AYI NEDJIMI Consultants

PIM Entra ID : Gestion des Accès Privilégiés Just-in-Time

Catégorie : Microsoft 365 Lecture : 10 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide complet Privileged Identity Management Entra ID : activation just-in-time, approval workflows, access reviews, alertes et réduction de 64% des.

Le risque des Standing Privileges

Dans un environnement traditionnel, les administrateurs disposent de privileges permanents (standing privileges). Un compte Global Administrator est actif 24 heures sur 24, 7 jours sur 7, qu'il soit utilise ou non. Cette approche presente des risques majeurs : Guide complet Privileged Identity Management Entra ID : activation just-in-time, approval workflows, access reviews, alertes et réduction de 64% des. Microsoft 365 est omniprésent en entreprise et sa surface d'attaque ne cesse de s'étendre. La sécurisation de pim entra id acces privilegies nécessite une approche structurée et des outils adaptés. Nous abordons notamment : pim pour les groupes, pim pour les ressources azure et access reviews : campagnes automatisees. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

- **Surface d'attaque elargie** : un compte compromis par phishing ou vol de credentials donne immediatement acces aux privileges les plus eleves.
- **Lateral movement facilite** : les attaquants utilisent les comptes privilegies permanents pour pivoter vers d'autres systemes, comme documente dans les techniques d'escalade de privileges AWS.
- **Absence de tracabilite** : sans activation explicite, il est difficile de distinguer une utilisation legitime d'un abus.
- **Non-conformite reglementaire** : les referentiels ISO 27001 (controle A.8.2) et NIS 2 exigent une gestion stricte des acces privilegies.
- **Drift des permissions** : les droits s'accumulent au fil du temps sans revue systematique, un phenomene appele privilege creep.

Le modele Zero Standing Privileges (ZSP)

PIM implemente le concept de Zero Standing Privileges : aucun utilisateur ne possede de privileges permanents en production. Les acces sont accordes a la demande (just-in-time), pour une duree limitee (time-bound), avec une justification obligatoire et, selon la criticite, une approbation manuelle. Ce modele reduit drastiquement la fenetre d'exposition :

Metrique	Sans PIM	Avec PIM
Duree d'exposition privileges	24/7 (8 760 h/an)	2-4 h/activation
Comptes Global Admin permanents	5-15	2 (break-glass)
Tracabilite des activations	Aucune	100 % audit trail
Incidents privileges (annuel)	Baseline	-64 %
Conformite ISO 27001 A.8.2	Partielle	Complete

Pour les roles moins critiques comme `User Administrator` ou `Helpdesk Administrator`, l'auto-activation sans approbation est acceptable, a condition que le MFA et la justification restent obligatoires. Cela permet aux equipes support d'intervenir rapidement sans attendre une validation manuelle, un principe similaire aux mecanismes d'activation decrits dans la gestion des applications enregistrees Azure AD.

Configuration via PowerShell et Microsoft Graph

Bien que le portail Entra ID offre une interface graphique pour configurer PIM, l'automatisation via Microsoft Graph API est recommandee pour les deployments a grande echelle. Voici un exemple de configuration du role Global Administrator en mode eligible avec approbation :

```
# Connexion a Microsoft Graph avec les permissions PIM
Connect-MgGraph -Scopes
"RoleManagement.ReadWrite.Directory","RoleEligibilitySchedule.ReadWrite.Directory"

# Recuperer l'ID du role Global Administrator
$roleDefinition = Get-MgRoleManagementDirectoryRoleDefinition -Filter "displayName eq
'Global Administrator'"

# Creer une attribution eligible pour un utilisateur
$params = @{
    action = "adminAssign"
    justification = "Attribution eligible PIM - projet securisation Q1 2026"
    roleDefinitionId = $roleDefinition.Id
    directoryScopeId = "/"
    principalId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"  # ObjectId utilisateur
    scheduleInfo = @{
        startDateTime = (Get-Date).ToUniversalTime().ToString("yyyy-MM-ddTHH:mm:ssZ")
        expiration = @{
            type = "afterDuration"
            duration = "P180D"  # 180 jours = 6 mois
        }
    }
}

New-MgRoleManagementDirectoryRoleEligibilityScheduleRequest -BodyParameter $params

# Configurer les parametres du role (activation settings)
$policyParams = @{
    rules = @(
        @{
            "@odata.type" = "#microsoft.graph.unifiedRoleManagementPolicyApprovalRule"
            id = "Approval_EndUser_Assignment"
            target = @{ caller = "EndUser"; operations = @("All"); level = "Assignment" }
            setting = @{
                isApprovalRequired = $true
                approvalStages = @(
                    @{
                        approvalStageTimeOutInDays = 1
                        isApproverJustificationRequired = $true
                        primaryApprovers = @(
                            @{
                                "@odata.type" = "#microsoft.graph.groupMembers"
                                groupId = "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy"  # Groupe
approbateurs
                            }
                        )
                    }
                )
            }
        },
        @{
            "@odata.type" =
"#microsoft.graph.unifiedRoleManagementPolicyAuthenticationContextRule"
            id = "AuthenticationContext_EndUser_Assignment"
            target = @{ caller = "EndUser"; operations = @("All"); level = "Assignment" }
            claimValue = "c1"  # Authentication context pour MFA renforce
            isEnabled = $true
        }
    )
}
```

