

Sécurisation d'une Infrastructure Réseau

Stratégie GRC et analyse des vulnérabilités

Johana Kassab - 27/08/24 - Bloc 1

Objectif : Sécurisation de l'infrastructure Death Star

Plan de la présentation :

Topologie du réseau

Analyse des vulnérabilités

Stratégie GRC

Conclusion

Questions

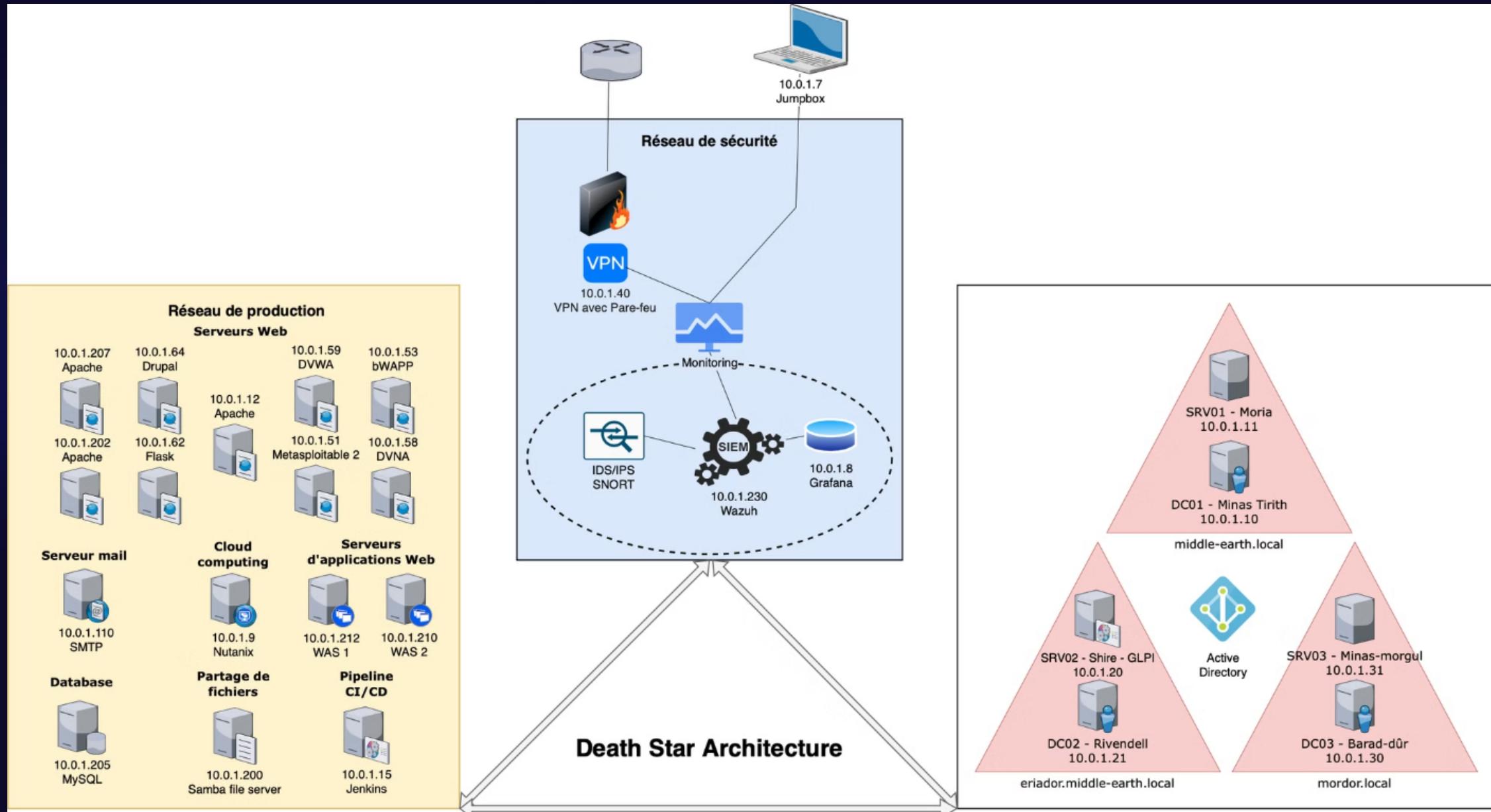
