Atelier IAM – Gestion des identités et des accès

Contexte

Vous êtes consultants en cybersécurité mandatés une entreprise fictive de 500 employés. Elle regroupe plusieurs services : RH, IT, Marketing, Finance, Juridique, Support client, Direction, et des partenaires externes.

L'entrprise utilise plusieurs applications :

- ERP (RH + Finance)
- CRM (clients)
- Messagerie interne
- Dépôt de code (Git)
- VPN entreprise
- Outil de ticketing
- Plateforme e-learning
- Intranet
- Outil de signature électronique
- Cloud partagé

Objectif

Votre mission est de concevoir une stratégie IAM efficace et sécurisée pour gérer les accès aux ressources de l’entreprise.

Profils fictifs à analyser

Utilisateur	Fonction / Rôle	Besoins d'accès principaux
Alice	RH	ERP RH, Messagerie, Intranet
Joe	Développeur IT	Git, VPN, Messagerie, Cloud partagé
Sarah	Prestataire externe	CRM uniquement
Marc	Commercial mobilité	CRM, VPN, Messagerie
Léa	Juriste	ERP Finance, Signature électronique, Intranet
Hugo	Responsable support	Outil ticketing, CRM, Messagerie
Léna	Directrice Marketing	CRM, Intranet, Plateforme e-learning, Messagerie
Tom	Responsable sécurité IT	Accès admin à tous les systèmes, audit, surveillance
Julie	Stagiaire RH	ERP RH (lecture), e-learning
Bob	Partenaire externe	Plateforme e-learning, CRM (lecture)

Tableau d’attribution des accès – À compléter

Utilisateur	Rôle / Groupe	Ressources nécessaires	Niveau d’accès (Lecture / Écriture / Admin)	Remarques
Alice				
Joe				
Sarah				
Marc				
Léa				
Hugo				
Léna				
Tom				
Julie				
Bob				

Étapes de l’atelier

1. Attribution des accès

- Étudiez les profils fournis.
- Déterminez les ressources nécessaires pour chaque utilisateur.
- Précisez le niveau d’accès (lecture, écriture, admin).
- Remplissez le tableau d’attribution.

2. Groupes et rôles

- Créez des groupes (RH, IT, etc.) et des rôles (Admin IT, Employé, Prestataire…).
- Associez chaque utilisateur à un groupe et un rôle.
- Définissez les accès associés à chaque rôle.

3. Scénarios d’incidents

Analysez les incidents simulés :

- Départ d’un stagiaire
- Activité suspecte sur le VPN
- Partage de mot de passe
- Accès non autorisé par un prestataire
- Perte d’un appareil avec accès sensible

Proposez des solutions IAM adaptées à chaque situation.

4. Contraintes réalistes

Prenez en compte :

- Un budget IT limité (MFA partiel)
- Des outils hérités sans SSO
- Des exigences RGPD

Réfléchissez à :

- Quels accès sécuriser en priorité ?
- Comment gérer les prestataires et stagiaires ?
- Quelles mesures IAM sont critiques pour la conformité RGPD ?

Mini Challenge IAM

Vrai ou Faux

1. Un compte orphelin ne pose pas de risque
2. Un stagiaire doit avoir les mêmes droits qu’un employé

3. Le MFA est inutile si les mots de passe sont forts
4. Le provisioning automatique permet de créer et supprimer les comptes selon le cycle de vie
5. Un prestataire externe doit avoir les mêmes droits qu'un employé

Questions

6. Quelle est la meilleure méthode pour gérer les accès d'un stagiaire ?

7. Quel mécanisme IAM permet de limiter l'accès selon l'heure ou le lieu ?

8. Quelle mesure réduit le risque lié au partage de mot de passe ?

9. Que faut-il faire lorsqu'un employé quitte l'entreprise ?

10. Quel est le principal risque d'un compte orphelin ?