Roles critiques et classification

Tous les roles Entra ID ne necessitent pas le meme niveau de controle. Classifiez vos roles en trois niveaux de criticite pour adapter les parametres PIM :

Niveau	Roles	Duree max	Approbation	MFA
Critique	Global Admin, Privileged Role Admin, Security Admin	2h	Oui (2 approbateurs)	FIDO2 / Passkey
Eleve	Exchange Admin, SharePoint Admin, Teams Admin, Intune Admin	4h	Oui (1 approbateur)	Authenticator
Standard	User Admin, Helpdesk Admin, License Admin, Reports Reader	8h	Non (self-service)	Authenticator

Avez-vous vérifié les permissions effectives de vos comptes de service Azure AD ?

PIM pour les groupes

Groupes assignables a des roles

Depuis 2024, PIM s'etend aux groupes de securite et aux groupes Microsoft 365 marques comme role-assignable. Cette fonctionnalite permet d'appliquer le modele JIT a l'appartenance aux groupes, ce qui offre des possibilites majeures :

- **Acces conditionnel granulaire** : un utilisateur active son appartenance a un groupe qui lui donne acces a une application specifique via Conditional Access, plutot qu'un role global.
- **Delegation securisee** : les proprietaires de groupes PIM peuvent gerer les membres eligibles de leur groupe sans necessiter le role Privileged Role Administrator.
- **Scenarios multi-tenant** : dans les architectures B2B, PIM pour les groupes permet de gerer l'acces des invites de maniere temporaire et tracee, reduisant les risques documentes dans les attaques sur les Identity Providers.

Configuration PIM pour un groupe

Pour activer PIM sur un groupe, celui-ci doit etre cree avec la propriete `isAssignableToRole = true`. Cette propriete est immutable apres creation. Voici la procedure :

```
# Creer un groupe role-assignable pour PIM
$groupParams = @{
    displayName = "PIM-Eligible-SharePoint-Admins"
    description = "Groupe PIM eligible pour le role SharePoint Administrator"
    mailEnabled = $false
    mailNickname = "pim-sp-admins"
    securityEnabled = $true
    isAssignableToRole = $true  # OBLIGATOIRE pour PIM
    "owners@odata.bind" = @(
        "https://graph.microsoft.com/v1.0/users/$ownerObjectId"
    )
}
New-MgGroup -BodyParameter $groupParams

# Attribuer le role SharePoint Admin a ce groupe (attribution active)
New-MgRoleManagementDirectoryRoleAssignment `
    -RoleDefinitionId $sharepointAdminRoleId `
    -PrincipalId $groupObjectId `
    -DirectoryScopeId "/"

# Les membres du groupe seront ensuite ajoutes en mode eligible via PIM
# L'activation de l'appartenance au groupe = activation du role SharePoint Admin
```

Cas concret
L'exploitation de la fonctionnalité de consentement OAuth dans Azure AD a permis à des attaquants de créer des applications malveillantes obtenant un accès persistant aux données Microsoft 365 des victimes. Cette technique de "consent phishing" contourne le MFA puisque l'utilisateur autorise lui-même l'accès.

PIM pour les ressources Azure

Scopes et hierarchie Azure RBAC

PIM pour les ressources Azure applique le modele JIT aux roles Azure RBAC (Owner, Contributor, Reader, roles custom) a differents niveaux de la hierarchie : Management Group, Subscription, Resource Group, ou Ressource individuelle. Cette granularite permet d'implementer le principe de moindre privilege avec precision :

- **Owner eligible sur une Subscription** : active uniquement pour les operations critiques (modification des policies, suppression de ressources).
- **Contributor eligible sur un Resource Group** : active par les developpeurs pour deployer du code en production.
- **Key Vault Administrator eligible** : active uniquement pour la rotation des secrets, selon les principes decrits dans la gestion des credentials Kerberos en Active Directory.