Topologie du réseau Death Star

Projet : Attack Of The Death Star

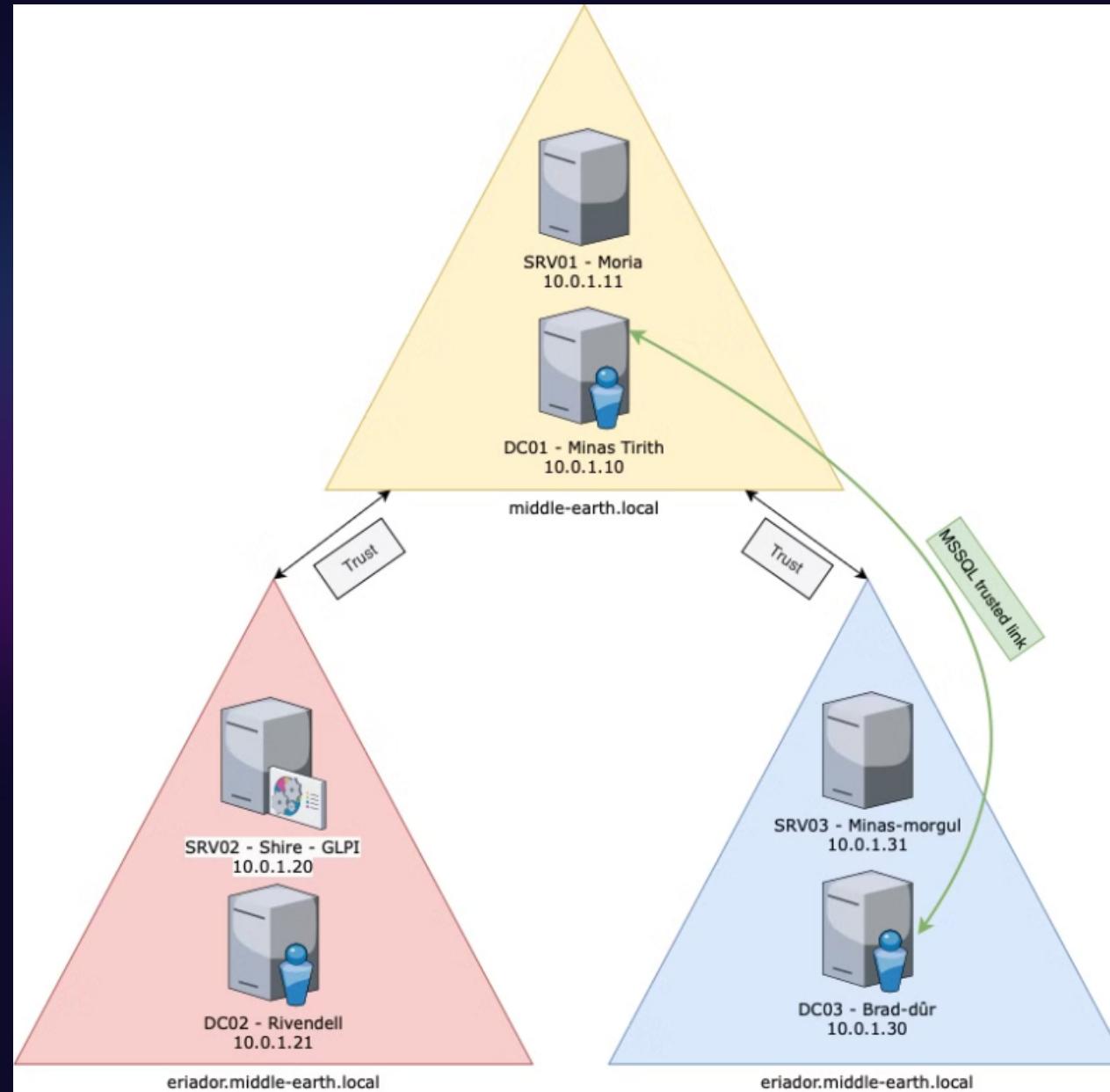
- Vue d'ensemble de la topologie
- Segment 1 : Réseau d'Administration (AD)
- Segment 2 : Réseau de sécurité
- Segment 3 : Réseau de production
- Hôtes virtualisés
- Scénarios de sécurité



