
HAFS
Distributeur à valeur ajoutée
VOTRE PARTENAIRE TECHNOLOGIQUE
POUR DES INFRASTRUCTURES IT SÉCURISÉES ET PERFORMANTES
EXPERTISE
Des solutions adaptées à chaque environnement
CONFIANCE
Un partenaire fiable à vos côtés
PERFORMANCE
Des infrastructures sécurisées et évolutives
SUPPORT
Un accompagnement technique de qualité
HAFS
Distributeur à valeur ajoutée
Des solutions IT innovantes pour un monde connecté et sécurisé
WIRELESS RADIO
Connectivité sans fil haute performance
RÉSEAUX & SÉCURITÉ IT
Des réseaux fiables et sécurisés
VIRTUALISATION CLOUD
Des solutions Cloud flexibles et évolutives
CYBERSECURITY
Protéger vos données et vos systèmes
VIDÉO PROTECTION
Solutions de vidéosurveillance intelligentes
HCI STOCKAGE SAUVEGARDE
Stockage, sauvegarde et haute disponibilité
SOLUTIONS IT | CYBERSÉCURITÉ | CLOUD | INFRASTRUCTURE RÉSEAU | STOCKAGE | PROTECTION

Axidian

Comment bâtir une stratégie PAM robuste :

Cybermenaces croissantes en Afrique et gestion des accès à privilèges

Sofia Alexandrovskaya

Regional Manager, Axidian

Ordre du jour

1. Risques et menaces liés aux identités
2. Scénarios d’attaque et comment le PAM aide
3. Q&A

Axidian

Axidian

Pour les identités.
Pour les personnes.

30+
pays sécurisés

800+
projets dans le monde

10+
ans sur le marché

4 produits
et un portefeuille en expansion

Abus des identités : voie rapide vers une violation

186 jours

pour identifier des identifiants compromis

4.67 M$

- coût moyen d'une violation*

*Source: IBM Cost of a data breach report 2025

- Un mot de passe volé
- Un compte privilégié exposé
- Un identifiant VPN réutilisé

Violation de la Caisse Nationale de Sécurité Sociale

500,000+
entreprises affectées

2 M+
employés affectés

50,000+
documents divulgués (identités, salaires, coordonnées bancaires)

Cyberattaque: Air Côte d'Ivoire

Compagnie nationale victime d'une **cyberattaque ransomware**

280 Go de données sensibles exfiltrées:

Données compromises :

- Passagers
- Informations financières
- Contrats internes

Cyberattaque: DGID au Sénégal

Les **services en ligne ont été perturbés**

L'incident a été présenté comme un **« problème technique »**

Menace de **fuite de données financières et fiscales** (ransomware / extorsion)