Discovery et onboarding des ressources

La premiere etape du deployment PIM pour les ressources Azure consiste a effectuer un inventaire (discovery) des attributions RBAC existantes. Le portail PIM affiche automatiquement toutes les souscriptions auxquelles vous avez acces. Pour chaque souscription, vous pouvez visualiser les attributions permanentes actuelles et les convertir en attributions eligibles.

```
// KQL - Identifier toutes les attributions Owner permanentes sur les souscriptions
AzureActivity
| where OperationNameValue == "Microsoft.Authorization/roleAssignments/write"
| where Authorization_d.action == "Microsoft.Authorization/roleAssignments/write"
| extend RoleDefinitionName = tostring(Properties_d.roleDefinitionName)
| where RoleDefinitionName == "Owner"
| summarize Count=count() by Caller, SubscriptionId
| order by Count desc
```

Access Reviews : campagnes automatisees

Principe des Access Reviews

Les Access Reviews (revues d'acces) sont le complement indispensable de PIM. Elles permettent de verifier periodiquement que les attributions eligibles sont toujours justifiees. Sans revue reguliere, les attributions eligibles s'accumulent et recreent progressivement une surface d'attaque elargie.

PIM integre nativement les Access Reviews avec deux modes principaux :

- **Self-review** : l'utilisateur lui-meme confirme ou renonce a son attribution eligible. Ce mode convient pour les roles Standard ou l'utilisateur est le mieux place pour savoir s'il utilise encore le role.
- **Manager review** : le manager hierarchique de l'utilisateur valide ou revoque l'attribution. Ce mode est recommande pour les roles Eleves et Critiques.

- **Group owner review** : pour PIM pour les groupes, le proprietaire du groupe valide les membres eligibles.
- **Designated reviewers** : une equipe specifique (SOC, equipe IAM) revoit l'ensemble des attributions critiques.

Configuration d'une campagne d'Access Review

Creez des campagnes recurrentes pour automatiser le processus de revue. Voici les parametres recommandes par niveau de criticite :

Parametre	Roles Critiques	Roles Eleves	Roles Standard
Frequence	Mensuelle	Trimestrielle	Semestrielle
Reviewers	SOC + Manager	Manager	Self-review
Duree de la revue	7 jours	14 jours	21 jours
Action si pas de reponse	Revoquer	Revoquer	Conserver
Auto-apply results	Oui	Oui	Oui

Decision helper : recommandations basees sur l'activite
Activez l'option **"Decision helpers"** dans les Access Reviews. PIM analysera les journaux d'audit des 30 derniers jours et indiquera aux reviewers si l'utilisateur a effectivement active son role durant cette periode. Un utilisateur qui n'a pas active un role eligible depuis 90 jours est un candidat fort a la revocation.

Monitoring et alertes

Alertes PIM integrees

PIM dispose d'un systeme d'alertes integre qui detecte les configurations a risque et les comportements anormaux. Les alertes les plus importantes a surveiller :

- **Roles being assigned outside of PIM** : detecte les attributions de roles effectuees directement via l'interface IAM sans passer par PIM, ce qui contourne les controles.
- **Too many permanent admins** : alerte lorsque le nombre d'attributions permanentes depasse le seuil configure (recommandation : maximum 5).
- **Roles don't require MFA** : identifie les roles dont la configuration PIM n'exige pas le MFA a l'activation.
- **Admins aren't using their privileged roles** : signale les attributions eligibles non utilisees depuis un nombre configurable de jours.
- **Potential stale accounts with privileged roles** : identifie les comptes qui n'ont pas change leur mot de passe depuis une periode prolongee.