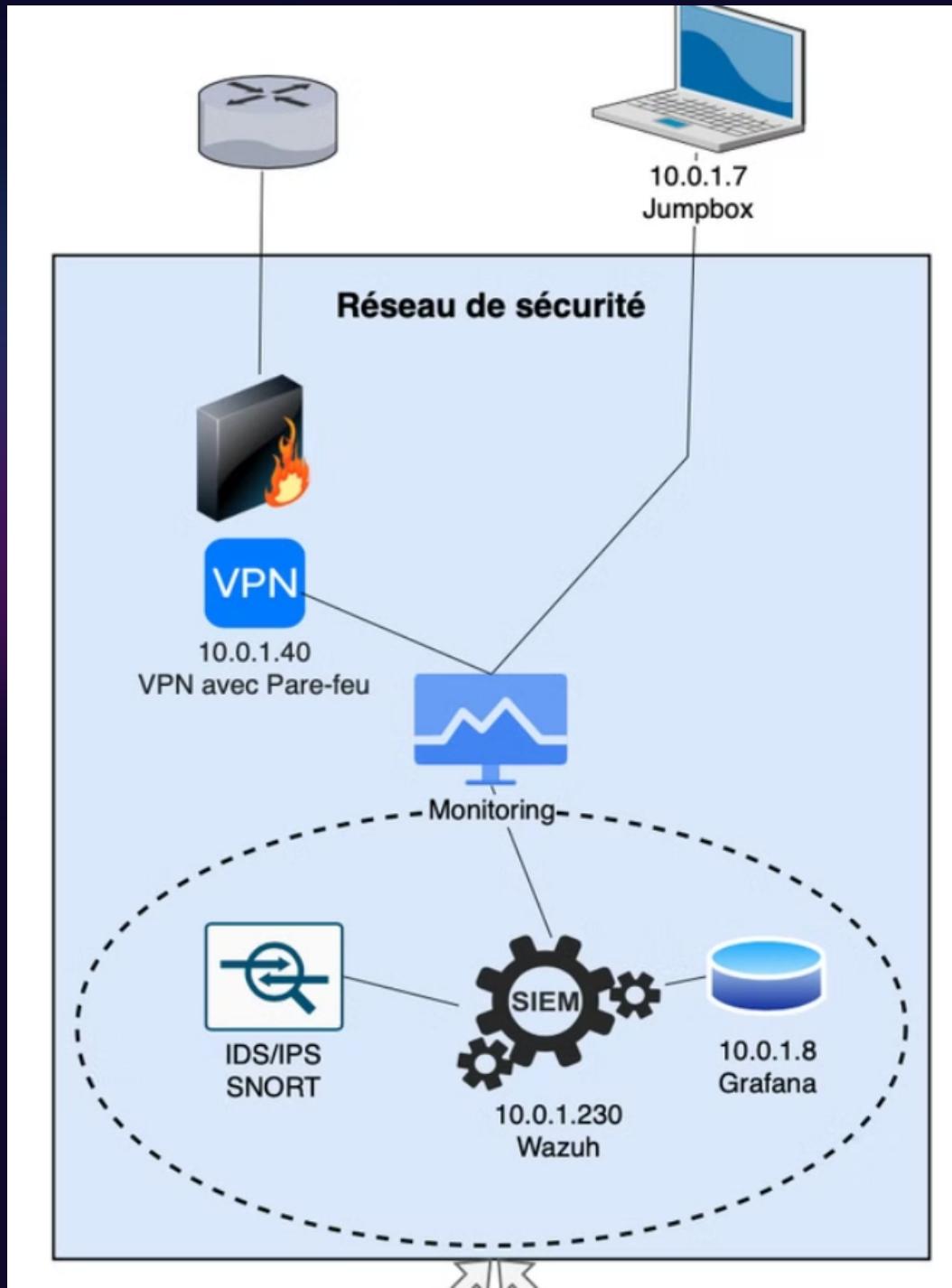
Vue d'ensemble du réseau



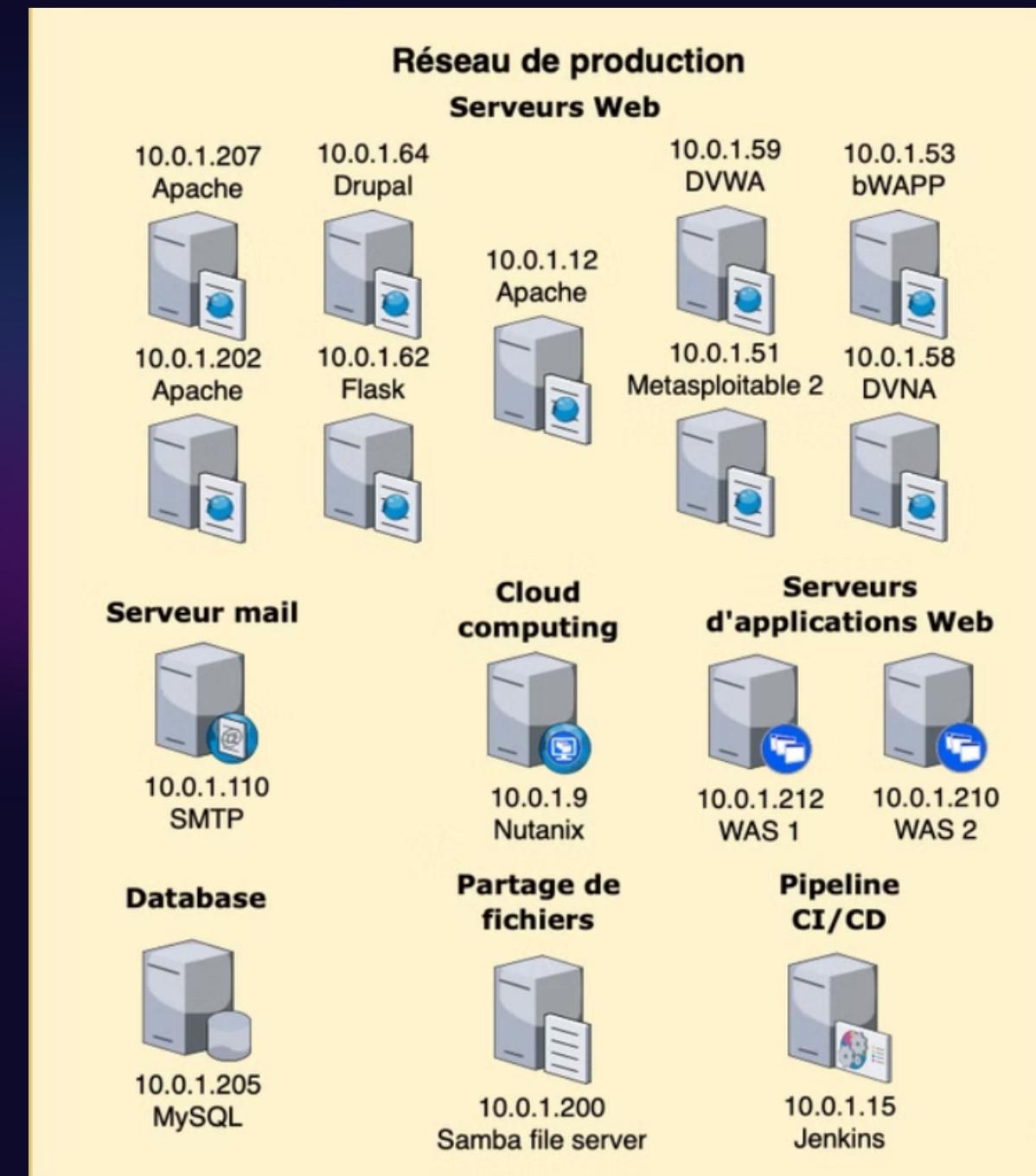
Réseau d'administration



Réseau de sécurité



Réseau de production



Scénarios de sécurité

Scans automatisés

Nessus et Linpeas/Winpeas

Analyse des bases de données

Accessibilité des données sensibles

Analyse de systèmes

Versions, variables, ...