Axidian

Risques liés aux identités : utilisateurs standard et privilégiés

Erreur humaine

Élévation de privilèges

Usurpation d'identité

Erreurs de configuration

Accumulation de privilèges

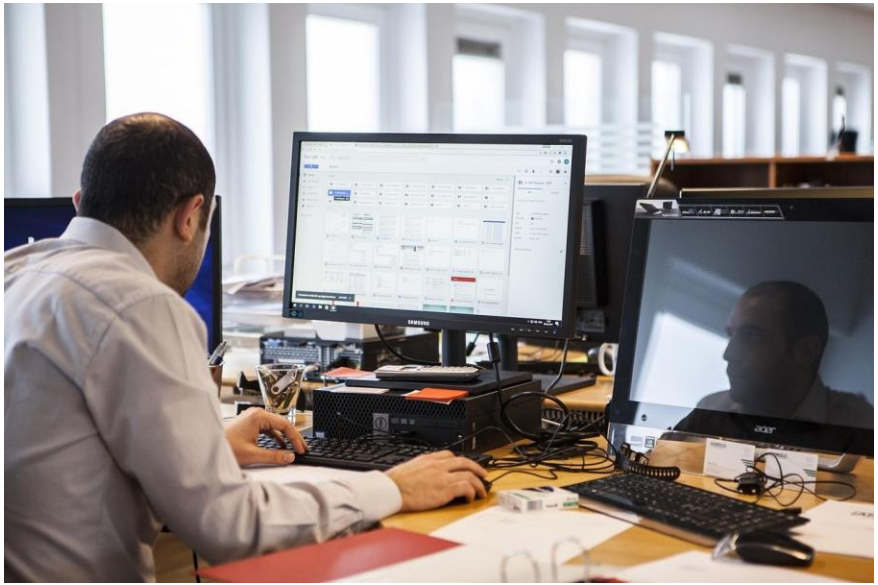
Travailleurs à distance

Mots de passe administrateur partagés

Comptes dormants

Accès des prestataires

Travailleurs à distance et prestataires



Parmi les catégories d'utilisateurs les plus à risque.

Se connectent souvent depuis des appareils personnels ou non gérés.

Savez-vous :

- quelles commandes ils exécutent ?
- combien de temps ils restent connectés ?
- à quels systèmes ils accèdent ?

Scénarios d'attaque vs Gestion des accès à privilèges (PAM)

LA CENTRALE
LE CHOIX INTELLIGENT

Axidian

Ingénierie sociale

- Emails de phishing
- Fausses pages VPN
- Usurpation d’identité par téléphone

La violation d’Uber en 2022
a commencé par une attaque d’ingénierie sociale.

Avec Axidian Privilege (PAM) :

- Pas d’identifiants codés en dur
- Secrets stockés dans un coffre-fort chiffré
- Accès Just-in-Time
- Surveillance des sessions
- MFA obligatoire

Attaques par force brute et credential stuffing

Vitesse de devinette des mots de passe :
Un mot de passe de 8 caractères peut être compromis en moins d’une heure.

Exploitation des mots de passe réutilisés :
Le credential stuffing utilise des mots de passe divulgués lors d’autres violations de données.

Axidian Privilege (PAM) réduit ce risque en :

- supprimant la visibilité des mots de passe pour les utilisateurs
- effectuant une rotation automatique des identifiants
- imposant des exigences de complexité
- limitant les tentatives de connexion
- détectant les échecs de connexion anormaux

+Avec la MFA, les attaques par force brute deviennent beaucoup plus difficiles.

Ransomware

Scan →Accès →
* Élévation de privilèges →
* Mouvement latéral →
* Déploiement du chiffrement

Les attaquants ciblent d’abord les comptes privilégiés.

Incidents au Maroc :
Marjane
Ministère de l’Éducation
INWI

Avec Axidian Privilege (PAM) :

- Supprimer les droits administrateur permanents
- Appliquer le principe du moindre privilège
- Surveiller l’activité des super-utilisateurs
- Bloquer les commandes sur liste noire
- Enregistrer les sessions
- Faire tourner les identifiants immédiatement après utilisation

Identifiants codés en dur et attaques applicatives

Les attaquants analysent souvent :

- le code source
- les fichiers de configuration
- les scripts de déploiement

à la recherche d'identifiants intégrés.

Avec l'AAPM (Application-to-Application Password Management), les identifiants sont :

- stockés dans un coffre-fort chiffré AES-256
- non visibles dans le code
- automatiquement renouvelés
- injectés de manière sécurisée lorsque nécessaire

Injection SQL et comptes dormants

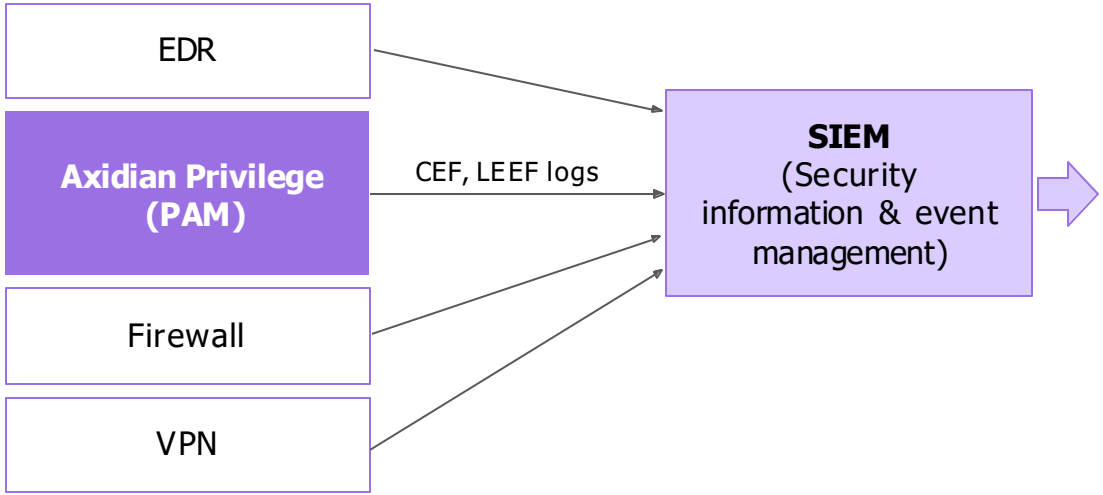
En exploitant des comptes anciens et des failles SQL, les attaquants peuvent :

- extraire des données sensibles
- modifier des enregistrements
- prendre le contrôle des serveurs de bases de données

Axidian Privilege (PAM) réduit ce risque en :

- la découverte automatique des comptes
- l’intégration continue des comptes privilégiés
- l’application du moindre privilège
- la liste blanche des commandes SQL
- le blocage des commandes dangereuses
- les alertes sur les requêtes suspectes

PAM +SIEM pour la détection des anomalies



Détection de :

- horaires d'accès inhabituels
- multiples échecs de connexion
- demandes d'accès rapides et consécutives
- tentatives d'accès à plusieurs systèmes critiques
- extractions excessives de mots de passe

Accélérer les investigations d'incident avec Axidian Privilege

Qui a accédé à quoi et quand	Sur quel système	Quelles commandes ont été exécutées
Enregistrement vidéo des sessions	Journaux texte	Captures d'écran
Copies fantômes des fichiers transférés	Métadonnées utilisateur	

PAM +SIEM +SOAR:

Les alertes déclenchent un confinement automatisé

Les comptes peuvent être verrouillés

Les identifiants sont renouvelés instantanément

PAM pour les entreprises

1. Réduction des risques
2. Facilitateur de conformité
3. Efficacité opérationnelle

Axidian

Privileged Access Management for Business

1. Réduction des risques

- Surface d'attaque réduite
- Accès privilégié contrôlé
- Impact réduit des rançongiciels

2. Conformité

- Contrôles **ISO 27001** (contrôle d'accès, gestion des identités, journalisation et supervision)
- **RGPD**
- Exigences de la législation locale

3. Efficacité opérationnelle

Jusqu'à 50 %des tickets du support concernent les mots de passe

- Rotation auto des mots de passe
- Réduire la charge du support

Prévenir une seule violation majeure peut économiser des millions en temps d'arrêt, amendes, analyses forensiques et atteinte à la réputation.

Département Commercial

WCA

HAFS

Distributeur à valeur ajoutée WCA

Vous accompagne

www.hafs-networks.com
Visitez notre site web

sales-ci@hafs-networks.com
Envoyez-nous un e-mail

(+225) 07 69 32 13 55
Contact commercial 1

(+225) 07 59 05 85 82
Contact commercial 2

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

Hillstone NETWORKS | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY Vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx | SEARCHINFORM RISK AND COMPLIANCE MANAGEMENT | MOBOTIX | EXTRAVIS Analyse Automatisée Réponse XDR | HAFS MediVision