Requetes KQL pour Microsoft Sentinel

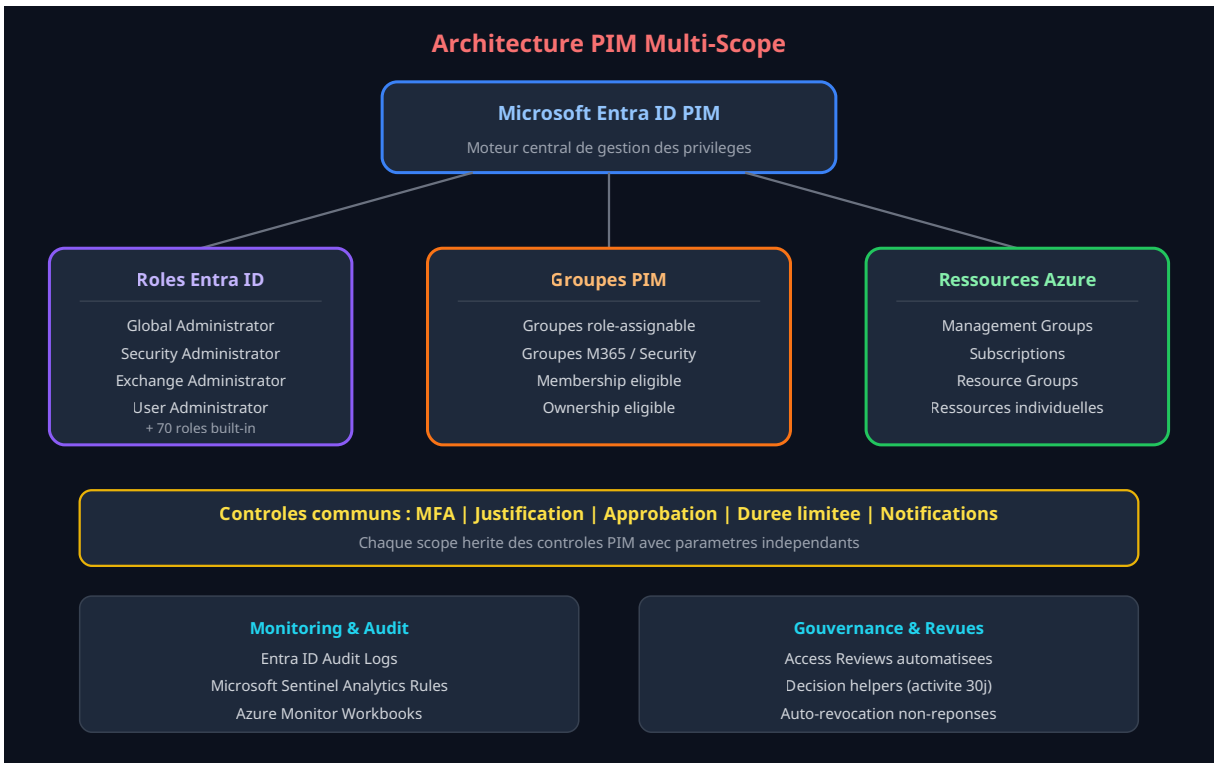
L'integration PIM avec Microsoft Sentinel permet de creer des regles analytiques avancees. Voici les requetes KQL essentielles pour le monitoring PIM :

```
// 1. Activations PIM en dehors des heures ouvrees (potentiel indicateur de compromission)
AuditLogs
| where OperationName == "Add member to role completed (PIM activation)"
| where TimeGenerated !between (datetime(06:00) .. datetime(20:00))
| extend ActivatedBy = tostring(InitiatedBy.user.userPrincipalName)
| extend RoleName = tostring(TargetResources[0].displayName)
| project TimeGenerated, ActivatedBy, RoleName, Result
| order by TimeGenerated desc

// 2. Activations refusees (tentatives suspectes)
AuditLogs
| where OperationName == "Add member to role request denied (PIM activation)"
| extend RequestedBy = tostring(InitiatedBy.user.userPrincipalName)
| extend RoleName = tostring(TargetResources[0].displayName)
| summarize DeniedCount=count() by RequestedBy, RoleName
| where DeniedCount > 3
| order by DeniedCount desc

// 3. Attributions permanentes hors PIM (contournement des controles)
AuditLogs
| where OperationName has "Add member to role"
| where OperationName !has "PIM"
| extend AddedBy = tostring(InitiatedBy.user.userPrincipalName)
| extend TargetUser = tostring(TargetResources[0].userPrincipalName)
| extend RoleName =
tostring(parse_json(tostring(TargetResources[0].modifiedProperties[1])).newValue)
| project TimeGenerated, AddedBy, TargetUser, RoleName

// 4. Volume d'activations par role (baseline comportementale)
AuditLogs
| where OperationName == "Add member to role completed (PIM activation)"
| extend RoleName = tostring(TargetResources[0].displayName)
| summarize ActivationCount=count() by RoleName, bin(TimeGenerated, 1d)
| render timechart
```

Workbooks Azure Monitor

Microsoft fournit un workbook PIM preconfigure dans Azure Monitor qui offre une vue consolidee des metriques cles : nombre d'activations par jour, ratio eligible/permanent, activations en attente d'approbation, et tendances sur 30/60/90 jours. Personnalisez ce workbook en ajoutant :

- Un widget montrant les activations par localisation geographique (detecte les activations depuis des pays inhabituels).
- Un graphique de correlation entre les activations PIM et les alertes Microsoft Defender for Identity.
- Un tableau des comptes eligibles n'ayant pas active leur role depuis plus de 60 jours.
- Un indicateur du nombre de comptes break-glass et la date de leur dernier test.



Bonnes pratiques et comptes break-glass

Les comptes break-glass : la securite de dernier recours

Les comptes break-glass (ou emergency access accounts) sont des comptes Global Administrator avec des attributions permanentes, exclus de PIM, des politiques Conditional Access et du MFA. Ils constituent le dernier recours en cas de panne majeure du systeme d'authentification (panne MFA, blocage PIM, compromission des comptes d'approbation).

