme e-commerce hébergée sur AWS. Permet aux utilisateurs de consulter et d'acheter une large gamme de produits technologiques en ligne.







Réalisé par :
Rabab SOLEIMAN
Redwane ZAGHOUINI
Mohamed Anouar BOUACHOUR

Sous la supervision de :
M. KOLSI Houssem

Scénario Cyber	Impact	Vraisemblance	Mitigation	Justification
Accès Non Autorisé aux Bases de Données	élevé	Faible	Chiffrer les données en transit et au repos. Utiliser des groupes de sécurité stricts pour limiter l'accès. Surveiller les accès via CloudWatch et CloudTrail.	La table de routage permet l'accès Internet sortant pour tous les sous-réseaux, y compris ceux contenant des bases de données sensibles.
Compromission des Clés IA	Élevé	Moyenne	Activer MFA pour toutes les actions critiques. Utiliser des rôles IAM avec des permissions minimales nécessaires. Surveiller et gérer les clés d'accès avec rotation régulière.	Des rôles IAM excessivement permissifs peuvent être exploités pour accéder à des ressources sensibles. Des clés compromises pourraient permettre des accès non autorisés, causant des pertes financières et des interruptions de service.
Compromission des S3 Buckets Publics	Élevé	Moyenne	on doit configurer les politiques des buckets S3 avec des permissions minimales. Activer "Block Public Access" pour les buckets sensibles. Utiliser AWS Config et CloudTrail pour surveiller les modifications.	Les S3 buckets stockent souvent des données sensibles . Des politiques S3 mal configurées pourraient permettre à des utilisateurs non autorisés d'accéder aux données sensibles stockées dans des buckets S3 publics.
Exploitation d'une Vulnérabilité dans le Code Lambda	Élevé	Faible	Scanner régulièrement le code Lambda pour des vulnérabilités. Limiter les permissions IAM associées aux fonctions Lambda. Mettre en place des tests de sécurité continus .	Utilisation de commandes shell sans mesures de sécurité supplémentaires. Les commandes shell non sécurisées peuvent être exploitées pour compromettre la fonction Lambda. L'utilisation de la commande subprocess.run avec shell=True pour exécuter pg_dump expose le système à des risques d'injection de commandes si les entrées ne sont pas correctement validées.

Scénario Cyber	Impact	Vraisemblance	Mitigation	Justification
Attaque par Déni de Service Distribué (DDoS)	Élevé	Moyenne	Utilisation d'AWS Shield : on doit activer AWS Shield Standard (inclus) ou Advanced pour protéger vos applications contre les attaques DDoS. Mise en Place de WAF (Web Application Firewall) : on doit Configurer AWS WAF pour filtrer le trafic et bloquer les requêtes malveillantes. Auto-scaling : on doit Configurer l'auto-scaling pour absorber les pics de trafic.	Les serveurs web sont directement accessibles depuis Internet (0.0.0.0/0), ce qui les rend vulnérables aux attaques DDoS et à d'autres types d'intrusions.
Exploitation de Vulnérabilités Logicielles	Élevé	Moyenne	Implémenter un processus de gestion des patches pour corriger rapidement les vulnérabilités. Utiliser des outils de scan de vulnérabilités pour identifier et corriger les failles.	Bases de données sur des instances EC2 avec potentielles vulnérabilités. Une mauvaise configuration des bases de données augmente le risque d'exploitation par des attaquants.
Exposition de Données Sensibles	Très élevé	Élevée	Configuration des Politiques S3, Activation de la Sécurité des S3 Buckets, Outils d'Audit	Les buckets S3 mal configurés peuvent conduire à une exposition accidentelle de données sensibles. Les informations de base de données telles que les mots de passe (db_password) sont passées en clair via les variables d'environnement (os.getenv), ce qui est risqué en cas de compromission du système ou de fuite d'informations.

Scénario Cyber	Impact	Vraisemblance	Mitigation	Justification
Mauvaise Configuration des Groupes de Sécurité	Élevé	Élevée	Effectuer des audits réguliers pour identifier et corriger les règles de sécurité excessivement permissives. Création des modèles de groupes de sécurité pour garantir des configurations cohérentes et sécurisées.	Des règles de sécurité excessivement permissives augmentent le risque de compromission.
Compromission des Instances EC2 (Web Servers)	Élevé	Moyenne	Utiliser un WAF pour filtrer les requêtes malveillantes. Appliquer des correctifs de sécurité régulièrement. Restreindre les permissions IAM pour limiter les actions des instances EC2.	Sous-réseau de production accessible depuis Internet. L'accès direct aux serveurs web depuis Internet expose les instances EC2 à des attaques
Compromission de Compte Administratif	Très élevé	Moyenne	Authentification Multi-Facteur (MFA), Limitation des Droits, Surveillance et Journaux	Accès complet à l'infrastructure via un compte administratif compromis.