Analyse des sites web

Injections, code, configuration, ...

Analyse des vulnérabilités

Contexte de l'audit : Démarche proactive face aux menaces

- Les vulnérabilités critiques et moyennement graves
- Utilisation du scoring CVSS pour juger de la criticité des vulnérabilités

Vulnérabilités critiques ...



Vuln. 1

Mots de passe en clair sur les pages HTML et PHP

Machines 53 et 59



Vuln. 2

Base de donnée non sécurisée (SHA-1)

Machine 53



Vuln. 3

Absence de filtrage sur les téléchargements

Machines 53 et 59

... et solutions



Vuln. 1

Chiffrement obligatoire des données sensibles

Machines 53 et 59



Vuln. 2

Migration vers des algorithmes de hachage sécurisés (SHA-256 ou Bcrypt)

Machine 53



Vuln. 3

Mise en place de processus de validation de fichiers

Machines 53 et 59

Vulnérabilités moyennement graves ...



Vuln. 4

Mots de passe en clair dans le code

Machines 53 et 59



Vuln. 5

SUID mal configuré

Machine 53



Vuln. 6

Connexion FTP anonyme

Machines 53 et 59

... et solutions



Vuln. 4

Mots de passe en clair dans le code

Machines 53 et 59



Vuln. 5

SUID mal configuré

Machine 53



Vuln. 6

Désactiver l'accès FTP anonyme

Machines 53 et 59

Stratégie de Gouvernance, Risques et Conformité (GRC)

Enjeux : Les failles de sécurité peuvent entraîner des risques financiers, réputationnels et légaux.

- **Gouvernance** : Politiques de sécurité proactive, gestion des accès.
- **Risques** : Mesures techniques comme le chiffrement et la segmentation réseau
- **Conformité** : Respect des normes (NIST, RGPD), mise en place d'audits réguliers

Sécurité et Gestion des accès

Gestion des accès

- **Mots de passe robustes** : Critères de complexité et stockage sécurisé
- **2FA** : Renforce la sécurité avec une authentification à 2 étapes

Sécurisation des données

- **Chiffrement des communications** (LDAPs, HTTPS) : Sécuriser les échanges de données
- **Chiffrement des données au repos** : Protection des données sur les serveurs

Monitoring

- **Surveillance en temps réel** : Déetecter les menaces instantanément
- **Logs** : Analyse des évènements et des accès pour identifier les incidents

Analyse de risques web

- **Détection des failles** : identifier et corriger les vulnérabilités web
- **Validation des entrées utilisateur** : Prévenir les attaques par assainissement des données

Gouvernance, continuité et conformité

Conformité et RGPD

- **Protection des données** : Chiffrement et anonymisation
- **Audits de conformité** : Révisions régulières pour assurer le respect des normes

Mises à jours régulières

- **Gestion des correctifs** : Mises à jour régulières pour combler les vulnérabilités
- **Continuité d'activité** : Garantir un système à jour et sécurisé

Formation du personnel

- **Sensibilisation** : Promouvoir les bonnes pratiques de sécurité
- **Formation continue** : Renforcer les compétences en cybersécurité

Continuité et reprise après sinistre

- **Continuité d'activité** : Plan de sauvegarde pour une reprise rapide
- **Site de secours** : RéPLICATION DES DONNÉES POUR UN REPRISE IMMÉDIATE

Conclusion :

Le moyens pour sécuriser l'infrastructure
Death Star seront mis en place.

Vulnérabilité et solutions à mettre en place ont été identifiés

Une stratégie GRC devrait être déployée



Merci de votre attention

Avez vous des questions ?

Johana Kassab - 27/08/24 - Bloc 1