Configuration obligatoire des comptes break-glass

- Creer exactement **2 comptes break-glass** (redundance).
- Utiliser des noms de compte non previsibles (pas admin-emergency, pas breakglass@).
- Pas d'association a une personne physique individuelle.
- Mots de passe de 25+ caracteres, stockes dans un coffre-fort physique (pas dans un gestionnaire de mots de passe numerique).
- Exclure de toutes les politiques Conditional Access (verifier avec le mode "What If").
- Creer une alerte Sentinel sur toute connexion reussie avec ces comptes.
- Tester les comptes break-glass chaque trimestre et documenter les tests.
- Le mot de passe ne doit jamais expirer (politique specifique).

```
// Alerte Sentinel : connexion reussie avec un compte break-glass
SigninLogs
| where UserPrincipalName in ("breakglass1@contoso.onmicrosoft.com",
"breakglass2@contoso.onmicrosoft.com")
| where ResultType == 0  // Connexion reussie
| project TimeGenerated, UserPrincipalName, IPAddress, Location, AppDisplayName,
DeviceDetail
// Severite : HAUTE - Declencher une notification immediate au RSSI
```

Checklist de deploiement PIM

Suivez cette checklist exhaustive pour un deploiement PIM reussi :

- **Phase 1 - Preparation** : inventorier tous les comptes privilegies permanents, classifier les roles par criticite, creer les comptes break-glass, valider les licences Entra ID P2.
- **Phase 2 - Configuration** : configurer les parametres PIM par role (activation, attribution, notification), definir les approbateurs, integrer avec l'ITSM, configurer les Conditional Access Policies associees.
- **Phase 3 - Migration** : convertir les attributions permanentes en attributions eligibles en commencant par les roles Standard, puis Eleves, puis Critiques. Communiquer proactivement avec les utilisateurs impactes.
- **Phase 4 - Access Reviews** : creer les campagnes recurrentes, configurer les decision helpers, definir les actions par defaut en cas de non-reponse.
- **Phase 5 - Monitoring** : deployer les requetes KQL dans Sentinel, creer les workbooks de suivi, configurer les alertes PIM integrees, tester les comptes break-glass.
- **Phase 6 - Amelioration continue** : revoir trimestriellement les metriques PIM, ajuster les durees d'activation selon l'usage reel, etendre PIM aux ressources Azure et aux groupes.

Integration avec le Zero Trust

PIM s'integre dans une architecture Zero Trust en tant que composant central du pilier **Identity**. Combinez PIM avec :

- **Conditional Access** : creez des politiques qui exigent un appareil conforme (Intune) et une localisation reseau connue pour les activations de roles critiques.
- **Continuous Access Evaluation (CAE)** : revoque les tokens en quasi-temps reel si les conditions changent pendant une session PIM active.
- **Microsoft Defender for Identity** : correle les activations PIM avec les alertes de comportement suspect dans Active Directory on-premises.
- **Entra ID Protection** : bloque les activations PIM si le risque utilisateur est eleve (sign-in risk ou user risk).

Questions frequentes

Comment mettre en place PIM Entra ID dans un environnement de production ?

La mise en place de PIM Entra ID en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Pourquoi PIM Entra ID est-il essentiel pour la securite des systemes d'information ?

PIM Entra ID constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

Comment auditer la configuration de sécurité de PIM Entra ID : Gestion des Accès Privilégiés Just-in-Time ?

Utilisez Microsoft Secure Score comme point de départ, puis complétez avec un audit CIS Benchmark pour Microsoft 365. Exportez la configuration via PowerShell pour une revue hors ligne.

Pour approfondir ce sujet, consultez notre outil open-source exchange-security-checker qui facilite la vérification de la sécurité Exchange Online.

> Points clés à retenir
>
> - PIM pour les groupes
> - PIM pour les ressources Azure
> - Access Reviews : campagnes automatisees
> - Monitoring et alertes
> - Bonnes pratiques et comptes break-glass
> - Questions frequentes

Conclusion

Privileged Identity Management dans Entra ID transforme fondamentalement la gestion des acces privilegies en remplacant le modele statique des permissions permanentes par un modele dynamique just-in-time. Les benefices sont quantifiables : reduction de 64 % des incidents lies aux comptes privilegies, conformite facilitee avec ISO 27001 et NIS 2, et tracabilite complete de chaque elevation de privilege.

La cle du succes reside dans une approche progressive : commencez par les roles les plus critiques (Global Administrator), etendez ensuite aux roles administratifs courants, puis deployez PIM pour les groupes et les ressources Azure. Combinez systematiquement PIM avec des Access Reviews automatisees pour eviter l'accumulation de privileges inutiles au fil du temps.

N'oubliez pas les comptes break-glass : ils constituent votre filet de securite en cas de defaillance du systeme PIM lui-meme. Testez-les regulierement, surveillez-les en permanence, et documentez leur procedure d'utilisation dans votre plan de continuite.

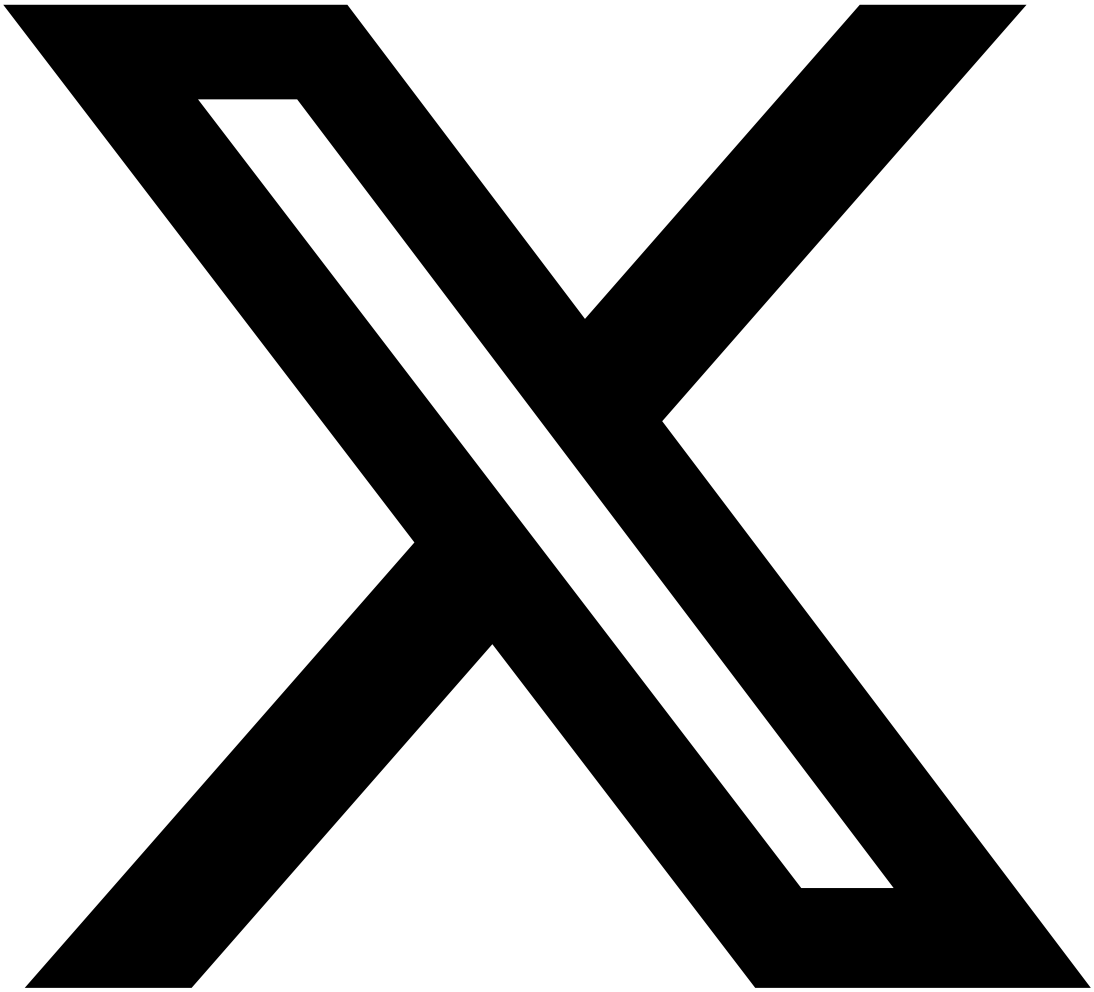
En combinant PIM avec Conditional Access, Continuous Access Evaluation et Microsoft Defender for Identity, vous construisez une architecture Zero Trust robuste ou chaque privilege est justifie, approuve, limite dans le temps et audite. C'est la fondation d'une posture de securite mature face aux menaces actuelles.

Sources et références : Microsoft Security Docs · CERT-FR

Articles complementaires

Microsoft 365
Applications enregistrees Azure AD
Securisation des app registrations et service principals
Cloud Security
Escalades de privileges AWS
Techniques d'elevation de privileges dans AWS IAM
Identity Security
Attaques Identity Providers
Okta, Entra, Keycloak : vecteurs d'attaque et defenses
Active Directory
Kerberos Exploitation AD
Attaques Kerberos et defenses dans Active Directory
Conformite
NIS 2 Directive Europeenne
Exigences NIS 2 pour la gestion des acces privilegies
Conformite
ISO 27001 Guide Complet
Controles d'acces et gestion des identites ISO 27001

Partagez cet article

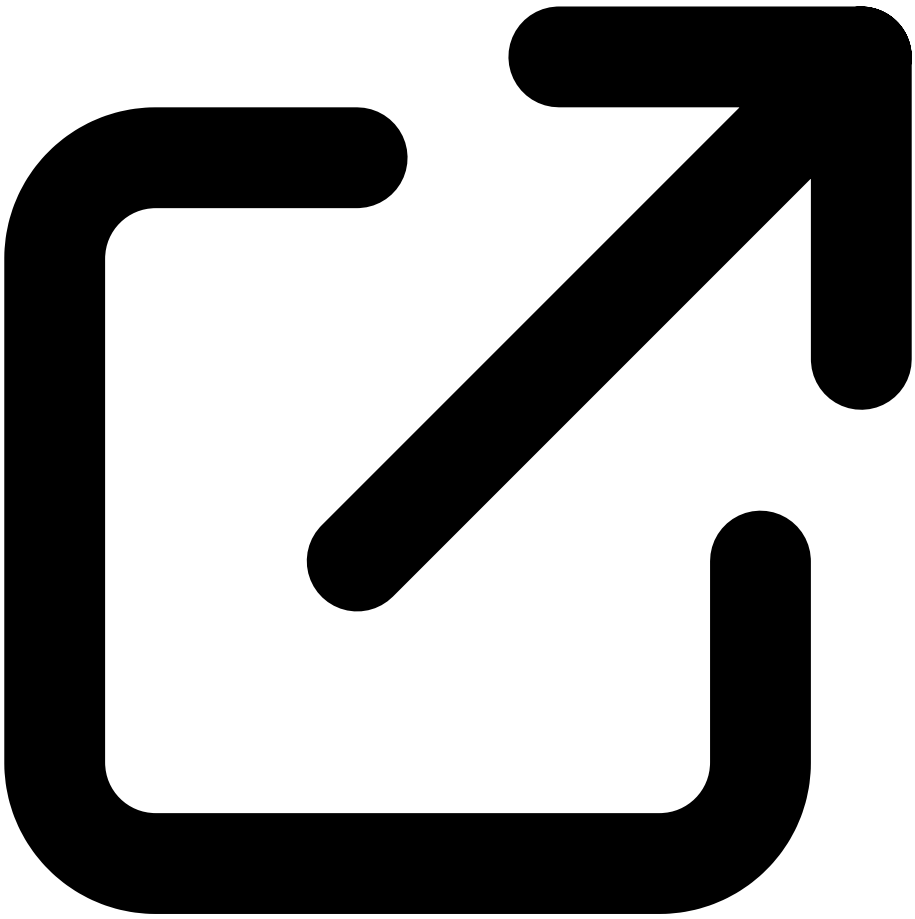


Partager sur X

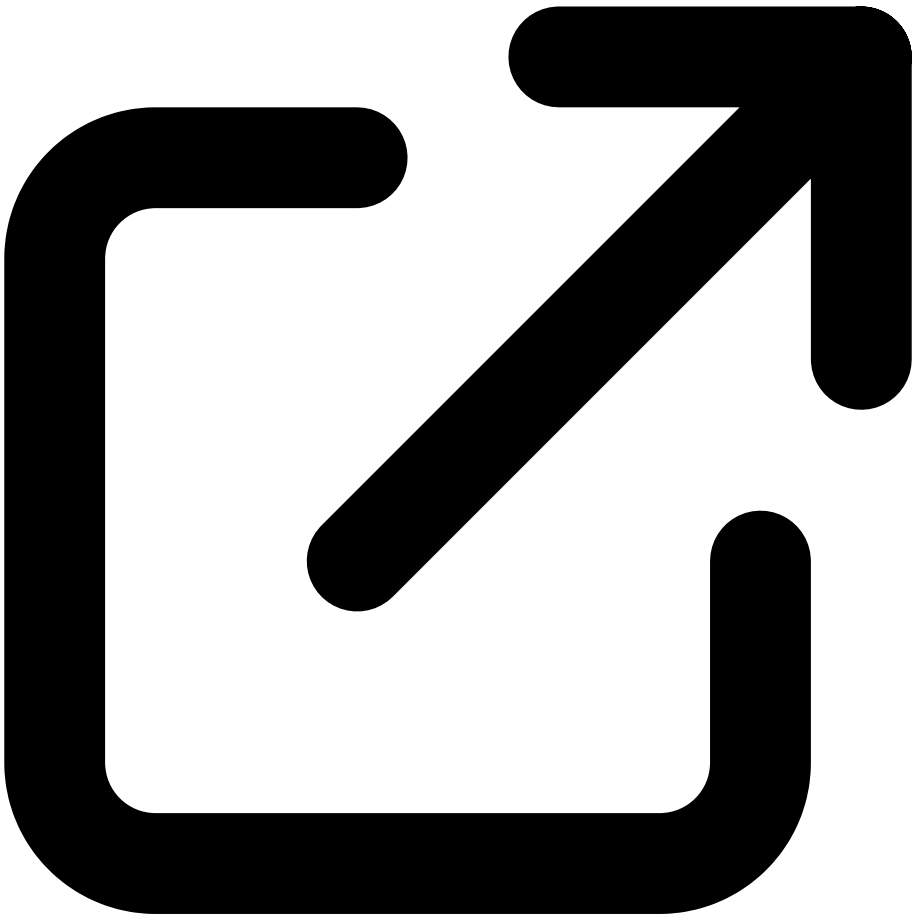
Partager sur LinkedIn

Ressources & References Officielles

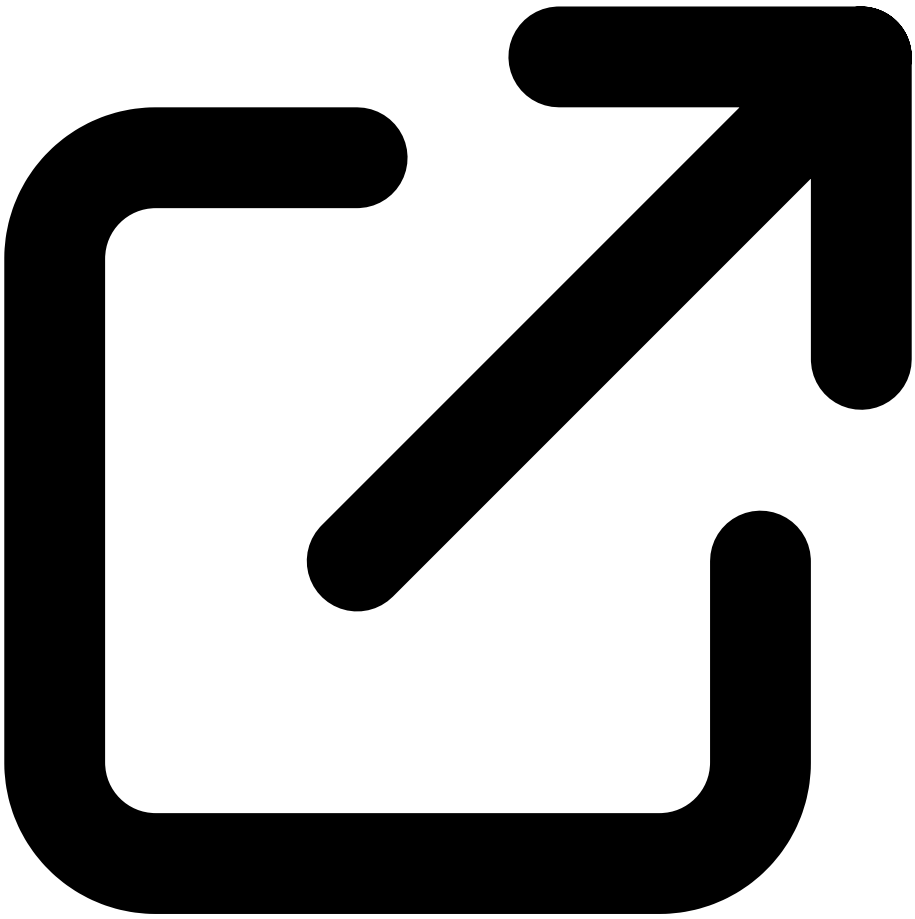
Documentations officielles Microsoft et ressources de la communaute



Microsoft - PIM Documentation
learn.microsoft.com



Microsoft - Access Reviews Overview
learn.microsoft.com



Microsoft - Emergency Access Accounts
learn.microsoft.com

Ayi NEDJIMI

Expert en Cybersécurité & Intelligence Artificielle

Consultant senior avec plus de 15 ans d'experience en securite offensive, audit d'infrastructure et developpement de solutions IA. Certifie OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer. Intervient sur des missions de pentest Active Directory, securite Cloud et conformite reglementaire pour des grands comptes et ETI.

LinkedIn Profil complet Tous ses articles

References et ressources externes

- Microsoft Entra PIM Documentation -- Guide officiel Privileged Identity Management
- MITRE ATT&CK T1078 -- Valid Accounts : techniques d'abus de comptes privilegies
- CIS Controls -- Center for Internet Security : controles de gestion des acces
- NIST SP 800-53 -- Security and Privacy Controls for Information Systems

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr