Checklist Sécurité MICROSOFT 365

Ayi NEDJIMI Consultants
ayinedjimi-consultants.fr
v4.6 — 2026-03-26 · 253 controles

Sommaire

Section 1 — GESTION DES IDENTITÉS ET DES ACCÈS

1.1 — Authentification Multi-Facteurs (MFA)

1.1.1 *Activer MFA pour tous les comptes Administrateurs* — Critique

MITRE ATT&CK : T1078.004 (Valid Accounts: Cloud) · T1556.006 (Modify Authentication: MFA) · T1621 (MFA Request Generation)

DESCRIPTION :

L'authentification multi-facteurs (MFA) est la mesure de sécurité la plus efficace pour protéger les comptes administrateurs contre les compromissions. Sans MFA, un mot de passe volé suffit à compromettre l'intégralité du tenant M365. Les comptes administrateurs disposant de privilèges élevés sont les cibles prioritaires des attaquants.

AUDIT :

- Accéder à : Entra ID > Protection > Authentification multifacteur > Paramètres
- Ou via PowerShell :

```
Get-MgUser -Filter "assignedLicenses/$count ne 0" | Get-MgUserAuthenticationMethod
```

AUDIT :

- Vérifier que 100% des comptes avec rôles admin ont MFA activé
- Vérifier dans les rapports de connexion qu'aucune connexion admin ne s'est faite sans MFA

REMÉDIATION :

1. Activer les **Paramètres de sécurité par défaut** (Security Defaults) si l'organisation n'utilise pas l'Accès Conditionnel
2. Ou créer une **Politique d'Accès Conditionnel** : Utilisateurs → Tous les utilisateurs avec rôles admin → Accorder → Exiger MFA
3. Enrôler tous les administrateurs dans MFA via : https://aka.ms/mfasetup
4. Méthodes recommandées par ordre de préférence : Application Authenticator > Clé FIDO2 > SMS (déconseillé)

   Impact si non conforme : Compromission totale du tenant en cas de phishing ou fuite de mot de passe administrateur.

1.1.2 *Activer MFA pour tous les utilisateurs* — Élevé

MITRE ATT&CK : T1078 (Valid Accounts) · T1586.003 (Compromise Accounts: Cloud) · T1199 (Trusted Relationship)

DESCRIPTION :

Tous les utilisateurs, pas uniquement les administrateurs, doivent utiliser le MFA. Un compte utilisateur standard compromis peut servir de pivot pour des attaques de latéralisation, l'exfiltration de données ou des attaques BEC (Business Email Compromise).

AUDIT :

- Entra ID > Protection > Authentification multifacteur > Rapport d'activité
- Vérifier le pourcentage d'utilisateurs enrôlés dans MFA
- PowerShell :

```
Get-MgReportAuthenticationMethodUserRegistrationDetail | Where-Object {$_.IsMfaRegistered -eq $false}
```

REMÉDIATION :

1. Déployer une Politique d'Accès Conditionnel ciblant tous les utilisateurs
2. Utiliser la fonctionnalité **Campagne d'enrôlement MFA** dans Entra ID pour guider les utilisateurs
3. Définir un délai de grâce raisonnable (14 jours maximum)
4. Former les utilisateurs via Microsoft Learn ou sessions internes

1.1.3 *Désactiver MFA via SMS comme méthode principale* — Moyen

DESCRIPTION :

Le SMS est vulnérable aux attaques de SIM swapping et d'interception SS7. Bien qu'il soit préférable à l'absence de MFA, il ne doit pas être la méthode principale recommandée par l'organisation.

AUDIT :

- Entra ID > Protection > Méthodes d'authentification > Stratégies
- Vérifier si le SMS est activé et quelle est sa priorité

REMÉDIATION :

1. Dans Entra ID > Méthodes d'authentification, favoriser Microsoft Authenticator avec **Number Matching** et **Additional Context**
2. Désactiver ou déprioriser le SMS pour les comptes sensibles
3. Activer les clés FIDO2 pour les environnements à haute sécurité
4. Activer la résistance au phishing : Paramètres > Number Matching = Activé

1.1.4 *Exiger une MFA Résistante au Phishing pour les Rôles Privilégiés* Critique

DESCRIPTION :
Les méthodes MFA classiques (notification push, TOTP) restent vulnérables aux attaques de type AiTM (Adversary-in-the-Middle) et phishing en temps réel (Evilginx2, Modlishka). Les méthodes résistantes au phishing — FIDO2/clés de sécurité physiques (YubiKey, etc.), Windows Hello for Business, ou certificats client — sont liées cryptographiquement au domaine légitime et ne peuvent pas être relayées par un proxy d'attaque.

AUDIT :
- Entra ID > Protection > Accès Conditionnel > Vérifier l'existence d'une politique exigeant une MFA résistante au phishing pour les rôles admin
- PowerShell :

```
Get-MgIdentityConditionalAccessPolicy | Where-Object {$_.DisplayName -like "*phishing*" -or $_.DisplayName -like "*FIDO*"} | Select
```

REMÉDIATION :
1. Créer une politique CA : Utilisateurs → Rôles d'annuaire (sélectionner tous les rôles admin)
2. Accorder → Exiger la force d'authentification → Créer une force d'authentification personnalisée avec : FIDO2 Security Key, Windows Hello for Business, Certificate-based Authentication (hardware)
3. Enrôler tous les administrateurs dans au moins une méthode résistante au phishing
4. Pour les environnements très sensibles : étendre aux utilisateurs à accès privilégié (RH, Finance, Direction)
   Impact si non conforme : Les campagnes AiTM (type EvilProxy, Evilginx) peuvent intercepter les tokens MFA push en temps réel.

1.1.5 *Désactiver SMS, Appel Vocal et Email OTP comme méthodes MFA* Critique

DESCRIPTION :
Le SMS, l'appel vocal et l'Email OTP sont explicitement déconseillés par le NIST SP 800-63B pour l'authentification des systèmes gouvernementaux et d'entreprise. Ces méthodes sont vulnérables au SIM swapping, à l'interception SS7, au vishing, et au forwarding de messages. La CISA impose leur désactivation dans les organisations fédérales américaines (BOD 25-01).

AUDIT :
- Entra ID > Protection > Méthodes d'authentification > Stratégies
- Vérifier le statut de "SMS", "Voice Call", "Email OTP"
- PowerShell :

```
Get-MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration -AuthenticationMethodConfigurationId "Sms" | Select-Object
Get-MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration -AuthenticationMethodConfigurationId "Voice" | Select-Objec
```

REMÉDIATION :
1. Entra ID > Protection > Méthodes d'authentification > Stratégies
2. Désactiver "SMS" (état : Désactivé)
3. Désactiver "Voice Call" (état : Désactivé)
4. Désactiver "Email OTP" (état : Désactivé)
5. Avant désactivation : s'assurer que 100% des utilisateurs ont une méthode alternative (Authenticator App ou FIDO2)
6. Utiliser la fonctionnalité de campagne d'enrôlement MFA pour migrer les utilisateurs

1.1.6 *Activer Number Matching pour Microsoft Authenticator* Élevé

DESCRIPTION :
Le Number Matching prévient les attaques de type MFA Fatigue (MFA Bombing) où un attaquant envoie des notifications push répétées jusqu'à ce que l'utilisateur accepte par erreur ou fatigue. Avec Number Matching, l'utilisateur doit saisir un code affiché sur l'écran de connexion.

AUDIT :
- Entra ID > Protection > Méthodes d'authentification > Microsoft Authenticator > Configurer
- Vérifier que "Correspondance de nombre" = Activé

REMÉDIATION :
1. Entra ID > Protection > Méthodes d'authentification > Microsoft Authenticator
2. Cliquer sur "Configurer"
3. Activer "Correspondance de nombre" pour tous les utilisateurs
4. Activer également "Contexte supplémentaire" (affiche l'application et la localisation)

1.1.7 *Finaliser la migration des méthodes d'authentification (Authentication Methods Migration)* Élevé

DESCRIPTION :
Microsoft dispose de deux systèmes de gestion des méthodes d'authentification : l'ancien (hérité, dans les paramètres MFA legacy) et le nouveau (Authentication Methods Policy dans Entra ID). Tant que la migration n'est pas complète, des politiques contradictoires peuvent coexister, créant des lacunes de sécurité et des configurations inattendues.

AUDIT :
- Entra ID > Protection > Méthodes d'authentification > Stratégies > Migration
- Vérifier que l'état est "Migration terminée" et non "En cours" ou "Non commencée"

REMÉDIATION :
1. Entra ID > Protection > Méthodes d'authentification > Gérer la migration
2. Auditer les méthodes activées dans l'ancienne console MFA
3. Reconfigurer de manière équivalente dans la nouvelle console Authentication Methods
4. Cliquer sur "Terminer la migration" une fois la configuration validée
5. Après migration : toute gestion se fait exclusivement via Authentication Methods Policy

1.1.8 *Bloquer l'authentification héritée (Legacy Authentication)* — Critique

DESCRIPTION :
Les protocoles d'authentification héritée (SMTP AUTH, POP3, IMAP, MAPI basique, EWS Basic Auth) ne supportent pas le MFA. Ils représentent un vecteur d'attaque majeur car ils permettent de bypasser entièrement le MFA via des attaques par force brute ou password spray.

AUDIT :

- Entra ID > Connexions > Filtrer par "Application cliente" → protocoles hérités
- PowerShell :

```
Get-MgAuditLogSignIn -Filter "clientAppUsed eq 'SMTP Auth' or clientAppUsed eq 'POP3' or clientAppUsed eq 'IMAP4'" | Select-Object
```

AUDIT :

- Vérifier les 30 derniers jours d'activité

REMÉDIATION :

1. Créer une Politique d'Accès Conditionnel : Bloquer les authentifications héritées
2. Utilisateurs : Tous
3. Applications cloud : Toutes
4. Conditions > Applications clientes : cocher "Autres clients"
5. Accorder : Bloquer l'accès
6. Avant le blocage, identifier les applications utilisant encore ces protocoles
7. Migrer les applications vers les protocoles modernes (OAuth 2.0, MSAL)
8. Dans Exchange : Désactiver SMTP AUTH au niveau tenant sauf exceptions justifiées

1.2 — Paramètres M365 Admin Center (Org Settings)

1.2.1 *Utiliser des licences à empreinte applicative réduite pour les comptes admin* — Élevé

Profile : E3 Level 1

DESCRIPTION :
Les comptes administrateurs dédiés ne doivent pas disposer de licences M365 complètes incluant Teams, Exchange, SharePoint, etc. Une licence complète augmente inutilement la surface d'attaque : si un compte admin est compromis, l'attaquant hérite de toutes les capacités de la licence. La recommandation CIS est d'utiliser des licences minimales (ex: Azure AD P2 seule) pour les comptes admin purs.

```
# Lister les comptes admin et leurs licences
$adminRoles = Get-MgDirectoryRole -Filter "DisplayName eq 'Global Administrator'"
$adminMembers = Get-MgDirectoryRoleMember -DirectoryRoleId $adminRoles.Id
foreach ($admin in $adminMembers) {
    $user = Get-MgUser -UserId $admin.Id -Property DisplayName,AssignedLicenses,UserPrincipalName
    Write-Output "$($user.UserPrincipalName): $($user.AssignedLicenses.SkuId -join ', ')"
}
```

AUDIT :
Vérifier qu'aucun compte admin dédié ne possède de licence incluant Exchange Online, Teams, SharePoint, OneDrive, etc.

REMÉDIATION :

1. Pour chaque compte admin dédié, retirer les licences M365 complètes
2. Assigner uniquement les licences nécessaires pour les fonctions admin (ex: Microsoft Entra ID P2, Microsoft 365 E3 sans Exchange/Teams si besoin de conformité)
3. Les admins utilisent leurs comptes utilisateur standards pour accéder à Teams, email, etc.
4. Vérifier que les comptes admin n'ont pas de boîte mail activée

VALEUR PAR DÉFAUT :
Aucune restriction — les comptes admin peuvent avoir n'importe quelle licence.

1.2.2 *Bloquer la connexion aux boîtes mail partagées (Shared Mailboxes)* — Élevé

Profile : E3 Level 1

DESCRIPTION :
Les boîtes mail partagées sont conçues pour être accédées via délégation, pas par connexion directe. Un compte de boîte mail partagée avec connexion activée peut être utilisé par un attaquant comme point d'entrée : ces comptes ont souvent des mots de passe anciens, ne sont pas soumis au MFA standard, et passent sous le radar des revues d'accès.

```
# Identifier les shared mailboxes avec connexion non bloquée
Get-Mailbox -RecipientTypeDetails SharedMailbox -ResultSize Unlimited |
    ForEach-Object {
        $mbx = $_
        $user = Get-MgUser -UserId $mbx.ExternalDirectoryObjectId -Property AccountEnabled,UserPrincipalName -ErrorAction SilentlyC
        if ($user.AccountEnabled -eq $true) {
            Write-Output "ATTENTION - Connexion active : $($user.UserPrincipalName)"
        }
    }
```

```
# Bloquer la connexion sur toutes les shared mailboxes (Microsoft Graph)
Get-Mailbox -RecipientTypeDetails SharedMailbox -ResultSize Unlimited | ForEach-Object {
    Update-MgUser -UserId $_.ExternalDirectoryObjectId -AccountEnabled:$false
}
```

REMÉDIATION :
Les boîtes mail partagées restent accessibles via délégation depuis les comptes utilisateur autorisés.

VALEUR PAR DÉFAUT :
Connexion activée par défaut sur les comptes de boîtes partagées.

1.2.3 *Restreindre les groupes publics aux groupes approuvés par l'organisation* — Moyen

Profile : E3 Level 2

DESCRIPTION :

Les groupes M365 publics (Microsoft 365 Groups avec accès public) permettent à n'importe quel utilisateur de l'organisation de rejoindre le groupe et d'accéder à son contenu (Teams, SharePoint, emails du groupe). Sans gouvernance, des données sensibles peuvent être stockées dans des groupes publics accessibles à tous.

```
# Lister les groupes publics non approuvés
Get-MgGroup -Filter "groupTypes/any(g:g eq 'Unified') and visibility eq 'Public'" |
    Select-Object DisplayName, Id, Visibility |
    Sort-Object DisplayName
```

REMÉDIATION :

1. M365 Admin Center > Équipes et groupes > Groupes actifs
2. Pour chaque groupe public non justifié : changer la visibilité en "Privé"
3. Créer une politique de nommage et de gouvernance pour les nouveaux groupes
4. PowerShell pour convertir en privé :

```
Update-MgGroup -GroupId <GroupId> -Visibility "Private"
```

REMÉDIATION :

1. Activer l'approbation d'un administrateur pour la création de nouveaux groupes publics

VALEUR PAR DÉFAUT :

La visibilité du groupe est définie lors de la création, par défaut souvent "Public".

1.2.4 *Configurer le délai d'expiration de session pour les appareils non gérés (≤ 3 heures)* — Élevé

Profile : E3 Level 2

DESCRIPTION :

Sans délai d'expiration de session, une session M365 reste active indéfiniment sur un appareil non géré (ordinateur partagé, cybercafé, appareil personnel). Un attaquant ayant un accès physique temporaire à l'appareil peut réutiliser la session. La CIS recommande 3 heures maximum pour les appareils non gérés.

AUDIT :

- M365 Admin Center > Paramètres > Org Settings > Sécurité et confidentialité > Délai d'expiration de session inactive
- PowerShell :

```
# Via SharePoint (contrôle le délai pour OWA/M365 web sur appareils non gérés)
Get-SPOTenant | Select-Object SignInAccelerationDomain, IdleSessionSignOut, IdleSessionSignOutWarnMinutes, IdleSessionSignOutMinute
```

REMÉDIATION :

1. M365 Admin Center > Paramètres > Org Settings > Sécurité et confidentialité
2. Activer "Délai d'expiration de session inactive pour les utilisateurs non actifs dans les applications web Microsoft 365"
3. Délai d'inactivité : 3 heures (ou moins selon la politique interne)
4. Avertissement avant déconnexion : 5 minutes
5. Via PowerShell SharePoint :

```
Set-SPOTenant -IdleSessionSignOut $true -IdleSessionSignOutWarnMinutes 5 -IdleSessionSignOutMinutes 180
```

VALEUR PAR DÉFAUT :

Pas de délai d'expiration configuré par défaut.

> **Note :** Les contrôles CIS 1.3.4 à 1.3.9 (Office Store, Forms, Customer Lockbox, Stockage tiers, Sway, Bookings) sont couverts en Section 12 — Gestion Administrative (contrôles 12.1.6 à 12.1.11).

1.2b — Politiques de Mots de Passe

1.3 — Accès Conditionnel (Conditional Access)

1.3.1 *Activer les Paramètres de Sécurité par Défaut ou l'Accès Conditionnel* — Critique

MITRE ATT&CK : T1078.004 (Valid Accounts: Cloud) · T1550.001 (Application Access Token) · T1110 (Brute Force)

DESCRIPTION :

Les Security Defaults fournissent un niveau de sécurité minimal sans configuration. Pour les organisations plus matures, l'Accès Conditionnel offre une granularité plus fine. L'un ou l'autre DOIT être activé. Un tenant sans l'un ni l'autre est extrêmement vulnérable.

AUDIT :

- Entra ID > Vue d'ensemble > Paramètres de sécurité par défaut (Security Defaults)
- OU Entra ID > Protection > Accès Conditionnel > Politiques

REMÉDIATION :

1. Si organisation < 50 utilisateurs sans équipe IT : activer Security Defaults
2. Si organisation avec besoins spécifiques : désactiver Security Defaults et créer des politiques CA granulaires
3. Ne jamais avoir les deux désactivés simultanément

1.3.2 *Politique CA : Exiger un appareil conforme ou hybride Azure AD* — Élevé

DESCRIPTION :
Restreindre l'accès aux ressources M365 aux seuls appareils conformes (gérés par Intune avec politiques de conformité validées) ou hybrides Azure AD réduit considérablement la surface d'attaque et empêche l'accès depuis des appareils personnels non sécurisés.

AUDIT :
- Accès Conditionnel > Politiques
- Vérifier l'existence d'une politique vérifiant la conformité des appareils

REMÉDIATION :
1. Créer politique CA : Utilisateurs → Tous, Ressources → Toutes apps cloud
2. Conditions > Plateformes d'appareils → Sélectionner plateformes concernées
3. Accorder → Exiger que l'appareil soit marqué comme conforme
4. Prérequis : Déployer Intune et définir des politiques de conformité

1.3.3 *Politique CA : Bloquer les pays à risque* — Élevé

DESCRIPTION :
Bloquer les connexions provenant de pays où l'organisation n'a pas d'activité réduit significativement la surface d'attaque pour les campagnes de phishing et de password spray souvent initiées depuis des pays spécifiques.

AUDIT :
- Accès Conditionnel > Emplacements nommés > Vérifier les politiques de blocage géographique

REMÉDIATION :
1. Entra ID > Protection > Accès Conditionnel > Emplacements nommés
2. Créer un emplacement "Pays autorisés" avec les pays légitimes
3. Créer politique CA : Conditions > Emplacements → Exclure les pays autorisés → Bloquer

1.3.4 *Politique CA : Protéger l'accès à Azure/Entra ID Management* — Critique

DESCRIPTION :
L'accès au portail Azure et aux APIs de gestion doit être restreint aux seuls utilisateurs légitimes depuis des postes de travail d'administration dédiés (PAW - Privileged Access Workstations).

AUDIT :
- Vérifier l'existence d'une politique CA ciblant "Microsoft Azure Management"
- Vérifier les conditions restrictives appliquées

REMÉDIATION :
1. Créer politique CA ciblant l'application "Microsoft Azure Management"
2. Restreindre aux administrateurs uniquement
3. Exiger MFA renforcé (FIDO2 ou Windows Hello for Business)
4. Optionnel : Restreindre aux PAW (appareils spécifiques via filtres d'appareils)

1.3.5 *Politique CA : Fréquence de reconnexion et sessions persistantes* — Moyen

DESCRIPTION :
Les sessions persistantes sur des appareils non gérés représentent un risque si l'appareil est compromis ou partagé. Définir une fréquence de reconnexion limite la durée d'exposition en cas de vol de session.

AUDIT :
- Politiques CA > Sessions > Vérifier les paramètres de fréquence de connexion

REMÉDIATION :
1. Pour appareils non conformes : fréquence de connexion = 1 heure
2. Pour appareils conformes : fréquence de connexion = 8 heures ou persistante
3. Désactiver "Rester connecté" pour les appareils non gérés
4. Politique CA : Conditions > Appareils non conformes → Session → Fréquence de connexion : 1h

1.3.6 *Bloquer le flux Device Code (Device Code Flow) — Storm-2372* Critique

Licence requise : Entra ID P1

DESCRIPTION :

Le Device Code Flow (`deviceCodeFlow`) est une méthode d'authentification OAuth conçue pour les appareils sans navigateur (TV, imprimantes). En 2025, le groupe d'attaquants **Storm-2372** (étatique) a massivement exploité ce flux pour du phishing : l'attaquant demande un code appareil, l'envoie à la victime par email/Teams, la victime entre le code sur un site légitime Microsoft et l'attaquant obtient un token d'accès complet sans jamais avoir besoin du mot de passe. Ce flux doit être bloqué par une politique CA.

```
# Vérifier si une politique CA bloque le Device Code Flow
$caPolicies = Get-MgIdentityConditionalAccessPolicy -All | Where-Object { $_.State -eq "enabled" }
$deviceCodePolicy = $caPolicies | Where-Object {
    $_.Conditions.AuthenticationFlows -ne $null -and
    $_.Conditions.AuthenticationFlows.TransferMethods -contains "deviceCodeFlow"
}
if ($deviceCodePolicy) {
    Write-Host "✅ Device Code Flow bloqué par la politique : $($deviceCodePolicy.DisplayName)" -ForegroundColor Green
} else {
    Write-Host "❌ CRITIQUE : Aucune politique CA ne bloque le Device Code Flow (Storm-2372 vector)" -ForegroundColor Red
}
```

REMÉDIATION :

1. Entra ID > Sécurité > Accès conditionnel > Nouvelle politique
2. Nom : "ANC-CA-Block-DeviceCodeFlow"
3. Utilisateurs : Tous les utilisateurs
4. Conditions > Flux d'authentification > Device Code Flow = Inclure
5. Contrôles d'accès > Accorder > Bloquer l'accès
6. État : Activé

```
# PowerShell via Graph
$params = @{
    displayName = "ANC-CA-Block-DeviceCodeFlow"
    state = "enabled"
    conditions = @{
        users = @{ includeUsers = @("All") }
        authenticationFlows = @{ transferMethods = "deviceCodeFlow" }
    }
    grantControls = @{ operator = "OR"; builtInControls = @("block") }
}
Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/identity/conditionalAccess/policies" -Method POST -Body ($params | Con
```

VALEUR PAR DÉFAUT :

Device Code Flow autorisé — aucune restriction par défaut.

1.3.7 *Bloquer le flux d'authentification legacy (Other Clients)* Critique

Licence requise : Entra ID P1

DESCRIPTION :

Les clients d'authentification legacy (MAPI, POP, IMAP, SMTP AUTH, Exchange ActiveSync ancienne version) ne supportent pas le MFA et l'Accès Conditionnel. Une politique CA doit bloquer explicitement les deux types : "Other clients" et "Exchange ActiveSync clients". De nombreux audits révèlent que seul l'un des deux est bloqué, laissant un vecteur ouvert.

```
# Vérifier les deux types de clients legacy
$caPolicies = Get-MgIdentityConditionalAccessPolicy -All | Where-Object { $_.State -eq "enabled" }

# Politique pour "Other clients"
$blockOther = $caPolicies | Where-Object {
    $_.Conditions.ClientAppTypes -contains "exchangeActiveSync" -or
    $_.Conditions.ClientAppTypes -contains "other"
} | Where-Object {
    $_.GrantControls.BuiltInControls -contains "block"
}

Write-Host "Legacy auth (Other) bloqué : $(if($blockOther){'✅'}else{'❌ CRITIQUE'})"
```

REMÉDIATION :

1. Politique CA couvrant `exchangeActiveSync` ET `other` client types
2. Vérifier que les deux sont dans la même politique ou deux politiques distinctes
3. Exclure uniquement les comptes Break Glass

VALEUR PAR DÉFAUT :

Clients legacy non bloqués — auth sans MFA possible.

1.3.8 *Politique CA : Auth résistante au phishing pour les administrateurs (FIDO2/Passkey)* Élevé

Licence requise : Entra ID P1 + Microsoft Authenticator / FIDO2

DESCRIPTION :

Le MFA classique (SMS, push notification) est vulnérable aux attaques de type AiTM (Adversary-in-the-Middle) et MFA fatigue. Les méthodes d'authentification résistantes au phishing (FIDO2, Windows Hello for Business, Certificate-based Auth) ne peuvent pas être interceptées car elles sont liées au domaine. La CISA exige ces méthodes pour les rôles hautement privilégiés.

```
# Vérifier une politique CA exigeant l'auth résistante au phishing pour les admins
$caPolicies = Get-MgIdentityConditionalAccessPolicy -All | Where-Object { $_.State -eq "enabled" }
$phishResistant = $caPolicies | Where-Object {
    $_.GrantControls.AuthenticationStrength -ne $null
} | Where-Object {
    $_.Conditions.Users.IncludeRoles.Count -gt 0
}
$phishResistant | Select-Object DisplayName, @{N='Strength';E={$_.GrantControls.AuthenticationStrength.DisplayName}} | Format-Table
```

REMÉDIATION :

1. Entra ID > Sécurité > Méthodes d'authentification > Niveaux d'authentification
2. Utiliser le niveau prédéfini "Phishing-resistant MFA"
3. Politique CA ciblant les rôles admin avec ce niveau d'authentification requis
4. Déployer les clés FIDO2 ou Windows Hello for Business pour les admins

VALEUR PAR DÉFAUT :

MFA standard (pas résistant au phishing) — méthodes SMS/push autorisées.

1.3.9 *Politique CA : Restreindre l'accès aux réseaux conformes uniquement (Compliant Network)* Élevé

Licence requise : Entra ID P1 + Entra Suite (pour Global Secure Access)

DESCRIPTION :

La condition "Réseau conforme" (Compliant Network) dans l'Accès Conditionnel restreint l'accès aux ressources M365 aux seuls appareils passant par le réseau approuvé de l'organisation — qu'il soit physique (réseau d'entreprise) ou virtuel (Microsoft Entra Internet Access). Elle complète les Named Locations en ajoutant une dimension de conformité réseau : même depuis une IP d'entreprise, un appareil personnel ou compromis peut être bloqué si le trafic ne transite pas par le SWG approuvé. C'est une défense clé contre les contournements de CA via VPN partagés.

```
# Vérifier l'existence d'une politique CA avec condition de réseau conforme
$caPolicies = Get-MgIdentityConditionalAccessPolicy -All | Where-Object { $_.State -eq "enabled" }
$compliantNetwork = $caPolicies | Where-Object {
    ($_.Conditions | ConvertTo-Json -Depth 5) -match "compliantNetwork|networkType"
}
if ($compliantNetwork) {
    Write-Host "✅ Politique CA avec Compliant Network trouvée : $($compliantNetwork.DisplayName)" -ForegroundColor Green
} else {
    Write-Host "⚠️  Aucune politique CA avec condition réseau conforme" -ForegroundColor Yellow
}
# Portail : Entra ID > CA > [Politique] > Conditions > Réseaux > Réseau conforme
```

REMÉDIATION :

1. Prérequis : déployer Microsoft Entra Internet Access (Global Secure Access)
2. Créer politique CA : Conditions > Réseaux > Inclure "Réseau conforme"
3. Applications cloud : Exchange Online, SharePoint Online, Teams
4. Accorder : Accorder l'accès (le réseau conforme est lui-même le contrôle)
5. Démarrer en mode "Rapport seul" avant d'activer pour mesurer l'impact

VALEUR PAR DÉFAUT :

Aucune condition réseau conforme — accès depuis n'importe quel réseau possible.

1.3b — Paramètres Utilisateurs Entra ID Supplémentaires

1.3c — Gestion des Appareils Entra ID

1.3d — Gestion Hybride

1.4 — Accès Conditionnel Basé sur le Risque (Identity Protection)

1.4.1 *Bloquer les utilisateurs détectés comme à haut risque* Critique

Licence requise : Entra ID P2

MITRE ATT&CK : T1078 (Valid Accounts) · T1586 (Compromise Accounts) · T1110.004 (Brute Force: Credential Stuffing)

DESCRIPTION :

Entra ID Identity Protection calcule un score de risque pour chaque utilisateur basé sur des signaux d'intelligence des menaces (Microsoft détecte des milliards de connexions et identifie des patterns d'attaque). Un utilisateur "haut risque" a probablement ses credentials dans une base de données compromise ou a montré des comportements anormaux. Ces comptes doivent être bloqués immédiatement jusqu'à remédiation sécurisée.

AUDIT :

- Entra ID > Protection > Accès Conditionnel > Vérifier l'existence d'une politique de risque utilisateur élevé
- PowerShell :

```
Get-MgIdentityConditionalAccessPolicy | Where-Object {
    $_.Conditions.UserRiskLevels -contains "high"
} | Select-Object DisplayName, State
```

REMÉDIATION :

1. Entra ID > Protection > Accès Conditionnel > Créer une politique
2. Conditions > Risque de l'utilisateur → Élevé
3. Accorder → Bloquer l'accès
4. Alternativement : Exiger MFA + Changement de mot de passe sécurisé (si vous souhaitez permettre une auto-remédiation)
5. Configurer les alertes pour notifier le SOC lors de la détection d'utilisateurs à haut risque (MS.AAD.2.2v1)

1.4.2 *Bloquer les connexions détectées comme à haut risque* Critique

Licence requise : Entra ID P2

DESCRIPTION :

Distinct du risque utilisateur, le risque de connexion évalue chaque tentative de connexion individuellement : voyage impossible (connexion depuis Paris puis New York en 10 minutes), adresses IP anonymisées (Tor, VPN connus malveillants), pulvérisation de mots de passe, etc. Ces connexions doivent être bloquées même si les credentials sont corrects.

AUDIT :

- Entra ID > Protection > Accès Conditionnel > Vérifier l'existence d'une politique de risque de connexion élevé
- Entra ID > Protection > Rapport sur les connexions risquées

REMÉDIATION :

1. Créer une politique CA : Conditions > Risque de connexion → Élevé
2. Accorder → Bloquer l'accès (ou Exiger MFA résistante au phishing)
3. Pour le risque moyen : Exiger MFA comme étape d'auto-remédiation
4. Réviser hebdomadairement le tableau de bord des connexions risquées

1.4b — Politique CA Supplémentaires (CIS v6.0.1)

1.5 — Gestion des Applications et Consentements

1.5.1 *Restreindre l'enregistrement d'applications aux administrateurs uniquement* Élevé

DESCRIPTION :

Par défaut, n'importe quel utilisateur peut enregistrer des applications dans Entra ID. Des applications malveillantes enregistrées par des utilisateurs compromis peuvent obtenir des tokens OAuth persistants avec des permissions larges sur les données de l'organisation.

```
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions.AllowedToCreateApps
```

AUDIT :

Doit retourner : `False`

```
$permObj = (Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions
$permObj.AllowedToCreateApps = $false
Update-MgPolicyAuthorizationPolicy -DefaultUserRolePermissions $permObj
```

1.5.2 *Restreindre le consentement aux applications tierces aux administrateurs uniquement* Critique

MITRE ATT&CK : T1528 (Steal Application Access Token) · T1550.001 (Use Alternate Auth Material: Application Access Token) · T1071.001 (Web Protocols)

DESCRIPTION :

Le consentement OAuth des utilisateurs est exploité dans les attaques de type "Consent Phishing" (ou OAuth Phishing) : un attaquant crée une application malveillante qui demande des permissions sur les données M365, envoie un lien à la victime, et obtient un accès persistant sans mot de passe ni MFA une fois le consentement accordé.

AUDIT :

- Entra ID > Applications d'entreprise > Paramètres utilisateur > Consentement utilisateur pour les applications
- Doit être configuré sur : "Ne pas autoriser le consentement utilisateur"

REMÉDIATION :

1. Entra ID > Applications d'entreprise > Consentement et permissions
2. Consentement utilisateur pour les applications : "Ne pas autoriser le consentement utilisateur"
3. Activer le workflow d'approbation administrateur (MS.AAD.5.3v1) pour que les utilisateurs puissent demander l'autorisation
4. Désigner des réviseurs de consentement (RSSI, équipe IT)

1.5.3 *Activer le workflow de consentement administrateur* — Élevé

DESCRIPTION :
Une fois le consentement utilisateur désactivé, les utilisateurs légitimes qui ont besoin d'une application tierce doivent pouvoir soumettre une demande d'approbation. Sans ce workflow, ils contournent les politiques en cherchant des alternatives non sécurisées.

AUDIT :
- Entra ID > Applications d'entreprise > Consentement et permissions > Workflow d'approbation administrateur

REMÉDIATION :
1. Entra ID > Applications d'entreprise > Paramètres utilisateur > Workflow d'approbation administrateur
2. Activer "Les utilisateurs peuvent demander le consentement administrateur pour les applications auxquelles ils ne peuvent pas accorder leur consentement"
3. Ajouter des réviseurs de consentement
4. Délai d'expiration des demandes : 30 jours

1.5.4 *Exiger des Éditeurs Vérifiés (Verified Publishers) pour les applications tierces* — Élevé

Licence requise : Entra ID P1

DESCRIPTION :
Les applications OAuth tierces d'éditeurs non vérifiés sont la source principale des attaques de Consent Phishing : n'importe qui peut créer une application Azure AD demandant des permissions M365, sans aucune validation d'identité. Les éditeurs vérifiés (Verified Publishers) ont prouvé leur identité via Microsoft Partner Network. Restreindre le consentement ou la visibilité aux seules applications d'éditeurs vérifiés réduit drastiquement la surface des applications malveillantes.

```
# Lister les applications tierces consentées sans éditeur vérifié
$sps = Get-MgServicePrincipal -All | Where-Object {
    $_.AppOwnerOrganizationId -ne (Get-MgContext).TenantId -and
    $_.VerifiedPublisher.DisplayName -eq $null
}
Write-Host "Applications tierces sans éditeur vérifié : $($sps.Count)"
$sps | Select-Object DisplayName, AppId | Format-Table
```

REMÉDIATION :
1. Entra ID > Applications d'entreprise > Consentement et permissions > Paramètres de consentement utilisateur
2. "Consentement pour les applications d'éditeurs vérifiés" : activer la restriction
3. Pour les applications existantes sans éditeur vérifié : évaluer le besoin et révoquer les consentements non justifiés
4. Entra ID > Applications d'entreprise > filtrer par "Non vérifié" et revoir chaque application
5. Former les utilisateurs à identifier le badge "Éditeur vérifié" avant de consentir

VALEUR PAR DÉFAUT :
Aucune restriction sur le statut d'éditeur — applications vérifiées et non vérifiées traitées identiquement.

1.5b — Méthodes d'Authentification Supplémentaires (CIS v6.0.1)

1.5c — Sécurité Avancée des Applications et Service Principals

1.6 — Journalisation et SIEM

1.6.1 *Envoyer les journaux de sécurité Entra ID vers un SIEM* — Critique

DESCRIPTION :
Les journaux Entra ID (connexions, audit, provisionning) doivent être transmis en temps réel vers un SIEM ou un SOC pour la corrélation, la détection et la réponse aux incidents. La rétention native M365 (90 jours standard) est insuffisante pour les investigations d'incidents découverts tarditement. Le NIST et l'OMB M-21-31 exigent 12 mois de rétention active + 18 mois de stockage froid.

AUDIT :
- Entra ID > Journaux de diagnostic (Diagnostic Settings)
- Vérifier qu'une destination est configurée (Log Analytics, Event Hub, Storage Account, SIEM partenaire)

REMÉDIATION :
1. Entra ID > Surveillance > Paramètres de diagnostic > Ajouter un paramètre de diagnostic
2. Sélectionner les journaux : SignInLogs, AuditLogs, NonInteractiveUserSignInLogs, ServicePrincipalSignInLogs, ManagedIdentitySignInLogs, RiskyUsers, UserRiskEvents
3. Destination : Log Analytics Workspace (Microsoft Sentinel recommandé) ou Event Hub vers SIEM tiers
4. Durée de rétention Log Analytics : 90 jours minimum, archive 18 mois
5. Pour conformité OMB M-21-31 : 12 mois actif + 18 mois stockage froid

1.7 — Gestion des Invités (Guest Access)

1.7.1 *Restreindre l'accès des invités aux objets de l'annuaire* — Élevé

DESCRIPTION :
Par défaut, les utilisateurs invités peuvent énumérer les objets de l'annuaire Entra ID (utilisateurs, groupes, applications). Cette capacité peut être utilisée pour de la reconnaissance interne par des comptes invités malveillants ou compromis.

AUDIT :
- Entra ID > Identités externes > Paramètres de collaboration externe
- Vérifier les permissions des utilisateurs invités

REMÉDIATION :
1. Entra ID > Identités externes > Paramètres de collaboration externe
2. Autorisations des utilisateurs invités : "Les utilisateurs invités ont un accès limité aux propriétés et appartenances des objets d'annuaire" (ou "L'accès des utilisateurs invités est restreint à...")
3. Ne pas utiliser "Les utilisateurs invités ont les mêmes accès que les membres"

1.7.2 *Restreindre qui peut inviter des utilisateurs invités* — Élevé

DESCRIPTION :
Si n'importe quel utilisateur peut inviter des guests, des invitations non contrôlées peuvent introduire des comptes externes non vérifiés dans le tenant, augmentant la surface d'attaque et les risques de fuite de données.

```
(Get-MgPolicyAuthorizationPolicy).AllowInvitesFrom
```

AUDIT :
Doit retourner : `adminsAndGuestInviters` ou `adminsOnly`

REMÉDIATION :
1. Entra ID > Identités externes > Paramètres de collaboration externe
2. "Qui peut inviter des utilisateurs invités" : Administrateurs et utilisateurs ayant le rôle d'inviteur d'invités
3. Ou : Uniquement les administrateurs (option la plus restrictive)

1.7.3 *Restreindre les invitations aux domaines externes approuvés* — Élevé

DESCRIPTION :
Sans liste blanche de domaines, des comptes invités peuvent être créés depuis n'importe quel domaine, y compris des domaines créés spécifiquement pour l'attaque. Restreindre aux domaines partenaires connus réduit ce risque.

AUDIT :
- Entra ID > Identités externes > Paramètres de collaboration externe > Restrictions de collaboration

REMÉDIATION :
1. Entra ID > Identités externes > Paramètres de collaboration externe
2. Restrictions de collaboration : "Autoriser les invitations uniquement aux domaines spécifiés"
3. Ajouter la liste des domaines partenaires approuvés
4. Révision trimestrielle de la liste des invités actifs

1.8 — Gestion des Rôles Privilégiés

1.8.1 *Activer Privileged Identity Management (PIM)* — Critique

Licence requise : Entra ID P2
MITRE ATT&CK : T1078.004 (Valid Accounts: Cloud) · T1548 (Abuse Elevation Control Mechanism) · T1098 (Account Manipulation)

DESCRIPTION :
PIM implémente le principe du Just-In-Time (JIT) : les administrateurs n'ont pas de droits permanents, ils les activent à la demande pour une durée limitée avec justification. Cela réduit drastiquement la fenêtre d'exposition en cas de compromission de compte admin.

AUDIT :
- Entra ID > Gestion des identités > Privileged Identity Management
- Vérifier les rôles configurés en mode "Eligible" vs "Active permanent"
- PowerShell :

```
Get-MgRoleManagementDirectoryRoleAssignment | Where-Object {$_.AssignmentType -eq "Assigned"} | Select-Object PrincipalId, RoleDefi
```

REMÉDIATION :
1. Activer PIM pour tous les rôles privilégiés Entra ID
2. Convertir les assignations permanentes en assignations "Éligibles"
3. Configurer : durée d'activation max = 4 heures, justification obligatoire, approbation pour rôles critiques
4. Configurer les alertes PIM (assignations permanentes détectées, activations suspectes)
5. Rôles prioritaires à protéger : Global Administrator, Privileged Role Administrator, Security Administrator, Exchange Administrator, SharePoint Administrator

1.8.2 *Limiter le nombre d'Administrateurs Globaux* Critique

MITRE ATT&CK : T1078.004 (Valid Accounts: Cloud) · T1136.003 (Create Account: Cloud) · T1087.004 (Account Discovery: Cloud)

DESCRIPTION :

Le rôle Global Administrator est le plus puissant de M365. Plus il y a de personnes avec ce rôle, plus la surface d'attaque est grande. Le CIS recommande entre 2 et 4 Global Admins maximum (pour la redondance sans excès).

AUDIT :

- Entra ID > Rôles et administrateurs > Administrateur général
- PowerShell :

```
Get-MgDirectoryRoleMember -DirectoryRoleId (Get-MgDirectoryRole -Filter "DisplayName eq 'Global Administrator'").Id | Select-Object
```

REMÉDIATION :

1. Conserver uniquement 2 à 4 Global Admins maximum
2. Remplacer le Global Admin par des rôles spécialisés (Exchange Admin, SharePoint Admin, etc.) pour les tâches spécifiques
3. Utiliser des comptes dédiés "break glass" (comptes d'urgence) distincts des comptes quotidiens
4. Activer PIM pour le rôle Global Admin

1.8.3 *Utiliser des rôles à granularité fine plutôt que Global Admin* Critique

DESCRIPTION :

Le Global Administrator a accès à TOUT dans le tenant M365. La grande majorité des tâches d'administration peuvent être effectuées avec des rôles spécialisés qui limitent l'impact d'une compromission. Un administrateur Exchange n'a pas besoin d'accéder à SharePoint ou Intune.

```
# Identifier les utilisateurs avec Global Admin qui pourraient avoir un rôle plus restreint
$gaMembers = Get-MgDirectoryRoleMember -DirectoryRoleId (Get-MgDirectoryRole -Filter "DisplayName eq 'Global Administrator'").Id
$gaMembers | ForEach-Object {
    Get-MgUserAppRoleAssignment -UserId $_.Id
}
```

REMÉDIATION :

Rôles de remplacement recommandés par fonction :

- Exchange : Exchange Administrator
- SharePoint : SharePoint Administrator
- Teams : Teams Administrator
- Sécurité : Security Administrator / Security Reader
- Utilisateurs : User Administrator
- Facturation : Billing Administrator
- Intune : Intune Administrator
- Conformité : Compliance Administrator

1.8.4 *Provisionner les administrateurs avec des comptes cloud uniquement* Critique

DESCRIPTION :

Les comptes admin synchronisés depuis l'Active Directory on-premises héritent des risques de l'AD : si un DC est compromis, l'attaquant obtient automatiquement les credentials des comptes admin cloud. Les comptes admin cloud-only sont isolés de cette chaîne de compromission.

```
# Vérifier les admins synchronisés depuis on-prem (OnPremisesSyncEnabled = true)
Get-MgDirectoryRoleMember -DirectoryRoleId (Get-MgDirectoryRole -Filter "DisplayName eq 'Global Administrator'").Id | ForEach-Objec
    Get-MgUser -UserId $_.Id | Select-Object DisplayName, UserPrincipalName, OnPremisesSyncEnabled
}
```

REMÉDIATION :

1. Créer de nouveaux comptes admin directement dans Entra ID (cloud-only)
2. Format recommandé : adm_prenom.nom@domaine.com (ne pas synchroniser depuis l'AD)
3. Migrer les assignations de rôles vers ces nouveaux comptes cloud-only
4. Révoquer les rôles sur les comptes synchronisés

1.8.5 *Exiger une approbation pour l'activation du rôle Global Administrator* Critique

Licence requise : Entra ID P2 (PIM)

DESCRIPTION :

Même avec PIM, l'activation du rôle le plus puissant (Global Admin) ne doit pas être auto-approuvée. Exiger une approbation humaine d'un second administrateur crée un contrôle de validation ("four-eyes principle") qui ralentit un attaquant ayant compromis un compte éligible.

AUDIT :

- Entra ID > PIM > Rôles Entra ID > Administrateur général > Paramètres
- Vérifier que "Approbation requise" est activé et qu'au moins un approbateur est configuré

REMÉDIATION :

1. PIM > Rôles Entra ID > Administrateur général > Paramètres du rôle > Modifier
2. Activation : Exiger l'approbation → Oui
3. Ajouter des approbateurs (au moins 2 personnes de confiance distinctes)
4. Durée maximale d'activation : 4 heures

1.8.6 *Configurer des alertes sur les activations de rôles privilégiés* — Élevé

Licence requise : Entra ID P2 (PIM)

DESCRIPTION :
Toute activation de rôle hautement privilégié doit déclencher une notification immédiate vers le SOC ou le RSSI. Les assignations permanentes de rôles (sans PIM) doivent également déclencher une alerte — elles peuvent indiquer qu'un attaquant a consolidé un accès persistant.

AUDIT :
- PIM > Rôles Entra ID > Alertes > Vérifier les alertes configurées
- Vérifier que les notifications email sont configurées pour chaque rôle critique

REMÉDIATION :
1. PIM > Rôles Entra ID > Alertes PIM : activer toutes les alertes disponibles
2. PIM > Chaque rôle critique > Paramètres > Notifications : configurer l'email du SOC/RSSI pour activation et assignation
3. Rôles prioritaires pour alertes : Global Admin, Privileged Role Admin, Security Admin, Exchange Admin, SharePoint Admin, User Admin
4. Créer des règles d'alerte Microsoft Sentinel (ou SIEM) pour corréler avec d'autres activités suspectes

1.8.7 *Créer des comptes d'urgence (Break Glass Accounts)* — Critique

MITRE ATT&CK : T1078.004 (Valid Accounts: Cloud) · T1098.001 (Account Manipulation: Additional Cloud Credentials) · T1556 (Modify Authentication Process)

DESCRIPTION :
Les comptes d'urgence permettent de récupérer l'accès au tenant en cas de panne MFA, de problème avec les politiques CA, ou de compromission des comptes admin normaux. Sans ces comptes, l'organisation risque d'être bloquée hors de son propre tenant.

AUDIT :
- Vérifier l'existence de 2 comptes d'urgence avec le rôle Global Admin
- Vérifier qu'ils sont exclus de TOUTES les politiques CA (y compris MFA)
- Vérifier qu'ils utilisent des mots de passe complexes stockés dans un coffre-fort physique
- Vérifier la surveillance des connexions sur ces comptes (alerte immédiate si utilisés)

REMÉDIATION :
1. Créer 2 comptes type : breakglass01@domaine.com et breakglass02@domaine.com
2. Mots de passe aléatoires de 32+ caractères, imprimés et stockés en coffre-fort physique
3. Exclure ces comptes de TOUTES les politiques CA
4. Créer une alerte : toute connexion sur ces comptes = notification immédiate SOC/RSSI
5. Tester trimestriellement que ces comptes fonctionnent
6. Ne jamais utiliser pour les tâches quotidiennes

1.8.8 *Utiliser des comptes admin dédiés (sans messagerie)* — Élevé

DESCRIPTION :
Les comptes administrateurs ne doivent pas recevoir d'emails. Un admin qui lit ses emails depuis son compte admin peut être victime de phishing, et si le compte admin est compromis via phishing, l'attaquant a directement accès aux privilèges admin. Les comptes admin doivent être distincts des comptes utilisateur quotidiens.

AUDIT :
- Vérifier que les comptes admin n'ont pas de boîte mail active ou de licence Exchange
- Vérifier que les admins utilisent des comptes séparés pour les tâches admin vs quotidiennes

REMÉDIATION :
1. Créer des comptes admin avec convention de nommage distincte (ex: adm_prenom.nom@domaine.com)
2. Ne pas assigner de licence Exchange/M365 aux comptes admin purs
3. Utiliser un compte utilisateur standard pour la messagerie et naviguer, un compte admin pour les tâches d'administration
4. Former les administrateurs à utiliser des navigateurs séparés ou profils distincts

1.8.9 *Activer les révisions d'accès pour les utilisateurs invités (Guests)* — Élevé

Profile : E3 Level 2

Licence requise : Entra ID P2

DESCRIPTION :
Au-delà des révisions d'accès pour les rôles admin, les comptes invités doivent faire l'objet de révisions régulières. Les invités sont souvent des prestataires, partenaires ou anciens collaborateurs dont l'accès n'est plus justifié mais n'a jamais été révoqué. Chaque invité actif est un risque potentiel.

AUDIT :
- Entra ID > Gestion des identités > Révisions d'accès
- Vérifier l'existence de révisions ciblant le groupe dynamique des guests

REMÉDIATION :
1. Créer une révision d'accès trimestrielle pour le groupe dynamique "Tous les invités"
2. Réviseurs : responsables métier ou sponsoring managers des invités
3. Paramètre : si non répondu dans 30 jours → supprimer l'accès automatiquement
4. Exiger une justification pour conserver l'accès

1.8.10 *Exiger une approbation pour l'activation du rôle Privileged Role Administrator* — Critique

Profile : E3 Level 1

Licence requise : Entra ID P2 (PIM)

DESCRIPTION :

Le rôle "Privileged Role Administrator" permet de modifier les attributions de rôles PIM elles-mêmes — c'est le "roi des rois" en termes de persistance : un attaquant obtenant ce rôle peut s'octroyer n'importe quel autre rôle. Il doit donc être traité avec le même niveau de contrôle que le Global Administrator.

AUDIT :

- PIM > Rôles Entra ID > Administrateur de rôles privilégiés > Paramètres
- Vérifier que "Approbation requise" est activé

REMÉDIATION :

1. PIM > Rôles Entra ID > Administrateur de rôles privilégiés > Paramètres du rôle > Modifier
2. Approbation requise pour activation : Oui
3. Approbateurs : au moins 2 Global Admins distincts
4. Durée maximale d'activation : 2 heures

1.8.11 *Activer les révisions d'accès (Access Reviews) pour les rôles admin* — Élevé

Licence requise : Entra ID P2

DESCRIPTION :

Les droits d'administration s'accumulent avec le temps (privilege creep). Les Access Reviews permettent une révision périodique des assignations de rôles pour s'assurer que seuls les utilisateurs légitimes conservent leurs droits.

AUDIT :

- Entra ID > Gestion des identités > Révisions d'accès
- Vérifier l'existence de révisions programmées pour les rôles admin

REMÉDIATION :

1. Créer des révisions d'accès trimestrielles pour tous les rôles admin
2. Désignation des réviseurs : managers directs ou RSSI
3. Paramètre : si le réviseur ne répond pas dans le délai → supprimer l'accès automatiquement
4. Révision annuelle pour les utilisateurs standards sur les applications sensibles

1.8.12 *Détecter les comptes administrateurs inactifs depuis plus de 90 jours* — Élevé

Licence requise : Entra ID P1

DESCRIPTION :

Les comptes administrateurs inactifs depuis plus de 90 jours représentent un risque élevé : ils sont souvent liés à des anciens employés, des comptes de service abandonnés ou des comptes créés temporairement et jamais désactivés. Un attaquant qui obtient ces credentials (breach, dark web) accède directement à des rôles élevés sans déclencher d'alerte comportementale.

```
# Admins inactifs depuis plus de 90 jours
$threshold = (Get-Date).AddDays(-90)
$adminRoles = Get-MgDirectoryRole
foreach ($role in $adminRoles) {
    $members = Get-MgDirectoryRoleMember -DirectoryRoleId $role.Id -All
    foreach ($member in $members) {
        $user = Get-MgUser -UserId $member.Id -Property "displayName,userPrincipalName,signInActivity" -ErrorAction SilentlyContinu
        if ($user -and $user.SignInActivity.LastSignInDateTime -lt $threshold) {
            [PSCustomObject]@{
                Role = $role.DisplayName
                User = $user.DisplayName
                UPN  = $user.UserPrincipalName
                LastSignIn = $user.SignInActivity.LastSignInDateTime
            }
        }
    }
} | Format-Table
```

REMÉDIATION :

1. Désactiver immédiatement les comptes admins sans connexion depuis > 90 jours
2. Révoquer les sessions actives : `Revoke-MgUserSignInSession -UserId`
3. Déplacer les comptes suspects dans un groupe de quarantaine avant suppression
4. Implémenter un processus offboarding qui inclut la révocation des rôles admin
5. Configurer une alerte automatique mensuelle sur les admins inactifs

VALEUR PAR DÉFAUT :

Aucune alerte sur l'inactivité des comptes admin.

1.8.13 *Vérifier que les administrateurs privilégiés ne sont pas exclus des politiques CA critiques* Critique

Licence requise : Entra ID P1

DESCRIPTION :

Les politiques de Conditional Access contiennent souvent des exclusions (comptes de service, comptes d'urgence). Si des administrateurs privilégiés ou des groupes admin se retrouvent dans les exclusions de politiques CA critiques (MFA, blocage auth legacy, conformité appareil), ces comptes peuvent contourner toutes les protections. C'est l'une des failles les plus fréquemment exploitées lors d'incidents M365.

```
# Vérifier les exclusions dans les politiques CA critiques
$caPolicies = Get-MgIdentityConditionalAccessPolicy -All | Where-Object { $_.State -eq "enabled" }
foreach ($policy in $caPolicies) {
    $excludedUsers = $policy.Conditions.Users.ExcludeUsers
    $excludedGroups = $policy.Conditions.Users.ExcludeGroups
    if ($excludedUsers.Count -gt 0 -or $excludedGroups.Count -gt 0) {
        # Vérifier si des admins privilégiés sont dans les exclusions
        foreach ($userId in $excludedUsers) {
            $user = Get-MgUser -UserId $userId -ErrorAction SilentlyContinue
            $adminRoles = Get-MgUserMemberOf -UserId $userId | Where-Object { $_.AdditionalProperties.'@odata.type' -eq '#microsoft
            if ($adminRoles) {
                Write-Host "⚠️ CRITICAL: Admin user $($user.DisplayName) excluded from policy: $($policy.DisplayName)" -ForegroundC
            }
        }
    }
}
```

REMÉDIATION :

1. Revoir toutes les exclusions des politiques CA — enlever les comptes admin non justifiés
2. Les exclusions doivent se limiter aux comptes Break Glass et aux comptes de service documentés
3. S'assurer que les exclusions sont temporaires et révisées mensuellement
4. Documenter chaque exclusion avec sa justification et sa date d'expiration
5. Utiliser les noms de groupes plutôt que des utilisateurs individuels pour faciliter l'audit

VALEUR PAR DÉFAUT :

Aucune validation automatique des exclusions CA.

1.8.14 *Détecter les comptes AD synchronisés dans des rôles cloud privilégiés* Critique

Licence requise : Entra ID P1

DESCRIPTION :

Les comptes synchronisés depuis l'Active Directory on-premises ne doivent **jamais** avoir de rôles cloud privilégiés. Si le compte AD on-prem est compromis (ransomware, DC compromise, GPO malveillante), l'attaquant hérite automatiquement des rôles cloud. La règle absolue : les admins cloud doivent être des comptes cloud-only. C'est le chemin d'attaque AD → M365 le plus fréquent en 2026.

```
# Comptes synchros avec rôles cloud privilégiés — vecteur critique
$adminRoles = Get-MgDirectoryRole
$syncedAdmins = @()
foreach ($role in $adminRoles) {
    $members = Get-MgDirectoryRoleMember -DirectoryRoleId $role.Id -All
    foreach ($member in $members) {
        $user = Get-MgUser -UserId $member.Id -Property "displayName,userPrincipalName,onPremisesSyncEnabled" -ErrorAction Silently
        if ($user -and $user.OnPremisesSyncEnabled -eq $true) {
            $syncedAdmins += [PSCustomObject]@{
                Role = $role.DisplayName
                User = $user.DisplayName
                UPN  = $user.UserPrincipalName
                OnPremSync = $true
            }
        }
    }
}
$syncedAdmins | Format-Table
# Résultat attendu : Aucun résultat
```

REMÉDIATION :

1. Créer des comptes cloud-only dédiés pour chaque admin ayant un compte synchro
2. Transférer les rôles admin cloud vers les comptes cloud-only
3. Supprimer les rôles cloud des comptes synchros
4. Désactiver les comptes synchros dans Entra ID (conserver pour accès on-prem uniquement)
5. Configurer une alerte sur toute future assignation de rôle cloud à un compte synchro

VALEUR PAR DÉFAUT :

Aucune restriction — les comptes synchros peuvent avoir des rôles cloud.

1.8.15 *Enforcer l'authentification Passwordless (FIDO2 / Windows Hello for Business) pour les comptes privilégiés* — Critique

Licence requise : Entra ID P1 + Entra ID P2 (recommandé)

DESCRIPTION :

L'authentification passwordless (FIDO2, Windows Hello for Business, Microsoft Authenticator Passwordless) élimine les risques liés aux mots de passe : credential stuffing, phishing, password spray. Pour les comptes privilégiés, c'est le niveau de protection le plus élevé recommandé par CISA en 2026. Les méthodes classiques MFA (OTP, SMS, Authenticator push) restent vulnérables aux attaques de type AiTM (Adversary-in-The-Middle). Le passwordless élimine ce vecteur car il n'y a pas de secret partageable.

```
# Vérifier les méthodes d'authentification des admins — identifier ceux sans Passwordless
$adminRoles = Get-MgDirectoryRole | Where-Object { $_.DisplayName -match "Administrator" }
foreach ($role in $adminRoles) {
    $members = Get-MgDirectoryRoleMember -DirectoryRoleId $role.Id -All
    foreach ($member in $members) {
        $methods = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/users/$($member.Id)/authentication/methods" -Method
        $hasPasswordless = $methods.value | Where-Object {
            $_.'@odata.type' -match "fido2|microsoftAuthenticatorAuthentication|windowsHelloForBusiness"
        }
        if (-not $hasPasswordless) {
            Write-Host "⚠️ Admin sans Passwordless: $($member.AdditionalProperties.displayName) — Role: $($role.DisplayName)" -Fore
        }
    }
}
```

REMÉDIATION :

1. Entra ID > Protection > Méthodes d'authentification > Politiques
2. Activer FIDO2 Security Keys pour les comptes admin (`Microsoft.Graph.Identity.SignIns`)
3. Créer une politique CA : Admins privilégiés → Exiger auth résistante au phishing (FIDO2/WHfB)
4. Déployer des clés FIDO2 physiques (YubiKey, Feitian) pour les Global Admins et les comptes Break Glass
5. Former les administrateurs à l'usage des clés FIDO2 et WHfB
6. Supprimer les méthodes SMS et appel vocal pour les comptes admin via la politique de méthodes d'auth

VALEUR PAR DÉFAUT :

Aucune exigence Passwordless — les admins peuvent utiliser des méthodes MFA traditionnelles vulnérables au phishing AiTM.

1.9 — Groupes, Appareils et Paramètres Avancés

1.9.1 *Créer un groupe dynamique pour les utilisateurs invités* — Élevé

Profile : E3 Level 1

DESCRIPTION :

Un groupe dynamique Entra ID avec la règle `(user.userType -eq "Guest")` permet d'appliquer automatiquement des politiques d'accès conditionnel, des restrictions et des contrôles de sécurité à tous les invités actuels et futurs. Sans ce groupe, les nouveaux comptes invités peuvent temporairement échapper aux contrôles de sécurité.

```
Connect-MgGraph -Scopes "Group.Read.All"
$groups = Get-MgGroup -All | Where-Object { $_.GroupTypes -contains "DynamicMembership" }
$groups | Where-Object { $_.MembershipRule -match "userType" } | ft DisplayName, MembershipRule
```

AUDIT :

Vérifier qu'un groupe existe avec la règle `(user.userType -eq "Guest")` .

```
$params = @{
    DisplayName = "Dynamic Guest Group"
    MailNickname = "DynGuestUsers"
    MailEnabled = $false
    SecurityEnabled = $true
    GroupTypes = @("DynamicMembership")
    MembershipRule = '(user.userType -eq "Guest")'
    MembershipRuleProcessingState = "On"
}
New-MgGroup @params
```

REMÉDIATION :

Utiliser ce groupe dans les politiques d'Accès Conditionnel ciblant les invités.

1.9.2 *Désactiver la création de groupes de sécurité par les utilisateurs* — Élevé

Profile : E3 Level 1

DESCRIPTION :

Par défaut, tous les utilisateurs peuvent créer des groupes de sécurité dans Azure Portal, l'API ou PowerShell. Cela peut conduire à une prolifération incontrôlée de groupes et à des escalades de privilèges si ces groupes sont ensuite utilisés pour gérer des accès.

```
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions | Select-Object AllowedToCreateSecurityGroups
# Valeur attendue : False
```

```
$params = @{
    defaultUserRolePermissions = @{
        AllowedToCreateSecurityGroups = $false
    }
}
Update-MgPolicyAuthorizationPolicy -BodyParameter $params
```

REMÉDIATION :

Ou via Entra ID > Groupes > Paramètres généraux : "Les utilisateurs peuvent créer des groupes de sécurité dans les portails Azure" → Non.

1.9.3 *Limiter le nombre maximum d'appareils par utilisateur (≤ 20)* — Élevé

Profile : E3 Level 1

DESCRIPTION :

Cette limite définit le nombre maximum d'appareils qu'un utilisateur peut inscrire dans Entra ID. Un quota élevé (défaut : 50) permet à un attaquant ayant compromis un compte d'inscrire de multiples appareils pour établir de la persistance. Microsoft recommande ≤ 20 appareils par utilisateur.

```
$Uri = "https://graph.microsoft.com/beta/policies/deviceRegistrationPolicy"
(Invoke-MgGraphRequest -Method GET -Uri $Uri).userDeviceQuota
# Valeur attendue : ≤ 20
```

REMÉDIATION :

- Entra ID > Appareils > Paramètres des appareils
- "Nombre maximum d'appareils par utilisateur" → 20 (ou moins)

1.9.4 *Ne pas ajouter le Global Administrator comme admin local lors de la jointure Entra* — Critique

Profile : E3 Level 1

DESCRIPTION :

Par défaut, le rôle Global Administrator est ajouté automatiquement au groupe des administrateurs locaux lors de la jointure Entra. Cela viole le principe du moindre privilège — les GA ont alors un accès admin local sur tous les appareils joints, ce qui crée un vecteur latéral majeur.

```
$Uri = "https://graph.microsoft.com/beta/policies/deviceRegistrationPolicy"
(Invoke-MgGraphRequest -Method GET -Uri $Uri).azureADJoin.localAdmins
# Valeur attendue : enableGlobalAdmins = False
```

REMÉDIATION :

- Entra ID > Appareils > Paramètres des appareils
- "Le rôle Global Administrator est ajouté comme administrateur local lors de la jointure Microsoft Entra" → Non

1.9.5 *Restreindre la jointure d'appareils à Entra ID* — Moyen

Profile : E3 Level 2

DESCRIPTION :

Par défaut, tous les utilisateurs peuvent joindre leurs appareils à Entra ID. Un attaquant ayant compromis un compte standard peut inscrire un appareil malveillant qui hérite des politiques MDM et semble conforme, obtenant ainsi un accès persistant aux ressources cloud sans déclencher de MFA.

```
$Uri = "https://graph.microsoft.com/beta/policies/deviceRegistrationPolicy"
(Invoke-MgGraphRequest -Method GET -Uri $Uri).azureADJoin.allowedToJoin
# Type attendu : #microsoft.graph.enumeratedDeviceRegistrationMembership (Sélectionné) ou #microsoft.graph.noDeviceRegistrationMemb
```

REMÉDIATION :

- Entra ID > Appareils > Paramètres des appareils
- "Les utilisateurs peuvent joindre des appareils à Microsoft Entra" → Sélectionné (définir un groupe autorisé) ou Aucun

1.9.6 *Masquer l'option "Rester connecté" (Stay signed in)* — Moyen

Profile : E3 Level 2

DESCRIPTION :

L'option "Rester connecté" crée un jeton d'actualisation persistant de 90 jours. Sur un ordinateur partagé ou public, cela permet à tout utilisateur suivant d'accéder aux données M365 sans authentification. Cette option doit être masquée pour tous les utilisateurs.

AUDIT :

- Entra ID > Entreprise > Paramètres utilisateur
- "Afficher l'option Maintenir la connexion" → Non

REMÉDIATION :

1. Entra ID Admin Center > Identité > Marque de société
2. Sélectionner votre configuration de marque
3. "Afficher l'option permettre aux utilisateurs de rester connectés" → Non
4. Sauvegarder

1.9.7 *Désactiver les connexions de compte LinkedIn* — Moyen

Profile : E3 Level 2

DESCRIPTION :

L'intégration LinkedIn permet aux utilisateurs de connecter leur compte professionnel Microsoft avec LinkedIn. Cela expose des informations organisationnelles (contacts, organigrammes) à un réseau social externe et peut faciliter des attaques de spear-phishing ciblées.

AUDIT :

- Entra ID > Utilisateurs > Paramètres utilisateur
- "Connexions de compte LinkedIn" → Non

REMÉDIATION :

1. Entra ID Admin Center > Identité > Utilisateurs > Paramètres utilisateur
2. "Les utilisateurs peuvent connecter leur compte professionnel ou scolaire avec LinkedIn" → Non
3. Sauvegarder

1.10 — Cross-Tenant Access, Tenant Restrictions et Évaluation Continue des Accès (CAE)

1.10.1 *Configurer les paramètres d'accès cross-tenant (XTAP)* Élevé

Profile : E3 Level 1

Licence requise : Entra ID P1

DESCRIPTION :

Les paramètres d'accès cross-tenant (Cross-Tenant Access Policies — XTAP) contrôlent comment les utilisateurs de votre tenant interagissent avec d'autres organisations Entra ID, et réciproquement. Par défaut, tous les accès B2B entre tenants sont autorisés sans restriction. Une mauvaise configuration permet à des utilisateurs externes non approuvés d'accéder à vos ressources ou à vos utilisateurs d'exfiltrer des données vers des tenants non contrôlés.

```
# Vérifier la politique par défaut cross-tenant
$policy = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/policies/crossTenantAccessPolicy" -Method GET
$policy | ConvertTo-Json -Depth 5

# Vérifier les politiques spécifiques par organisation partenaire
$partners = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/policies/crossTenantAccessPolicy/partners" -Method GET
$partners.value | Select-Object tenantId, displayName | Format-Table
```

AUDIT :

Vérifier que la politique par défaut est restrictive (inboundTrust, b2bCollaborationInbound/Outbound configurés).

REMÉDIATION :

1. Entra ID > Identités externes > Paramètres d'accès cross-tenant
2. **Paramètres par défaut** : Configurer pour bloquer toute collaboration B2B par défaut
3. **Paramètres inbounds** : Bloquer tous les utilisateurs externes sauf exceptions autorisées
4. **Paramètres outbounds** : Restreindre les applications accessibles depuis l'extérieur
5. Créer des politiques spécifiques pour les partenaires de confiance uniquement
6. Activer l'authentification multi-facteurs de confiance pour les partenaires spécifiques (MFA trust)

VALEUR PAR DÉFAUT :

Toutes les collaborations B2B sont autorisées par défaut.

1.10.2 *Implémenter les Tenant Restrictions v2 (TRv2)* Élevé

Profile : E3 Level 1

Licence requise : Entra ID P1 + proxy réseau ou Windows 11 intégré

DESCRIPTION :

Les Tenant Restrictions v2 (TRv2) empêchent les utilisateurs d'accéder à des tenants M365 non autorisés depuis les appareils ou réseaux de l'organisation. C'est une défense critique contre l'exfiltration de données via des tenants personnels ou non approuvés. Un utilisateur pourrait créer un tenant gratuit et y transférer des données sensibles — TRv2 bloque cette technique.

```
# Vérifier la politique de restriction de tenant
$policy = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/policies/crossTenantAccessPolicy/default" -Method GET
$policy.tenantRestrictions | ConvertTo-Json

# Pour Windows 11 : vérifier via registre (à exécuter sur les postes de travail)
# HKLM\SOFTWARE\Policies\Microsoft\Windows\TenantRestrictions
```

REMÉDIATION :

1. Entra ID > Identités externes > Paramètres d'accès cross-tenant > Paramètres par défaut > Restrictions de tenant
2. Activer les restrictions de tenant et définir les tenants autorisés
3. Pour les appareils Windows 11 : configurer via Intune la stratégie TRv2 (Global Secure Access ou proxy)
4. Pour les environnements avec proxy : injecter les en-têtes `Restrict-Access-To-Tenants` et `Restrict-Access-Context`
5. Utiliser Microsoft Entra Global Secure Access si disponible

VALEUR PAR DÉFAUT :

Aucune restriction de tenant configurée — les utilisateurs peuvent accéder à n'importe quel tenant.

1.10.3 *Activer l'Évaluation Continue des Accès (CAE)* Élevé

Profile : E3 Level 1

Licence requise : Entra ID P1

DESCRIPTION :

L'Évaluation Continue des Accès (CAE — Continuous Access Evaluation) permet à Entra ID de révoquer en temps quasi-réel les tokens d'accès lorsqu'un événement critique se produit (désactivation de compte, réinitialisation de mot de passe, modification de risque). Sans CAE, un token valide peut être utilisé pendant jusqu'à 1 heure même si le compte a été compromis et désactivé entre-temps. CAE réduit cette fenêtre à quelques secondes/minutes.

```
# Vérifier l'état de CAE
$caePolicy = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/policies/continuousAccessEvaluationPolicy" -Method GET
$caePolicy | ConvertTo-Json

# Résultat attendu : migrationState = "migrationComplete" ou isEnabled = $true
```

AUDIT :

- Portail Entra ID > Protection > Évaluation continue des accès

REMÉDIATION :

1. Entra ID > Protection > Évaluation continue des accès
2. Activer CAE pour l'ensemble du tenant (migration vers le mode "Tous les utilisateurs")
3. Vérifier que les applications clés supportent CAE (Exchange Online, SharePoint, Teams — supportés nativement)
4. Configurer les politiques CA avec le mode "Strict Location Enforcement" si nécessaire
5. PowerShell :

```
$params = @{
    isEnabled = $true
}
Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/policies/continuousAccessEvaluationPolicy" -Method PATCH -Body ($param
```

VALEUR PAR DÉFAUT :

CAE activé en mode migration partielle — à forcer en mode complet.

1.10.4 *Auditer les accès B2B et réaliser des Access Reviews régulières* Moyen

Profile : E3 Level 2

Licence requise : Entra ID P2

DESCRIPTION :

Les utilisateurs invités (B2B) accumulent souvent des accès non nécessaires au fil du temps. Sans revues périodiques, des anciens partenaires, prestataires ou collaborateurs temporaires conservent des accès indéfiniment. Les Access Reviews automatisent ce processus de certification et révocation périodique des accès.

```
# Lister les Access Reviews actives
$reviews = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/identityGovernance/accessReviews/definitions" -Method GET
$reviews.value | Select-Object displayName, status, createdDateTime | Format-Table

# Compter les utilisateurs invités actifs
(Get-MgUser -Filter "userType eq 'Guest'" -All).Count
```

REMÉDIATION :

1. Entra ID > Gouvernance des identités > Access Reviews > Nouvelle révision d'accès
2. Configurer une révision trimestrielle de tous les utilisateurs invités
3. Assigner les réviseurs (managers des sponsors ou groupe d'administration)
4. Activer la révocation automatique si non réponse dans le délai (auto-apply)
5. Configurer une politique d'expiration pour les comptes invités inactifs depuis 90 jours

VALEUR PAR DÉFAUT :

Aucune Access Review configurée — les accès invités ne sont jamais révisés.

SECTION 1.11 — GOUVERNANCE DES DROITS (ENTITLEMENT MANAGEMENT)

> **Contexte :** La gouvernance des droits (Entra ID Entitlement Management) est l'une des surfaces d'attaque les plus négligées. Des access packages avec des rôles supprimés, des groupes inexistants ou des approbateurs invalides créent des voies d'escalade silencieuses. Maester (MT.1106–1110) est le seul outil à automatiser ces vérifications.

1.11 — Gestion des Access Packages et Catalogues

1.11.1 *Auditer les ressources d'access packages avec rôles obsolètes* Élevé

Licence requise : Entra ID P2 (Governance)

DESCRIPTION :

Les access packages peuvent référencer des rôles d'applications qui ont été supprimés ou des Service Principals qui n'existent plus. Ces références fantômes créent des incohérences dans la gouvernance des droits et peuvent masquer des accès non révoqués.

```
# Vérifier les ressources de catalogues avec des rôles invalides
$catalogs = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/identityGovernance/entitlementManagement/catalogs" -Method
foreach ($catalog in $catalogs.value) {
    $resources = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/identityGovernance/entitlementManagement/catalogs/$($
    $resources.value | Where-Object { $_.roles.Count -eq 0 } | ForEach-Object {
        Write-Host "⚠️ Catalog: $($catalog.displayName) — Resource sans rôles: $($_.displayName)" -ForegroundColor Yellow
    }
}
```

REMÉDIATION :

1. Entra ID > Gouvernance des identités > Gestion des droits > Catalogues
2. Identifier les ressources sans rôles ou avec des rôles supprimés
3. Supprimer les ressources invalides des catalogues
4. Mettre à jour les access packages affectés

VALEUR PAR DÉFAUT :

Aucune validation automatique des ressources — les rôles supprimés restent référencés.

1.11.2 *Détecter les access packages référençant des groupes supprimés* Élevé

Licence requise : Entra ID P2

DESCRIPTION :

Les access packages peuvent référencer des groupes de sécurité ou M365 qui ont été supprimés. Quand un utilisateur reçoit un access package avec un groupe supprimé, l'assignation échoue silencieusement — l'utilisateur pense avoir les droits mais ne les a pas, ou inversement, les droits restent assignés sans le groupe de contrôle.

```
# Détecter les groupes supprimés dans les access packages
$accessPackages = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/identityGovernance/entitlementManagement/accessPacka
foreach ($pkg in $accessPackages.value) {
    foreach ($rrs in $pkg.resourceRoleScopes) {
        $resourceId = $rrs.resourceRole.resource.id
        $group = Get-MgGroup -GroupId $resourceId -ErrorAction SilentlyContinue
        if (-not $group) {
            Write-Host "⚠️ Access Package '$($pkg.displayName)' — Groupe supprimé: $resourceId" -ForegroundColor Red
        }
    }
}
```

REMÉDIATION :

1. Identifier tous les access packages avec des groupes supprimés
2. Supprimer les références invalides
3. Recréer les groupes si nécessaire ou remplacer par des groupes existants
4. Révoquer et réassigner les droits aux utilisateurs concernés

VALEUR PAR DÉFAUT :

Pas de validation — les groupes supprimés restent dans les access packages.

1.11.3 *Identifier les politiques d'access packages inactives ou orphelines* Moyen

Licence requise : Entra ID P2

DESCRIPTION :

Des politiques d'assignation d'access packages peuvent devenir "orphelines" si les conditions de déclenchement ne sont plus valides (groupe de portée supprimé, politique expirée). Ces politiques peuvent créer des assignations inattendues ou bloquer des demandes légitimes.

```
$assignments = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/identityGovernance/entitlementManagement/assignmentPoli
$assignments.value | Where-Object { $_.status -eq "inactive" -or $_.status -eq "disabled" } |
    Select-Object displayName, status, createdDateTime | Format-Table
```

REMÉDIATION :

1. Désactiver et supprimer les politiques inactives sans assignations actives
2. Documenter les politiques légitimement désactivées (maintenance planifiée)
3. Révision semestrielle de toutes les politiques d'access packages

VALEUR PAR DÉFAUT :

Politiques inactives conservées indéfiniment.

1.11.4 *Valider les approbateurs des workflows d'access packages* Élevé

Licence requise : Entra ID P2

DESCRIPTION :

Les workflows d'approbation des access packages peuvent référencer des utilisateurs qui ont quitté l'organisation ou dont le compte a été supprimé. Si l'approbateur n'existe plus, les demandes d'accès restent en attente indéfiniment ou passent sans approbation réelle.

```
# Vérifier les approbateurs valides dans les politiques d'access packages
$policies = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/identityGovernance/entitlementManagement/assignmentPolicie
foreach ($policy in $policies.value) {
    if ($policy.requestApprovalSettings.approvalStages) {
        foreach ($stage in $policy.requestApprovalSettings.approvalStages) {
            foreach ($approver in $stage.primaryApprovers) {
                if ($approver.objectType -eq "User") {
                    $user = Get-MgUser -UserId $approver.id -ErrorAction SilentlyContinue
                    if (-not $user -or $user.AccountEnabled -eq $false) {
                        Write-Host "⚠️ Policy: $($policy.displayName) — Approbateur invalide: $($approver.id)" -ForegroundColor Red
                    }
                }
            }
        }
    }
}
```

REMÉDIATION :

1. Identifier toutes les politiques avec des approbateurs invalides
2. Remplacer les approbateurs inexistants par des utilisateurs actifs
3. Préférer des groupes de sécurité comme approbateurs (plutôt que des individus)
4. Alerte automatique sur la désactivation d'un compte approbateur

VALEUR PAR DÉFAUT :

Aucune validation des approbateurs — les workflows peuvent bloquer silencieusement.

1.11.5 *Détecter les catalogues sans access packages associés* Faible

Licence requise : Entra ID P2

DESCRIPTION :

Des catalogues contenant des ressources mais sans access packages associés représentent des ressources "flottantes" qui ne peuvent pas être attribuées via le processus officiel de gouvernance. Ces ressources peuvent soit être des reliquats de configuration, soit des ressources qui devraient être accessibles mais ne le sont pas.

```
$catalogs = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/identityGovernance/entitlementManagement/catalogs" -Method
foreach ($catalog in $catalogs.value) {
    $packages = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/identityGovernance/entitlementManagement/accessPackage
    if ($packages.value.Count -eq 0) {
        $resources = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/identityGovernance/entitlementManagement/catalogs
        if ($resources.value.Count -gt 0) {
            Write-Host "⚠️ Catalogue '$($catalog.displayName)' a $($resources.value.Count) ressources mais aucun access package" -F
        }
    }
}
```

REMÉDIATION :

1. Créer des access packages pour les ressources dans des catalogues vides
2. Ou supprimer les ressources non gouvernées de ces catalogues
3. Supprimer les catalogues vides inutiles

VALEUR PAR DÉFAUT :

Aucune alerte — les catalogues sans access packages sont ignorés.

1.12 — Protection des Tokens et Sessions Avancées

1.12.1 *Activer la Protection des Tokens (Token Protection) pour Exchange, SharePoint et Teams* Critique

Licence requise : Entra ID P2 + appareils Entra Joined

DESCRIPTION :

La protection des tokens (Token Protection / Token Binding) lie cryptographiquement le token d'accès à l'appareil qui l'a obtenu. Sans cette protection, un attaquant ayant volé un access token (via AiTM, memory injection ou exfiltration réseau) peut le rejouer depuis n'importe quel autre appareil — c'est l'attaque **Pass-the-Token**. Avec Token Protection activé dans une politique CA, le token devient inutilisable en dehors de l'appareil d'origine car il est lié à la clé TPM.

```
# Vérifier les politiques CA avec Token Protection activé
$caPolicies = Get-MgIdentityConditionalAccessPolicy -All | Where-Object { $_.State -eq "enabled" }
$tokenProtected = $caPolicies | Where-Object {
    ($_.SessionControls | ConvertTo-Json -Depth 5) -match "tokenProtection|primaryRefreshToken"
}
if ($tokenProtected) {
    Write-Host "✅ Token Protection configuré : $($tokenProtected.DisplayName)" -ForegroundColor Green
} else {
    Write-Host "❌ Aucune politique CA avec Token Protection" -ForegroundColor Red
}
# Portail : Entra ID > Protection > Accès Conditionnel > créer politique > Session > Token Protection = Activé
```

REMÉDIATION :

1. Créer une politique CA : Applications cloud → Exchange Online, SharePoint Online, Teams
2. Session > Protection des tokens = **Activé**
3. Conditions : Appareils joints Entra ID ou conformes (requis pour le binding TPM)
4. Exclure les appareils sans TPM (anciens postes) en phase de déploiement progressif
5. Prioriser pour les comptes admin et utilisateurs sensibles en premier

VALEUR PAR DÉFAUT :

Token Protection désactivé — les tokens peuvent être rejoués depuis n'importe quel appareil.

1.12.2 *Activer les Actions Protégées (Protected Actions) pour les opérations Entra critiques* Critique

Licence requise : Entra ID P2

DESCRIPTION :

Les Actions Protégées (Protected Actions) exigent une ré-authentification fraîche (step-up MFA) avant d'exécuter des opérations Entra ID particulièrement sensibles, même si l'administrateur est déjà connecté avec une session valide. Un attaquant avec un token admin volé ne peut pas supprimer une politique CA, modifier les paramètres d'authentification ou assigner un rôle permanent sans déclencher un nouveau challenge MFA résistant au phishing.

Actions prioritaires à protéger : suppression de politiques CA, modification des paramètres fédérés, assignation de rôles permanents, modification de la liste des mots de passe interdits.

```
# Vérifier les actions protégées configurées dans les niveaux d'authentification
$authStrengths = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/policies/authenticationStrengthPolicies" -Method GET
$authStrengths.value | Select-Object displayName, policyType | Format-Table
# Via portail : Entra ID Admin Center > Protection > Actions protégées
# Vérifier que les opérations critiques nécessitent une force d'authentification phishing-resistant
```

REMÉDIATION :

1. Entra ID Admin Center > Protection > Actions protégées
2. Créer un groupe d'actions protégées : sélectionner les opérations critiques
3. Assigner la force d'authentification "Phishing-resistant MFA" (FIDO2 / Certificate-based)
4. Actions prioritaires à protéger :
5. Supprimer une politique d'accès conditionnel
6. Modifier les paramètres d'autorisation
7. Assigner des rôles PIM permanents
8. Modifier la fédération d'identité
9. Tester que la ré-authentification step-up est bien déclenchée

VALEUR PAR DÉFAUT :

Aucune action protégée configurée — les opérations sensibles n'exigent pas de step-up auth.

1.13 — Global Secure Access (Microsoft Entra Internet/Private Access)

1.13.1 *Déployer Microsoft Entra Internet Access (Secure Web Gateway cloud-natif)* Moyen

Licence requise : Entra Suite ou Microsoft 365 E5

DESCRIPTION :

Microsoft Entra Internet Access est un Secure Web Gateway (SWG) cloud-natif intégré à Entra ID. Il filtre le trafic Internet, applique les politiques CA au niveau réseau et implémente les Tenant Restrictions v2 sans proxy traditionnel. Cas d'usage critiques : bloquer l'accès aux tenants M365 non autorisés depuis les appareils d'entreprise (prévention de l'exfiltration via tenant personnel), filtrer les sites malveillants, surveiller le shadow IT.

AUDIT :

- Microsoft Entra Admin Center > Global Secure Access > Tableau de bord
- Vérifier le profil de transfert "Internet Access" et le nombre d'utilisateurs connectés
- Entra Admin Center > Global Secure Access > Trafic > Journaux réseau

REMÉDIATION :

1. Entra Admin Center > Global Secure Access > Démarrage > Activer Global Secure Access
2. Activer le profil de transfert de trafic "Internet Access"
3. Déployer le client Global Secure Access via Intune (Windows 10/11)
4. Configurer le filtrage de contenu web (catégories : malware, phishing, adulte, Shadow IT)
5. Activer la protection avancée contre les menaces web
6. Configurer Tenant Restrictions v2 via le profil Global Secure Access

VALEUR PAR DÉFAUT :

Non déployé — nécessite une activation et une licence spécifique.

1.13.2 *Remplacer le VPN traditionnel par Microsoft Entra Private Access (ZTNA)* Moyen

Licence requise : Entra Suite

DESCRIPTION :

Microsoft Entra Private Access est un Zero Trust Network Access (ZTNA) qui remplace le VPN en autorisant l'accès aux ressources privées on-premises (applications métier, fichiers réseau, serveurs) basé sur l'identité et la conformité de l'appareil — et non sur l'appartenance au réseau. Contrairement au VPN, il n'accorde pas l'accès à tout le réseau : seules les applications spécifiquement publiées sont accessibles, réduisant drastiquement le mouvement latéral possible en cas de compromission.

AUDIT :

- Entra Admin Center > Global Secure Access > Private Access
- Vérifier les Application Segments configurés et les connecteurs déployés

REMÉDIATION :

1. Entra Admin Center > Global Secure Access > Private Access
2. Créer des Application Segments pour chaque ressource interne (IP/FQDN + port)
3. Déployer des connecteurs Entra Private Access sur le réseau interne (Windows ou Linux)
4. Migrer progressivement les cas d'usage VPN vers Private Access
5. Appliquer des politiques CA : conformité appareil + MFA pour chaque accès

VALEUR PAR DÉFAUT :

Non déployé — VPN traditionnel sans contrôle d'identité granulaire.

1.14 — Lifecycle Workflows — Automatisation Joiner/Mover/Leaver

1.14.1 *Automatiser l'offboarding (Leaver) via Lifecycle Workflows Entra ID* Élevé

Licence requise : Entra ID Governance (P2)

DESCRIPTION :

Les Lifecycle Workflows automatisent les processus d'offboarding : désactivation du compte à J0, révocation des sessions actives, retrait des groupes sensibles, notification au manager, suppression différée. Sans cette automatisation, les offboardings manuels génèrent des comptes actifs plusieurs jours après le départ d'un employé et des accès non révoqués — source principale de comptes "zombies" exploitables.

```
# Lister les Lifecycle Workflows actifs de type Leaver
$workflows = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/identityGovernance/lifecycleWorkflows/workflows" -Method
$leaverWorkflows = $workflows.value | Where-Object { $_.category -eq "leaver" }
if ($leaverWorkflows) {
    $leaverWorkflows | Select-Object displayName, isEnabled, @{N="Tasks";E={$_.tasks.Count}} | Format-Table
    Write-Host "✅ $($leaverWorkflows.Count) workflow(s) Leaver configuré(s)" -ForegroundColor Green
} else {
    Write-Host "❌ Aucun Lifecycle Workflow Leaver configuré" -ForegroundColor Red
}
```

REMÉDIATION :

1. Entra ID Admin Center > Gouvernance des identités > Lifecycle Workflows
2. Créer un workflow "Leaver" avec les tâches ordonnées :
3. J0 : Désactiver le compte utilisateur
4. J0 : Révoquer toutes les sessions actives
5. J0 : Retirer des groupes sensibles
6. J0 : Envoyer notification au manager
7. J+7 : Supprimer les licences
8. J+30 : Supprimer le compte (ou J+90 selon politique RH)
9. Connecter à la date de départ via attribut `employeeLeaveDateTime`
10. Tester en mode simulation avant activation

VALEUR PAR DÉFAUT :

Aucun Lifecycle Workflow configuré — offboarding 100% manuel, risque de délai.

1.14.2 *Configurer les Lifecycle Workflows pour les Joiners (onboarding + TAP automatique)* Moyen

Licence requise : Entra ID Governance (P2)

DESCRIPTION :

Les workflows Joiner créent automatiquement un Temporary Access Pass (TAP) pour l'enrôlement MFA à J-1, assignent les licences selon le département et ajoutent l'utilisateur aux groupes appropriés. Sans automatisation, les délais d'onboarding et les erreurs d'assignation de droits sont fréquents. Le TAP automatique garantit que les nouveaux arrivants enrôlent une méthode MFA forte dès le premier jour sans passer par le helpdesk.

```
$workflows = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/identityGovernance/lifecycleWorkflows/workflows" -Method
$joinerWorkflows = $workflows.value | Where-Object { $_.category -eq "joiner" }
$joinerWorkflows | Select-Object displayName, isEnabled, @{N="Tasks";E={$_.tasks.Count}} | Format-Table
```

REMÉDIATION :

1. Créer un workflow "Joiner" déclenchant J-1 avant la date d'arrivée :
2. J-1 : Générer un TAP (valable 24h, utilisation unique)
3. J-1 : Envoyer email de bienvenue au manager avec le TAP
4. J0 : Assigner les licences selon le département
5. J0 : Ajouter aux groupes appropriés
6. Connecter à la date d'arrivée via attribut `employeeHireDate`
7. Activer la tâche "Activer le compte" uniquement le jour J (pas avant)

VALEUR PAR DÉFAUT :

Aucun workflow Joiner — provisioning 100% manuel.

1.15 — Unités Administratives et Délégation Granulaire

1.15.1 *Implémenter des Restricted Management AUs pour protéger les comptes critiques* Élevé

Licence requise : Entra ID P1

DESCRIPTION :

Les Unités Administratives Restreintes (Restricted Management Administrative Units) placent des comptes dans une "zone de protection maximale" : même les Global Administrators ne peuvent pas modifier les paramètres, réinitialiser les mots de passe ou désactiver les méthodes d'authentification des membres sans être gestionnaires de l'AU. C'est la protection la plus forte pour les comptes Break Glass, les comptes RSSI et les comptes SOC — un attaquant ayant compromis un Global Admin ne peut pas neutraliser ces comptes.

```
# Lister les Restricted Management AUs
$aus = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/directory/administrativeUnits?`$filter=isMemberManagementRestri
if ($aus.value.Count -gt 0) {
    Write-Host "✅ $($aus.value.Count) Restricted Management AU(s) configurée(s)" -ForegroundColor Green
    foreach ($au in $aus.value) {
        $members = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/directory/administrativeUnits/$($au.id)/members" -M
        Write-Host "  AU: $($au.displayName) — $($members.value.Count) membre(s) protégé(s)"
    }
} else {
    Write-Host "❌ Aucune Restricted Management AU — comptes critiques non protégés" -ForegroundColor Red
}
```

REMÉDIATION :

1. Entra ID Admin Center > Identité > Rôles et administrateurs > Unités administratives > Nouvelle AU
2. Activer `isMemberManagementRestricted = $true` (Portail ou API Graph)
3. Ajouter les membres à protéger : comptes Break Glass, compte RSSI, comptes SOC, SPs critiques
4. Désigner des gestionnaires de l'AU dédiés (distincts des GA standard)
5. Documenter qui peut gérer cette AU et les procédures d'accès d'urgence

VALEUR PAR DÉFAUT :

Aucune Restricted Management AU — tous les GA peuvent modifier tous les comptes sans restriction.

1.15.2 *Déléguer la gestion des utilisateurs par Unités Administratives sans droits globaux* Moyen

Licence requise : Entra ID P1

DESCRIPTION :

Les Unités Administratives permettent de déléguer la gestion des utilisateurs et des groupes par périmètre organisationnel (pays, département, filiale) sans accorder des droits sur l'ensemble du tenant. Un IT admin d'une filiale n'a besoin que de gérer les utilisateurs de sa filiale — pas d'un rôle global. Sans AUs, toute délégation nécessite un rôle tenant-wide avec surface d'attaque étendue.

```
$aus = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/directory/administrativeUnits" -Method GET
$aus.value | Select-Object displayName, description, membershipType | Format-Table
# Vérifier que les admins délégués n'ont PAS de rôles au niveau tenant
$scopedRoles = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/directory/administrativeUnits" -Method GET
```

REMÉDIATION :

1. Créer des AUs par département, filiale ou région géographique
2. Assigner le rôle "User Administrator" ou "Helpdesk Administrator" limité à l'AU (pas au tenant)
3. Révoquer les rôles globaux des administrateurs locaux qui n'en ont pas besoin
4. Configurer des AUs dynamiques si la structure est basée sur des attributs AD (`department`, `country`)

VALEUR PAR DÉFAUT :

Aucune AU configurée — délégation au niveau tenant uniquement.

1.16 — Santé, Recommandations et Conformité Entra ID

1.16.1 *Activer et traiter les Recommandations de Sécurité Entra ID*

Élevé

Licence requise : Entra ID P2

DESCRIPTION :

Microsoft Entra ID génère automatiquement des recommandations de sécurité personnalisées basées sur l'analyse en temps réel du tenant : "X utilisateurs admin sans MFA résistant au phishing", "X applications avec secrets expirés", "Per-user MFA encore actif pour Y comptes". Ces recommandations sont priorisées par impact. Les ignorer laisse des lacunes connues et documentées non traitées, ce qui constitue une faute de gestion en cas d'incident.

```
# Lister les recommandations actives haute priorité
$recommendations = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/directory/recommendations" -Method GET
$active = $recommendations.value | Where-Object { $_.status -notin @("completedBySystem","completedByUser","dismissed") }
Write-Host "Recommandations actives non traitées : $($active.Count)"
$active | Sort-Object priority | Select-Object displayName, status, priority, @{N="Impact";E={$_.impactedResources.Count}} | Format
# Résultat attendu : 0 recommandation haute priorité en statut actif
```

REMÉDIATION :

1. Entra ID Admin Center > Identité > Vue d'ensemble > Recommandations
2. Trier par priorité (Critique / Élevé)
3. Traiter chaque recommandation selon les instructions Microsoft intégrées
4. Recommandations non applicables : les "Ignorer" avec justification documentée
5. Révision mensuelle des nouvelles recommandations générées

VALEUR PAR DÉFAUT :

Recommandations générées mais aucune action automatique — elles restent actives indéfiniment.

1.16.2 *Surveiller la santé de la synchronisation Entra Connect (Connect Health)*

Élevé

Licence requise : Entra ID P1

Applicabilité : Environnements hybrides uniquement

DESCRIPTION :

Entra Connect Health surveille la santé des serveurs de synchronisation AD. Un problème non détecté peut entraîner : des comptes désactivés on-premises qui restent actifs dans le cloud (accès fantôme persistant), des mots de passe non synchronisés (écart AD/Entra exploitable), ou des groupes de sécurité incorrects. La latence de synchronisation > 30 minutes est souvent le premier signe d'une compromission de l'infrastructure hybride.

```
# Vérifier la latence de synchronisation via Graph
$syncState = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/directory/onPremisesSynchronization" -Method GET -ErrorAc
$syncState.value | Select-Object lastSyncDateTime, synchronizationClientErrorCount | Format-Table
# Via portail : Entra ID > Surveillance et santé > Entra Connect Health > Alertes actives
```

REMÉDIATION :

1. Installer l'agent Entra Connect Health sur tous les serveurs Entra Connect / Cloud Sync
2. Configurer des alertes email (SOC ou RSSI) pour les erreurs de synchronisation
3. Objectif : délai de synchronisation ≤ 30 minutes, 0 objets en quarantaine
4. Vérifier quotidiennement : erreurs d'exportation, objets en conflit, agents déconnectés
5. Configurer une alerte si la synchronisation s'arrête > 1 heure

VALEUR PAR DÉFAUT :

Connect Health doit être installé manuellement — aucune surveillance sans agent.

1.17 — PIM pour Groupes et Gestion des Comptes de Service

1.17.1 *Activer PIM pour les Groupes d'Accès Privilégiés (PIM for Groups)*

Élevé

Licence requise : Entra ID P2

DESCRIPTION :

PIM for Groups étend le contrôle Just-In-Time (JIT) au-delà des rôles Entra ID vers les **groupes de sécurité** : groupes donnant accès aux applications SaaS, aux ressources Azure, ou aux rôles personnalisés. Un groupe "Finance-Admins" donnant accès aux environnements de production financiers peut être géré via PIM — les membres ne sont actifs que lorsqu'ils ont besoin de cet accès, avec approbation et justification documentée. Les memberships permanents créent une surface d'attaque inutile.

```
# Lister les groupes gérés via PIM for Groups
$privilegedGroups = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/privilegedAccess/aadGroups/resources?`$filter=stat
Write-Host "Groupes gérés via PIM for Groups : $($privilegedGroups.value.Count)"
$privilegedGroups.value | Select-Object displayName, status | Format-Table

# Identifier les groupes candidats (avec app role assignments, non gérés par PIM)
Get-MgGroup -Filter "securityEnabled eq true" -All | ForEach-Object {
    $assignments = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/groups/$($_.Id)/appRoleAssignments" -Method GET
    if ($assignments.value.Count -gt 0) {
        [PSCustomObject]@{ Group = $_.DisplayName; AppRoles = $assignments.value.Count }
    }
} | Sort-Object AppRoles -Descending | Format-Table
```

REMÉDIATION :

1. Entra ID > Gestion des identités > Privileged Identity Management > Groupes
2. Identifier les groupes sensibles (accès applicatifs élevés, rôles custom, accès Azure)
3. "Gérer" → activer la gestion PIM pour ces groupes
4. Configurer : durée d'activation max = 4h, approbation requise, justification obligatoire
5. Convertir les membres permanents en membres "Éligibles"

VALEUR PAR DÉFAUT :

Groupes de sécurité sans contrôle JIT — memberships permanents par défaut.

1.17.2 *Migrer les comptes de service avec mots de passe vers Managed Identities ou Workload Federation* — Élevé

Licence requise : Entra ID Free + Azure

DESCRIPTION :

Les comptes de service avec mots de passe sont une cible privilégiée : mots de passe rarement changés, souvent exclus du MFA et des politiques CA, rarement surveillés. Microsoft recommande de migrer vers les **Managed Identities** (ressources Azure) ou les **Workload Identity Federations** (CI/CD et applications externes). Ces alternatives éliminent complètement les mots de passe — l'identité est cryptographiquement liée à la ressource, aucun secret ne peut être volé ou rejoué.

```
# Comptes utilisateurs ressemblant à des comptes de service actifs
Get-MgUser -All -Property "UserPrincipalName,DisplayName,SignInActivity,AccountEnabled" |
    Where-Object {
        ($_.UserPrincipalName -match "svc|service|bot|auto|system|app|api") -and
        $_.AccountEnabled -eq $true
    } | Select-Object UserPrincipalName, @{N="LastSignIn";E={$_.SignInActivity.LastSignInDateTime}} | Format-Table

# Service Principals avec password credentials à migrer
Get-MgServicePrincipal -All -Property "DisplayName,PasswordCredentials" |
    Where-Object { $_.PasswordCredentials.Count -gt 0 } |
    Select-Object DisplayName, @{N="NbSecrets";E={$_.PasswordCredentials.Count}},
        @{N="ExpirationLaPlusProche";E={($_.PasswordCredentials | Sort-Object EndDateTime | Select-Object -First 1).EndDateTime}} |
    Format-Table
```

REMÉDIATION :

1. Inventorier tous les comptes de service avec mots de passe et leur propriétaire
2. Migrer vers Managed Identity si ressource Azure (VM, Function App, Logic App)
3. Migrer vers Workload Identity Federation si CI/CD (GitHub Actions, Azure DevOps, GitLab)
4. Pour les cas impossibles à migrer : secret rotatif < 90j + exclusion CA documentée + alerte sur usage
5. Supprimer immédiatement les comptes de service inactifs depuis > 90 jours

VALEUR PAR DÉFAUT :

Aucune restriction — comptes de service avec mots de passe en persistance indéfinie.

1.18 — Workload Identity Federations et CI/CD Security

1.18.1 *Auditer les Federated Identity Credentials (OIDC) pour CI/CD* — Critique

Licence requise : Entra ID Free

DESCRIPTION :

Les Workload Identity Federations (GitHub Actions, Azure DevOps, GitLab, Kubernetes) permettent aux pipelines CI/CD de s'authentifier dans Entra ID via des tokens OIDC éphémères — sans secret stocké. C'est une excellente pratique, mais une mauvaise configuration (audience trop large, subject trop générique comme `repo:org/*`) permet à un attaquant ayant accès à n'importe quel repo de l'organisation d'obtenir un token valide vers le tenant M365. C'est un vecteur d'attaque supply chain critique en 2026.

```
# Lister toutes les Federated Identity Credentials configurées
$apps = Get-MgApplication -All -Property "displayName,federatedIdentityCredentials"
$apps | Where-Object { $_.FederatedIdentityCredentials.Count -gt 0 } | ForEach-Object {
    $app = $_
    $app.FederatedIdentityCredentials | ForEach-Object {
        [PSCustomObject]@{
            App      = $app.DisplayName
            Name     = $_.Name
            Issuer   = $_.Issuer
            Subject  = $_.Subject
            Audience = $_.Audiences -join ","
        }
    }
} | Format-Table
# Alertes : Subject contenant "*", "repo:org/*", ou audience non standard
```

REMÉDIATION :

1. Revoir chaque Federated Credential et vérifier que le Subject est précis (ex: `repo:org/repo:environment:prod`)
2. Supprimer les credentials avec Subject trop large (`*` ou `repo:org/*`)
3. Vérifier que l'Audience est `api://AzureADTokenExchange` uniquement
4. Limiter les permissions de l'App Registration associée au strict minimum
5. Documenter chaque Federated Credential avec son propriétaire et son use case

VALEUR PAR DÉFAUT :

Aucune validation des claims — Subject et Audience non contraints par défaut.

1.18.2 *Restreindre les permissions des App Registrations utilisées par les pipelines CI/CD* Élevé

Licence requise : Entra ID Free

DESCRIPTION :

Les App Registrations utilisées par les pipelines CI/CD (déploiement, tests automatisés, provisioning) accumulent souvent des permissions Graph élevées pour "simplifier" les workflows. Une pipeline compromise ou un token OIDC mal configuré peut alors exécuter des opérations critiques (créer des comptes, modifier des politiques CA, exfiltrer des données). Le principe du moindre privilège doit s'appliquer strictement aux identités CI/CD.

```
# Apps utilisées en CI/CD avec permissions Graph élevées
$dangerousPerms = @("Directory.ReadWrite.All","RoleManagement.ReadWrite.Directory","Application.ReadWrite.All","User.ReadWrite.All"
$apps = Get-MgApplication -All
foreach ($app in $apps) {
    $graphPerms = $app.RequiredResourceAccess |
        Where-Object { $_.ResourceAppId -eq "00000003-0000-0000-c000-000000000000" } |
        Select-Object -ExpandProperty ResourceAccess
    $high = $graphPerms | Where-Object { $_.Id -in $dangerousPerms }
    if ($high) {
        Write-Host "⚠️ $($app.DisplayName) — Permissions élevées : $($high.Id -join ', ')" -ForegroundColor Red
    }
}
```

REMÉDIATION :

1. Inventorier toutes les App Registrations liées aux pipelines CI/CD
2. Remplacer les permissions ReadWrite par des permissions ReadOnly si possible
3. Utiliser des rôles personnalisés Entra ID avec permissions minimales
4. Revoir trimestriellement les permissions des apps CI/CD avec le responsable DevOps

VALEUR PAR DÉFAUT :

Aucune restriction spécifique aux apps CI/CD — elles peuvent demander toutes les permissions.

Section 2 — MICROSOFT DEFENDER FOR OFFICE 365

2.1 — Politiques de Sécurité Prédéfinies (Preset Security Policies)

2.1.1 *Activer les politiques de sécurité Standard et Stricte*

Critique

DESCRIPTION :
Microsoft propose des politiques de sécurité prédéfinies (Standard et Stricte) qui regroupent en un seul clic toutes les configurations optimales anti-spam, anti-phishing, anti-malware, Safe Attachments et Safe Links, alignées sur les recommandations Microsoft. Elles simplifient la configuration et garantissent un niveau de protection cohérent. La politique Stricte doit s'appliquer aux utilisateurs les plus sensibles.

AUDIT :

- Portail Microsoft Defender > Email & Collaboration > Politiques > Politiques de sécurité prédéfinies
- Vérifier que Standard Protection et Strict Protection sont activées

REMÉDIATION :

1. Portail Defender > Email & Collaboration > Politiques & Règles > Stratégies contre les menaces > Stratégies de sécurité prédéfinies
2. Activer "Protection standard" → Assigner à : Tous les destinataires
3. Activer "Protection stricte" → Assigner à : Utilisateurs sensibles (Direction, Finance, RH, IT)
4. EOP (Exchange Online Protection) ET Defender for Office 365 doivent tous deux être configurés
5. La politique stricte prend la priorité sur la standard pour les utilisateurs des deux groupes

2.1.2 *Ajouter les comptes sensibles à la politique Stricte*

Critique

DESCRIPTION :
Les comptes des dirigeants, de la finance, des RH et du service IT sont les cibles prioritaires des attaques BEC, du spear phishing et des fraudes au président. Ces utilisateurs doivent bénéficier du niveau de protection le plus élevé (politique Stricte) avec toutes les protections contre l'usurpation d'identité activées.

AUDIT :

- Portail Defender > Politiques de sécurité prédéfinies > Protection stricte > Utilisateurs, groupes et domaines inclus

REMÉDIATION :

1. Dans la politique Stricte, ajouter explicitement :
2. Tous les membres de la direction (PDG, DAF, DRH, DSI, RSSI, etc.)
3. Tous les membres de l'équipe finance et comptabilité
4. Tous les administrateurs IT et sécurité
5. Tout utilisateur avec accès à des systèmes critiques
6. Créer un groupe Entra ID "Utilisateurs Protection Stricte" pour faciliter la gestion

2.2 — Protection Anti-Phishing

2.2.1 *Configurer les politiques Anti-Phishing*

Critique

Licence requise : Defender for Office 365 Plan 1 ou 2

DESCRIPTION :
Les attaques de phishing représentent le vecteur d'intrusion n°1 dans les organisations. Les politiques anti-phishing de Defender for Office 365 incluent la protection contre l'usurpation d'identité (impersonation) de domaines et d'utilisateurs clés, ainsi que des fonctionnalités d'intelligence sur les boîtes mail.

AUDIT :

- Portail Microsoft Defender > Email & Collaboration > Politiques > Anti-phishing
- Vérifier la politique par défaut et les politiques personnalisées
- PowerShell :

```
Get-AntiPhishPolicy | Select-Object Name, Enabled, PhishThresholdLevel, EnableTargetedUserProtection, EnableOrganizationDomainsProt
```

REMÉDIATION :

1. Niveau de seuil de phishing : 3 (Agressif) ou 2 (Standard) minimum
2. Activer la protection contre l'usurpation d'identité :
3. Utilisateurs protégés : PDG, DAF, DG, RSSI (ajouter adresses explicitement)
4. Domaines protégés : activer pour les domaines de l'organisation
5. Activer Mailbox Intelligence
6. Activer Mailbox Intelligence pour la protection contre l'usurpation d'identité
7. Action si usurpation détectée : Mettre en quarantaine

2.2.2 *Configurer DMARC, DKIM et SPF* — Critique

DESCRIPTION :
Ces trois protocoles d'authentification email forment un triple rempart contre l'usurpation d'identité (spoofing). SPF définit les serveurs autorisés à envoyer des emails pour le domaine. DKIM signe cryptographiquement les messages. DMARC définit la politique en cas d'échec SPF/DKIM et permet les rapports d'abus.

```
# Vérification SPF
Resolve-DnsName -Name "_spf.domaine.com" -Type TXT
# Vérification DKIM
Get-DkimSigningConfig | Select-Object Domain, Enabled, Status
# Vérification DMARC
Resolve-DnsName -Name "_dmarc.domaine.com" -Type TXT
```

AUDIT :
Ou utiliser : https://mxtoolbox.com/SuperTool.aspx

REMÉDIATION :

SPF :

```
v=spf1 include:spf.protection.outlook.com -all
```

REMÉDIATION :
(Le `-all` est obligatoire pour refuser tous les autres serveurs)

DKIM :

1. Exchange Admin Center > Email Authentication > DKIM
2. Activer DKIM pour chaque domaine
3. Publier les enregistrements CNAME fournis par Microsoft dans le DNS

DMARC :

```
v=DMARC1; p=reject; rua=mailto:dmarc-reports@domaine.com; ruf=mailto:dmarc-forensics@domaine.com; pct=100
```

REMÉDIATION :

- Commencer avec `p=none` pour observer, puis `p=quarantine`, puis `p=reject`

2.2.3 *Activer la Protection contre l'usurpation (Anti-Spoofing)* — Critique

DESCRIPTION :
L'anti-spoofing empêche les emails qui semblent provenir de domaines internes mais qui arrivent de sources externes non autorisées. C'est une protection critique contre les attaques BEC.

```
Get-AntiPhishPolicy | Select-Object Name, EnableSpoofIntelligence, AuthenticationFailAction
```

REMÉDIATION :

1. Activer Spoof Intelligence dans les politiques anti-phishing
2. Action en cas de spoofing détecté : Déplacer en dossier Courrier indésirable ou Mettre en quarantaine
3. Réviser régulièrement le tableau de bord Spoof Intelligence pour valider/bloquer les expéditeurs légitimes

2.3 — Protection Anti-Malware et Safe Attachments

2.3.1 *Activer Safe Attachments* — Critique

Licence requise : Defender for Office 365 Plan 1

MITRE ATT&CK : T1566.001 (Phishing: Spearphishing Attachment) · T1204.002 (User Execution: Malicious File) · T1027 (Obfuscated Files or Information)

DESCRIPTION :
Safe Attachments ouvre les pièces jointes dans un environnement sandbox isolé avant de les livrer à l'utilisateur. Cette protection est essentielle contre les malwares zero-day qui n'ont pas encore de signature antivirus connue.

```
Get-SafeAttachmentPolicy | Select-Object Name, Enable, Action, Redirect, RedirectAddress
```

REMÉDIATION :

1. Portail Defender > Email & Collaboration > Politiques > Safe Attachments
2. Activer Safe Attachments pour tous les domaines
3. Action : Bloquer (Block) — les pièces jointes malveillantes sont bloquées
4. Activer Safe Attachments pour SharePoint, OneDrive et Teams
5. Activer le rapport de malwares en temps réel

2.3.2 *Activer Safe Links* — Critique

Licence requise : Defender for Office 365 Plan 1

DESCRIPTION :
Safe Links réécrit les URLs dans les emails et les documents Office pour passer par le service de vérification Microsoft au moment du clic. Cela protège contre les liens malveillants, même ceux qui deviennent malveillants après la livraison de l'email (time-of-click protection).

```
Get-SafeLinksPolicy | Select-Object Name, IsEnabled, EnableForInternalSenders, EnableSafeLinksForTeams, TrackClicks, AllowClickThro
```

REMÉDIATION :

1. Activer Safe Links pour tous les domaines et utilisateurs
2. Activer Safe Links pour les applications Office 365
3. Activer Safe Links pour Teams
4. AllowClickThrough : Désactivé (l'utilisateur ne peut pas bypasser l'alerte)
5. TrackClicks : Activé (pour les rapports)
6. Ne PAS utiliser de liste d'exclusion (Do not rewrite URLs list) sauf exception justifiée

2.3.3 *Configurer la politique Anti-Malware avec types de fichiers étendus* — Élevé

DESCRIPTION :
La politique anti-malware standard de M365 peut être renforcée pour bloquer proactivement les types de fichiers à haut risque (.exe, .ps1, .vbs, .bat, .js, etc.) même sans signature malware connue.

```
Get-MalwareFilterPolicy | Select-Object Name, EnableFileFilter, FileTypes
```

REMÉDIATION :

1. Exchange Admin Center > Protection > Filtre anti-programme malveillant
2. Activer le filtrage des types de fichiers courants
3. Types de fichiers à bloquer minimums : .exe, .dll, .ps1, .vbs, .bat, .cmd, .com, .js, .jar, .wsf, .msi
4. Configurer des notifications à l'administrateur pour les pièces jointes bloquées

2.4 — Protection contre le Spam

2.4.1 *Configurer les politiques Anti-Spam* — Élevé

DESCRIPTION :
Les emails de spam sont souvent le vecteur initial des campagnes de phishing et d'infection par malware. Une politique anti-spam bien configurée réduit significativement l'exposition des utilisateurs.

```
Get-HostedContentFilterPolicy | Select-Object Name, SpamAction, HighConfidenceSpamAction, PhishSpamAction, BulkSpamAction, BulkThre
```

REMÉDIATION :

1. Spam Action : Mettre en quarantaine (recommandé) ou Dossier Courrier indésirable
2. High Confidence Spam : Mettre en quarantaine
3. Phish : Mettre en quarantaine
4. Bulk Email : Seuil BCL ≤ 6 (niveau 4-5 recommandé pour organisations sensibles)
5. Activer les rapports de spam pour les utilisateurs (pour signalement)

2.4.2 *Configurer l'impersonation utilisateurs ciblés (Targeted User Impersonation Protection)* — Élevé

Licence requise : Microsoft Defender for Office 365 Plan 1

DESCRIPTION :
La protection contre l'usurpation d'identité ciblée (user impersonation) protège les comptes à haut risque (dirigeants, finances, IT) contre les emails qui imitent leur adresse ou leur nom. Un email qui semble venir du PDG mais utilise un domaine légèrement différent (ex: `ceo@contoso-corp.com`) peut tromper les collaborateurs. Cette protection doit être configurée pour les comptes sensibles dans la politique anti-phishing.

```
# Vérifier la protection impersonation dans les politiques anti-phishing
Get-AntiPhishPolicy | Select-Object Name, EnableTargetedUserProtection, TargetedUsersToProtect, TargetedUserProtectionAction | Form
# Résultat attendu : EnableTargetedUserProtection = True, TargetedUsersToProtect contient les comptes sensibles
```

REMÉDIATION :

1. Portail Defender > Email & Collaboration > Politiques > Anti-phishing
2. Modifier la politique Stricte ou créer une politique dédiée VIP
3. Section "Impersonation" > Activer "Activer la protection des utilisateurs"
4. Ajouter : CEO, CFO, RSSI, DRH, responsables financiers, admins IT
5. Action : Déplacer vers quarantaine (pas juste ajouter un conseil de sécurité)

```
Set-AntiPhishPolicy -Identity "Default" `
    -EnableTargetedUserProtection $true `
    -TargetedUsersToProtect @("ceo@contoso.com","cfo@contoso.com") `
    -TargetedUserProtectionAction Quarantine
```

VALEUR PAR DÉFAUT :
Protection impersonation ciblée désactivée.

2.4.3 *Configurer l'impersonation domaines owned et partenaires clés* Élevé

Licence requise : Microsoft Defender for Office 365 Plan 1

DESCRIPTION :

En complément de l'impersonation utilisateur, la protection d'impersonation de domaine protège contre les emails qui imitent vos domaines owned (ex: `contoso-corp.com` au lieu de `contoso.com`) et les domaines de vos partenaires/fournisseurs clés. C'est une couche de protection supplémentaire contre le Business Email Compromise (BEC).

```
Get-AntiPhishPolicy | Select-Object Name, EnableTargetedDomainsProtection, TargetedDomainsToProtect, EnableOrganizationDomainsProte
# Résultat attendu : EnableOrganizationDomainsProtection = True (domaines owned)
# TargetedDomainsToProtect = liste des domaines partenaires
```

```
Set-AntiPhishPolicy -Identity "Default" `
    -EnableOrganizationDomainsProtection $true `
    -EnableTargetedDomainsProtection $true `
    -TargetedDomainsToProtect @("partner1.com","supplier.com") `
    -TargetedDomainProtectionAction Quarantine
```

VALEUR PAR DÉFAUT :

Protection impersonation domaine désactivée.

2.4.4 *Activer ZAP (Zero-Hour Auto Purge) pour Microsoft Teams* Moyen

Licence requise : Microsoft Defender for Office 365 Plan 1

DESCRIPTION :

Le ZAP (Zero-Hour Auto Purge) pour Teams détecte et supprime automatiquement les messages malveillants envoyés dans Teams après leur délivrance. C'est le pendant du ZAP email pour Teams — si un fichier malveillant est détecté après partage dans un canal, il est automatiquement mis en quarantaine.

```
# Vérifier ZAP pour Teams
$atpPolicy = Get-AtpPolicyForO365
$atpPolicy | Select-Object Name, ZapEnabled, EnableATPForSPOTeamsODB | Format-List
# ZapEnabled doit être True
```

```
Set-AtpPolicyForO365 -EnableATPForSPOTeamsODB $true -ZapEnabled $true
```

REMÉDIATION :

- Portail Defender > Email & Collaboration > Paramètres > Paramètres Microsoft Teams > ZAP pour Teams

VALEUR PAR DÉFAUT :

ZAP Teams désactivé sur les anciens tenants.

2.4.5 *Configurer la DLP avec un périmètre complet (EXO + OD + SPO + Teams + Devices)* Élevé

Licence requise : Microsoft 365 E3 + Purview DLP

DESCRIPTION :

Une politique DLP doit couvrir l'ensemble des services M365 simultanément pour être efficace. Si seul Exchange est couvert, un utilisateur peut exfiltrer des données via Teams ou SharePoint. Le périmètre minimum recommandé par CISA inclut : Exchange, OneDrive, SharePoint, Teams ET les appareils (endpoint DLP).

```
Connect-IPPSSession
$dlpPolicies = Get-DlpCompliancePolicy | Where-Object { $_.Mode -eq "Enable" }
foreach ($policy in $dlpPolicies) {
    $locations = @()
    if ($policy.ExchangeLocation.Count -gt 0) { $locations += "Exchange" }
    if ($policy.SharePointLocation.Count -gt 0) { $locations += "SharePoint" }
    if ($policy.OneDriveLocation.Count -gt 0) { $locations += "OneDrive" }
    if ($policy.TeamsLocation.Count -gt 0) { $locations += "Teams" }
    if ($policy.EndpointDlpLocation.Count -gt 0) { $locations += "Devices" }
    Write-Host "$($policy.Name): $($locations -join ', ')"
}
# Résultat attendu : au moins une politique couvre les 5 locations
```

REMÉDIATION :

1. Microsoft Purview > Prévention des pertes de données > Modifier la politique existante
2. Étendre l'emplacement à : Exchange + SharePoint + OneDrive + Teams + Appareils
3. Vérifier que les règles existantes s'appliquent à tous les emplacements ajoutés

VALEUR PAR DÉFAUT :

DLP souvent configuré uniquement pour Exchange.

Section 3 — EXCHANGE ONLINE ET MESSAGERIE

3.1 — Configuration de la Messagerie

3.1.1 *Désactiver le transfert automatique des emails vers des domaines externes* — Critique

MITRE ATT&CK : T1114.003 (Email Collection: Email Forwarding Rule) · T1048 (Exfiltration Over Alternative Protocol) · T1567 (Exfiltration Over Web Service)

DESCRIPTION :

Le transfert automatique d'emails est l'une des techniques les plus utilisées par les attaquants après compromission d'un compte. L'attaquant configure un transfert silencieux vers sa propre boîte mail pour exfiltrer durablement les communications de l'organisation.

```
Get-TransportRule | Where-Object {$_.RedirectMessageTo -ne $null -or $_.BlindCopyTo -ne $null} | Select-Object Name, RedirectMessag
Get-RemoteDomain | Select-Object DomainName, AutoForwardEnabled
Get-HostedOutboundSpamFilterPolicy | Select-Object AutoForwardingMode
```

REMÉDIATION :

1. Politique de spam sortant : AutoForwardingMode = Off
2. Remote Domain (domaine par défaut) : AutoForwardEnabled = False
3. Créer une règle de transport pour bloquer les transferts automatiques :
4. Condition : Le message a les propriétés → Définir l'en-tête "X-MS-Exchange-Inbox-Rules-Loop"
5. Action : Rejeter avec message "Le transfert automatique d'emails vers des domaines externes est interdit"
6. Créer une alerte pour détecter les règles de boîte mail créant des transferts

3.1.2 *Activer l'audit de la boîte mail (Mailbox Auditing)* — Élevé

DESCRIPTION :

L'audit des boîtes mail enregistre les actions effectuées sur les emails (lecture, suppression, transfert, accès délégué). Ces journaux sont essentiels pour les investigations forensics après incident et la détection d'accès non autorisés.

```
Get-OrganizationConfig | Select-Object AuditDisabled
Get-Mailbox -ResultSize Unlimited | Where-Object {$_.AuditEnabled -eq $false} | Select-Object UserPrincipalName, AuditEnabled
```

REMÉDIATION :

1. Activer l'audit global :

```
Set-OrganizationConfig -AuditDisabled $false
```

REMÉDIATION :

1. Pour les boîtes mail non auditées :

```
Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditEnabled $true -AuditAdmin Update,Copy,Move,MoveToDeletedItems,SoftDelete,Hard
```

REMÉDIATION :

1. Durée de rétention des journaux : 90 jours minimum (365 jours recommandé)

3.1.3 *Désactiver SMTP AUTH au niveau de l'organisation* — Élevé

DESCRIPTION :

SMTP AUTH (port 587 avec authentification basique) ne supporte pas le MFA et est souvent utilisé par des malwares ou des attaquants ayant compromis des credentials. Sa désactivation globale force les applications à utiliser OAuth 2.0.

```
Get-TransportConfig | Select-Object SmtpClientAuthenticationDisabled
Get-CASMailbox -ResultSize Unlimited | Where-Object {$_.SmtpClientAuthenticationDisabled -eq $false} | Select-Object UserPrincipalN
```

REMÉDIATION :

1. Désactiver SMTP AUTH globalement :

```
Set-TransportConfig -SmtpClientAuthenticationDisabled $true
```

REMÉDIATION :

1. Pour les applications nécessitant SMTP AUTH (imprimantes, systèmes legacy) :
2. Créer un compte dédié avec SMTP AUTH activé uniquement pour ce compte
3. Restreindre l'envoi à un seul destinataire ou groupe
4. Surveiller l'activité de ce compte
5. Migrer vers Microsoft Graph API pour l'envoi programmatique d'emails

3.1.4 *Configurer les connexions sécurisées TLS pour les emails entrants* — Moyen

DESCRIPTION :

Forcer le TLS pour les communications email entrant depuis les partenaires commerciaux clés protège contre l'interception des emails en transit (man-in-the-middle).

```
Get-ReceiveConnector | Select-Object Name, RequireTLS, TLSCertificateName
Get-TransportConfig | Select-Object TLSReceiveDomainSecureList, TLSSendDomainSecureList
```

REMÉDIATION :

1. Pour les partenaires critiques : configurer des connecteurs avec TLS obligatoire et vérification de certificat
2. Exchange Admin Center > Flux de messagerie > Connecteurs
3. Activer MTA-STS (Mail Transfer Agent Strict Transport Security) pour le domaine

3.1.5 *Désactiver les protocoles POP3 et IMAP4* — Élevé

DESCRIPTION :
POP3 et IMAP4 utilisent l'authentification basique qui ne supporte pas le MFA. Ces protocoles hérités doivent être désactivés sauf nécessité absolue documentée.

```
Get-CASMailboxPlan | Select-Object DisplayName, PopEnabled, ImapEnabled
Get-CASMailbox -ResultSize Unlimited | Where-Object {$_.PopEnabled -eq $true -or $_.ImapEnabled -eq $true} | Select-Object UserPrin
```

```
Set-CASMailboxPlan -Identity ExchangeOnlineEnterprise -PopEnabled $false -ImapEnabled $false
Get-CASMailbox -ResultSize Unlimited | Set-CASMailbox -PopEnabled $false -ImapEnabled $false
```

3.1.6 *Implémenter les avertissements d'expéditeur externe* — Élevé

DESCRIPTION :
Signaler visuellement les emails provenant de l'extérieur de l'organisation réduit le risque de phishing interne (usurpation d'identité d'un collègue ou d'un dirigeant). Un utilisateur averti qu'il reçoit un email externe sera plus méfiant avant de cliquer sur un lien ou ouvrir une pièce jointe.

```
Get-TransportRule | Where-Object {$_.Name -like "*external*" -or $_.PrependSubject -like "*[Externe]*"} | Select-Object Name, State
```

REMÉDIATION :
1. Exchange Admin Center > Règles de flux de messagerie > Créer une règle
2. Condition : "L'expéditeur se trouve" → À l'extérieur de l'organisation
3. ET : "Le destinataire se trouve" → À l'intérieur de l'organisation
4. Action : Insérer une clause d'exclusion de responsabilité → `⚠️ ATTENTION : Cet email provient d'un expéditeur externe à l'organisation.`
5. Ou : Ajouter le préfixe `[EXTERNE]` au sujet de l'email
6. Exception : Exclure les domaines partenaires connus si souhaité (pour éviter la lassitude des utilisateurs)

3.1.7 *Désactiver les listes d'autorisation IP dans les politiques anti-spam* — Élevé

DESCRIPTION :
Les listes d'autorisation d'adresses IP dans les politiques anti-spam font passer les emails de ces IPs sans aucun filtrage de spam, phishing ou malware. Ces IPs peuvent changer de propriétaire, être compromises, ou être utilisées pour du "trusted sender abuse". Les listes "safe" (expéditeurs approuvés) ont le même problème.

```
# Vérifier la liste blanche IP dans la politique de filtre de connexion
Get-HostedConnectionFilterPolicy | Select-Object Name, IPAllowList, EnableSafeList
```

REMÉDIATION :
1. Portail Defender > Email & Collaboration > Politiques > Anti-spam > Politique de filtre de connexion
2. IPAllowList : Supprimer toutes les entrées
3. EnableSafeList : Désactiver
4. Si des IPs doivent être autorisées pour des raisons légitimes : utiliser les règles de transport avec filtrage maintenu plutôt que l'bypass total

3.1.8 *Activer la purge automatique Zero-Hour (ZAP)* — Élevé

DESCRIPTION :
ZAP (Zero-Hour Auto Purge) permet à Microsoft Defender de reclassifier et retirer des boîtes mail des emails qui ont été initialement livrés mais reconnus ultérieurement comme malveillants (malware, phishing). Cette protection post-livraison est essentielle car les IOCs de nouveaux malwares peuvent n'être disponibles qu'après la livraison initiale.

```
Get-HostedContentFilterPolicy | Select-Object Name, ZapEnabled
Get-MalwareFilterPolicy | Select-Object Name, ZapEnabled
```

REMÉDIATION :
1. Portail Defender > Email & Collaboration > Politiques > Anti-spam
2. ZAP pour les spams : Activé
3. ZAP pour le phishing : Activé
4. Anti-malware : ZAP également activé par défaut, vérifier qu'il n'a pas été désactivé

3.1.9 *Ne pas ajouter de domaines dans les listes d'autorisation anti-spam* — Critique

DESCRIPTION :
Ajouter des domaines entiers en liste blanche anti-spam est extrêmement dangereux : tout email prétendant venir de ce domaine (y compris des spoofs) passera le filtrage. Même les domaines partenaires de confiance ne doivent pas être en liste blanche, car ils peuvent être compromis et utilisés pour envoyer des spams ou du phishing vers l'organisation.

```
Get-HostedContentFilterPolicy | Select-Object Name, AllowedSenderDomains
```

AUDIT :
Doit retourner : vide / aucune entrée

REMÉDIATION :
1. Portail Defender > Email & Collaboration > Politiques > Anti-spam
2. Dans chaque politique > Expéditeurs autorisés et domaines autorisés → Supprimer tous les domaines autorisés
3. Pour les partenaires légitimes qui rencontrent des faux positifs : utiliser des règles de transport ciblées ou des connecteurs entrants avec TLS, plutôt qu'une liste blanche

3.1.10 *Activer le chiffrement des emails sensibles (OME)* Moyen

Licence requise : Microsoft 365 E3 ou supérieur

DESCRIPTION :

Office Message Encryption (OME) chiffre automatiquement les emails contenant des informations sensibles (données personnelles, financières, médicales) pour protéger leur contenu en cas d'interception ou d'envoi à un mauvais destinataire.

```
Get-OMEConfiguration | Select-Object Identity, OTPEnabled, SocialIdSignIn
Get-TransportRule | Where-Object {$_.ApplyRightsProtectionTemplate -ne $null} | Select-Object Name
```

REMÉDIATION :

1. Activer Azure Information Protection (AIP)
2. Créer des règles de transport pour le chiffrement automatique basé sur des mots clés ou classifications de données
3. Former les utilisateurs à l'utilisation du chiffrement manuel

3.1.11 *Valider DMARC p=reject (pas seulement p=none)* Critique

Licence requise : Entra ID Free (DNS public)

DESCRIPTION :

Avoir un enregistrement DMARC avec `p=none` signifie uniquement **monitoring** — les emails qui échouent DMARC sont quand même délivrés. Ce n'est PAS une protection. Seul `p=reject` (ou `p=quarantine` comme étape transitoire) protège contre l'usurpation de domaine. La grande majorité des organisations ont `p=none` et croient être protégées.

```
# Vérifier DMARC pour tous les domaines acceptés
$acceptedDomains = Get-AcceptedDomain
foreach ($domain in $acceptedDomains.DomainName) {
    try {
        $dmarc = Resolve-DnsName -Name "_dmarc.$domain" -Type TXT -ErrorAction Stop
        $dmarcRecord = ($dmarc.Strings | Where-Object { $_ -like "v=DMARC1*" }) -join ""
        $policy = if ($dmarcRecord -match "p=(\w+)") { $Matches[1] } else { "ABSENT" }
        $color = if ($policy -eq "reject") { "Green" } elseif ($policy -eq "quarantine") { "Yellow" } else { "Red" }
        Write-Host "$domain : p=$policy" -ForegroundColor $color
    } catch { Write-Host "$domain : DMARC ABSENT" -ForegroundColor Red }
}
```

AUDIT :

Résultat attendu : `p=reject` pour tous les domaines (ou `p=quarantine` comme étape de transition documentée)

REMÉDIATION :

1. Démarrer avec `p=none` + `rua=mailto:dmarc-reports@votre-domaine.com` pour collecter les rapports
2. Analyser les rapports (outil : DMARC Analyzer, dmarcian, Valimail)
3. Passer à `p=quarantine` après validation (0% de faux positifs)
4. Passer à `p=reject` une fois stable
5. `_dmarc.contoso.com TXT "v=DMARC1; p=reject; rua=mailto:dmarc@contoso.com; ruf=mailto:dmarc@contoso.com; pct=100"`

VALEUR PAR DÉFAUT :

DMARC souvent absent ou `p=none` — aucune protection réelle.

3.1.12 *Valider SPF avec hard fail (-all) et non soft fail (~all)* Élevé

DESCRIPTION :

Un enregistrement SPF avec `~all` (soft fail / tilde) indique aux serveurs destinataires que les emails hors périmètre sont "suspects mais pas rejetés" — ils sont souvent quand même délivrés. Seul `-all` (hard fail / tiret) indique un rejet. La grande majorité des organisations utilisent `~all` par précaution, laissant le spoofing possible.

```
$acceptedDomains = Get-AcceptedDomain
foreach ($domain in $acceptedDomains.DomainName) {
    try {
        $spf = Resolve-DnsName -Name $domain -Type TXT -ErrorAction Stop
        $spfRecord = ($spf.Strings | Where-Object { $_ -like "v=spf1*" }) -join ""
        if ($spfRecord -match "-all") { Write-Host "✅ $domain : SPF hard fail (-all)" -ForegroundColor Green }
        elseif ($spfRecord -match "~all") { Write-Host "⚠️ $domain : SPF soft fail (~all) — protection incomplète" -ForegroundColor
        else { Write-Host "❌ $domain : SPF absent ou mal configuré" -ForegroundColor Red }
    } catch { Write-Host "❌ $domain : Erreur DNS" -ForegroundColor Red }
}
```

REMÉDIATION :

1. Identifier tous les serveurs légitimes d'envoi d'emails pour votre domaine
2. Lister les IPs/services autorisés dans le SPF (include:, ip4:, ip6:)
3. Remplacer `~all` par `-all` dans tous les enregistrements SPF
4. Tester avec des outils SPF checker avant publication

VALEUR PAR DÉFAUT :

`~all` (soft fail) — souvent utilisé pour éviter les faux positifs.

3.1.13 *Vérifier les 7 alertes obligatoires Microsoft (MS.EXO.16.1)* Élevé

Licence requise : Microsoft 365 E3

DESCRIPTION :

La CISA exige que 7 alertes spécifiques soient activées et configurées pour envoyer des notifications. Ces alertes couvrent les événements de sécurité les plus critiques : détection de malware, activités suspectes dans la boîte mail, connexions depuis des pays inhabituels, etc.

```
Connect-IPPSSession
$requiredAlerts = @(
    "Email messages containing malware removed after delivery",
    "Email messages containing phish URLs removed after delivery",
    "Email reported by user as malware or phish",
    "Suspicious email sending patterns detected",
    "Unusual increase in email reported as phish",
    "Messages have been delayed",
    "Tenant restricted from sending email"
)
$existingAlerts = Get-ProtectionAlert | Where-Object { $_.IsSystemPolicy -eq $false -or $_.Disabled -eq $false }
foreach ($required in $requiredAlerts) {
    $found = $existingAlerts | Where-Object { $_.Name -like "*$required*" -and -not $_.Disabled }
    Write-Host "$(if($found){'✅'}else{'❌'}) $required"
}
```

REMÉDIATION :

1. Microsoft Purview > Alertes > Gérer les politiques d'alerte
2. Vérifier que les 7 alertes CISA sont activées avec notifications email
3. Configurer les notifications vers une adresse surveillée (SOC, équipe sécurité)
4. Les alertes doivent être envoyées vers un SIEM ou une adresse monitored H24

VALEUR PAR DÉFAUT :

Certaines alertes système activées, mais pas nécessairement les 7 requises.

3.1.14 *Activer les conseils de sécurité "First Contact" et Mailbox Intelligence* Moyen

Licence requise : Microsoft Defender for Office 365 Plan 1

DESCRIPTION :

Les conseils de sécurité "First Contact" alertent l'utilisateur lorsqu'il reçoit pour la première fois un email d'un expéditeur. La Mailbox Intelligence utilise l'IA pour identifier les expéditeurs inhabituels. Ces deux fonctionnalités réduisent significativement le risque de BEC et de phishing en alertant l'utilisateur avant qu'il ne réponde ou clique.

```
Get-AntiPhishPolicy | Select-Object Name, EnableFirstContactSafetyTips, EnableMailboxIntelligence, EnableMailboxIntelligenceProtect
# Résultat attendu : EnableFirstContactSafetyTips = True, EnableMailboxIntelligence = True
```

```
Set-AntiPhishPolicy -Identity "Default" `
    -EnableFirstContactSafetyTips $true `
    -EnableMailboxIntelligence $true `
    -EnableMailboxIntelligenceProtection $true `
    -MailboxIntelligenceProtectionAction MoveToJmf
```

VALEUR PAR DÉFAUT :

First Contact Safety Tips désactivé, Mailbox Intelligence activé mais sans protection.

3.1.15 *Bloquer les règles de transport bypass pour la simulation de phishing (PhishSim)* Élevé

Licence requise : Microsoft Defender for Office 365 Plan 2

DESCRIPTION :

Les règles de transport créées pour contourner Safe Attachments/Safe Links lors de simulations de phishing (Attack Simulator) utilisent souvent des IPs ou des domaines de prestataires. Si ces IPs/domaines sont connus, un vrai attaquant peut les usurper pour que ses emails passent dans les règles de bypass. Ces règles doivent être limitées aux IPs légitimes du prestataire de simulation et révisées régulièrement.

```
# Identifier les règles qui bypassent Safe Attachments ou Safe Links
Get-TransportRule | Where-Object {
    $_.SetHeaderName -eq "X-MS-Exchange-Organization-SkipSafeAttachmentProcessing" -or
    $_.SetHeaderName -eq "X-MS-Exchange-Organization-SkipSafeLinksProcessing" -or
    $_.SetSCL -eq -1
} | Select-Object Name, State, Conditions, SetHeaderName | Format-List
```

REMÉDIATION :

1. Identifier toutes les règles bypass Safe Attachments/Safe Links
2. Vérifier qu'elles sont uniquement liées à des IPs de prestataires de simulation connus
3. Supprimer les règles inutilisées ou génériques (conditions trop larges)
4. Utiliser la fonctionnalité native "Attack Simulation Training" de Microsoft qui ne nécessite pas de règles de transport

VALEUR PAR DÉFAUT :

Les règles bypass sont créées manuellement — aucune restriction par défaut.

3.1.16 *Configurer ARC (Authenticated Received Chain) pour les flux d'emails complexes* Moyen

Licence requise : Exchange Online

DESCRIPTION :

ARC (Authenticated Received Chain) préserve les résultats d'authentification email (SPF/DKIM/DMARC) lorsque les emails transitent par des intermédiaires légitimes (filtres anti-spam tiers, services de routage). Sans ARC, les emails légitimes réacheminés peuvent échouer DMARC et être rejetés ou marqués comme spam.

```
# Vérifier les sealers ARC de confiance configurés
Get-ArcConfig | Format-List
# Ou via :
Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/admin/edge/internetExplorerMode/siteLists" -Method GET -ErrorAction Si
Get-TransportConfig | Select-Object ArcTrustedSealers
```

REMÉDIATION :

1. Exchange Admin Center > Mail flow > Paramètres ARC
2. Ajouter les domaines des intermédiaires légitimes comme ARC sealers de confiance
3. Vérifier régulièrement les rapports DMARC pour identifier les échecs liés au réacheminement

VALEUR PAR DÉFAUT :

Aucun ARC sealer de confiance configuré.

3.1.17 *Auditer les délégations de boîte mail (Send As, Full Access, Send on Behalf)* Élevé

Licence requise : Exchange Online

DESCRIPTION :

Les délégations de boîte mail (`Full Access`, `Send As`, `Send on Behalf`) accordent à d'autres utilisateurs des droits d'accès complets à une boîte mail. Ces délégations s'accumulent dans le temps et sont rarement révoquées. Un attaquant qui compromet un compte avec délégation sur une boîte VIP peut envoyer des emails au nom du dirigeant ou lire tous ses emails en toute discrétion.

```
# Audit complet des délégations Send As
Get-Mailbox -ResultSize Unlimited | ForEach-Object {
    $mbx = $_
    $sendAs = Get-RecipientPermission -Identity $mbx.Identity -AccessRights SendAs | Where-Object { $_.Trustee -ne "NT AUTHORITY\SE
    $fullAccess = Get-MailboxPermission -Identity $mbx.Identity | Where-Object { $_.AccessRights -contains "FullAccess" -and $_.Use
    if ($sendAs -or $fullAccess) {
        Write-Host "📬 $($mbx.DisplayName)" -ForegroundColor Yellow
        $sendAs | ForEach-Object { Write-Host "  Send As: $($_.Trustee)" }
        $fullAccess | ForEach-Object { Write-Host "  Full Access: $($_.User)" }
    }
}
```

REMÉDIATION :

1. Inventorier toutes les délégations actives
2. Supprimer les délégations non justifiées ou liées à d'anciens employés
3. Documenter les délégations légitimes (assistants direction, secrétariats)
4. Révision semestrielle des délégations

VALEUR PAR DÉFAUT :

Délégations accumulées sans révision périodique.

3.2 — Gestion des Calendriers et du Partage

3.2.1 *Restreindre le partage de calendriers avec des domaines externes* Moyen

DESCRIPTION :

Un calendrier partagé avec des domaines externes peut révéler des informations sensibles : présence/absence des dirigeants, sujets de réunions confidentielles, participants à des négociations stratégiques.

```
Get-SharingPolicy | Select-Object Name, Enabled, Domains
```

REMÉDIATION :

1. Restreindre le partage à "Disponibilité uniquement" (FreeBusy) pour les domaines externes non partenaires
2. Créer des politiques de partage spécifiques pour les partenaires de confiance
3. Interdire le partage "Détails complets" avec des domaines non approuvés

3.2.2 *Interdire le partage de dossiers de contacts avec des domaines externes* Élevé

Profile : E3 Level 1

DESCRIPTION :

Les dossiers de contacts Exchange partagés avec des domaines externes exposent l'annuaire interne de l'organisation : noms, fonctions, numéros de téléphone, adresses email. Ces informations sont exploitables pour des campagnes de spear phishing et de social engineering.

```
Get-SharingPolicy | Select-Object Name, Enabled, Domains
# Vérifier qu'aucune politique n'autorise ContactsSharing vers des domaines All
```

```
# Modifier la politique de partage par défaut pour interdire ContactsSharing
Set-SharingPolicy -Identity "Default Sharing Policy" -Domains "Anonymous:CalendarSharingFreeBusySimple" # Retirer ContactsSharing
```

3.2.3 *Restreindre le partage de calendriers aux domaines de confiance spécifiés (whitelist)* Élevé

Profile : E3 Level 1

DESCRIPTION :

Les contrôles 3.2.1 et 3.2.2 restreignent le type d'information partageable (calendrier/contacts). Ce contrôle va plus loin en limitant les domaines vers lesquels le partage est autorisé. Sans whitelist, tout domaine externe peut recevoir des informations de disponibilité, même si le partage de données complètes est bloqué. Une liste de domaines de confiance approuvés garantit que seuls les partenaires connus peuvent voir les calendriers.

```
# Vérifier la politique de partage par défaut et les domaines autorisés
Get-SharingPolicy | Select-Object Name, Enabled, Domains | Format-List
# Résultat attendu : Domains contient uniquement des domaines partenaires explicites, pas "Anonymous" ou "*"
```

REMÉDIATION :

1. Exchange Admin Center > Flux de messagerie > Politiques de partage
2. Modifier "Default Sharing Policy" pour limiter aux domaines de confiance
3. Créer des politiques de partage spécifiques par partenaire si nécessaire

```
# Limiter aux domaines approuvés
Set-SharingPolicy -Identity "Default Sharing Policy" -Domains "partenaire1.com:CalendarSharingFreeBusySimple","partenaire2.com:Cale
```

REMÉDIATION :

1. Désactiver la politique par défaut si aucun partage externe n'est nécessaire

VALEUR PAR DÉFAUT :

Partage autorisé vers tous les domaines selon le type configuré.

3.2.4 *Désactiver les réponses automatiques d'absence du bureau (OOF) vers les domaines externes* Moyen

Profile : E3 Level 1

DESCRIPTION :

Les messages d'absence du bureau (Out-of-Office) envoyés automatiquement vers l'extérieur divulguent des informations exploitables : dates de congé, nom et contact du remplaçant, numéros de téléphone internes, structure hiérarchique. Ces informations facilitent les attaques BEC ciblées (usurpation d'identité pendant l'absence d'un décideur) et le spear phishing. Exchange peut être configuré pour n'envoyer les OOF qu'en interne.

```
# Vérifier la politique OOF au niveau tenant
Get-RemoteDomain -Identity "Default" | Select-Object DomainName, AutoReplyEnabled, AutoForwardEnabled
# Résultat attendu : AutoReplyEnabled = False pour le domaine Default (externe)

# Vérifier aussi les remote domains spécifiques
Get-RemoteDomain | Select-Object DomainName, AutoReplyEnabled | Format-Table
```

```
# Désactiver les OOF automatiques vers l'extérieur
Set-RemoteDomain -Identity "Default" -AutoReplyEnabled $false
# Appliquer à tous les remote domains
Get-RemoteDomain | Set-RemoteDomain -AutoReplyEnabled $false
```

REMÉDIATION :

Exchange Admin Center > Flux de messagerie > Domaines distants > Modifier "Default" > désactiver "Autoriser les réponses automatiques"

VALEUR PAR DÉFAUT :

AutoReplyEnabled = True — les OOF sont envoyés vers tous les domaines externes.

3.2.5 *Bloquer la connexion directe aux boîtes aux lettres partagées* Critique

Profile : E3 Level 1

DESCRIPTION :

Les boîtes partagées ne doivent pas permettre de connexion directe avec un mot de passe. Si la connexion est activée, un attaquant peut se connecter directement avec les identifiants de la boîte partagée, contournant la traçabilité (qui a fait quoi). L'accès doit uniquement être possible via permissions déléguées.

```
Connect-ExchangeOnline
$SharedMailboxes = Get-EXOMailbox -RecipientTypeDetails SharedMailbox -ResultSize Unlimited
$SharedMailboxes | ForEach-Object {
    Get-MgUser -UserId $_.ExternalDirectoryObjectId -Property DisplayName,UserPrincipalName,AccountEnabled
} | Where-Object { $_.AccountEnabled -eq $true } | ft DisplayName, UserPrincipalName, AccountEnabled
# Résultat attendu : aucune boîte partagée avec AccountEnabled = True
```

```
# Désactiver la connexion pour toutes les boîtes partagées
$SharedMBX = Get-EXOMailbox -RecipientTypeDetails SharedMailbox -ResultSize Unlimited
$SharedMBX | ForEach-Object {
    Update-MgUser -UserId $_.ExternalDirectoryObjectId -AccountEnabled:$false
}
```

3.2.6 *Vérifier qu'aucune règle de transport n'autorise des domaines entiers* — Critique

Profile : E3 Level 1

DESCRIPTION :

Des règles de transport qui fixent le niveau de confiance spam (SCL) à -1 pour des domaines entiers contournent complètement le filtrage anti-spam pour ces domaines. Si un domaine autorisé est compromis, tous les emails malveillants depuis ce domaine atteignent directement les boîtes sans filtrage.

```
Get-TransportRule | Where-Object { $_.SetSCL -eq -1 -and $_.SenderDomainIs -ne $null } |
    ft Name, SenderDomainIs, SetSCL
# Résultat attendu : aucune règle retournée
```

REMÉDIATION :

1. Supprimer toutes les règles de transport qui autorisent des domaines entiers via SCL=-1
2. Si un besoin de partenaire existe, utiliser plutôt des connecteurs avec TLS mutuellement authentifié

```
# Identifier et supprimer
Get-TransportRule | Where-Object { $_.SetSCL -eq -1 } | Remove-TransportRule -Confirm:$true
```

3.2.7 *Désactiver AuditBypassEnabled sur toutes les boîtes aux lettres* — Critique

Profile : E3 Level 1

MITRE ATT&CK : T1562.008 (Impair Defenses: Disable Cloud Logs) · T1070 (Indicator Removal) · T1562 (Impair Defenses)

DESCRIPTION :

La propriété `AuditBypassEnabled` désactive l'audit pour une boîte spécifique. Des outils de migration ou des comptes de service peuvent activer ce contournement, créant des zones aveugles dans la surveillance de sécurité. Aucune boîte ne devrait avoir ce paramètre activé.

```
Get-MailboxAuditBypassAssociation -ResultSize Unlimited |
    Where-Object { $_.AuditBypassEnabled -eq $true } |
    ft Name, AuditBypassEnabled
# Résultat attendu : aucune boîte retournée
```

```
# Corriger toutes les boîtes avec AuditBypass activé
Get-MailboxAuditBypassAssociation -ResultSize Unlimited |
    Where-Object { $_.AuditBypassEnabled -eq $true } |
    ForEach-Object { Set-MailboxAuditBypassAssociation -Identity $_.Name -AuditBypassEnabled $false }
```

3.2.8 *Configurer des limites d'envoi dans la politique anti-spam sortant* — Élevé

Profile : E3 Level 1

DESCRIPTION :

La politique anti-spam sortant doit définir des limites sur le nombre de destinataires par heure et par jour. Sans ces limites, un compte compromis peut envoyer des milliers de spams/phishings en quelques heures, nuisant à la réputation du domaine et pouvant conduire à son blacklistage.

```
Get-HostedOutboundSpamFilterPolicy -Identity Default |
    Select-Object RecipientLimitExternalPerHour, RecipientLimitInternalPerHour,
    RecipientLimitPerDay, ActionWhenThresholdReached
# Valeurs recommandées : ≤500 externe/h, ≤1000 interne/h, ≤1000/jour, ActionWhenThresholdReached = BlockUser
```

```
Set-HostedOutboundSpamFilterPolicy -Identity Default `
    -RecipientLimitExternalPerHour 500 `
    -RecipientLimitInternalPerHour 1000 `
    -RecipientLimitPerDay 1000 `
    -ActionWhenThresholdReached BlockUser `
    -NotifyOutboundSpam $true `
    -NotifyOutboundSpamRecipients @("security@votredomaine.com")
```

3.2.9 *Désactiver la liste sûre du filtre de connexion* — Élevé

Profile : E3 Level 1

DESCRIPTION :

La "liste sûre" (SafeList) du filtre de connexion est une liste maintenue par Microsoft de soi-disant expéditeurs de confiance. Si elle est activée, les emails de ces expéditeurs contournent le filtrage anti-spam. Cette liste est gérée par Microsoft et peut inclure des expéditeurs compromis ou mal configurés.

```
Get-HostedConnectionFilterPolicy -Identity Default | Select-Object EnableSafeList
# Valeur attendue : False
```

```
Set-HostedConnectionFilterPolicy -Identity Default -EnableSafeList $false
```

3.2.10 *Activer les notifications pour les malwares envoyés par des utilisateurs internes*

Élevé

Profile : E3 Level 1

DESCRIPTION :

Quand un malware est détecté dans un email envoyé par un utilisateur interne, l'administrateur doit être notifié immédiatement. Cela permet de détecter rapidement un compte compromis ou un appareil infecté avant que la propagation ne s'élargisse dans l'organisation.

```
Get-MalwareFilterPolicy | Select-Object Identity, EnableInternalSenderAdminNotifications, InternalSenderAdminAddress
# Valeur attendue : EnableInternalSenderAdminNotifications = True et adresse admin configurée
```

```
Set-MalwareFilterPolicy -Identity Default `
    -EnableInternalSenderAdminNotifications $true `
    -InternalSenderAdminAddress "security@votredomaine.com"
```

3.2.11 *Détecter et bloquer les règles de boîte de réception malveillantes (Inbox Rules)*

Critique

MITRE ATT&CK : T1114.003 (Email Collection: Email Forwarding Rule) · T1074 (Data Staged) · T1564.008 (Hide Artifacts: Email Hiding Rules)

Profile : E3 Level 1

DESCRIPTION :

Les règles de boîte de réception malveillantes sont l'un des indicateurs les plus fiables d'une compromission BEC (Business Email Compromise). Après avoir compromis un compte, les attaquants créent des règles qui : (1) redirigent les emails vers des dossiers masqués, (2) transfèrent les emails vers des comptes externes, (3) suppriment automatiquement les alertes de sécurité. Ces règles permettent à l'attaquant de maintenir un accès persistant discret pendant des semaines ou des mois.

```
# Détecter les règles de redirection/transfert automatique suspectes
$mailboxes = Get-Mailbox -ResultSize Unlimited
foreach ($mailbox in $mailboxes) {
    $rules = Get-InboxRule -Mailbox $mailbox.UserPrincipalName -IncludeHidden -ErrorAction SilentlyContinue
    $suspiciousRules = $rules | Where-Object {
        $_.ForwardTo -ne $null -or
        $_.ForwardAsAttachmentTo -ne $null -or
        $_.RedirectTo -ne $null -or
        ($_.DeleteMessage -eq $true -and $_.SubjectContainsWords -match "security|alert|breach|phish|invoice|wire|payment")
    }
    if ($suspiciousRules) {
        Write-Host "⚠️ Règle suspecte sur: $($mailbox.UserPrincipalName)" -ForegroundColor Red
        $suspiciousRules | Select-Object Name, ForwardTo, RedirectTo, DeleteMessage | Format-Table
    }
}
```

REMÉDIATION :

1. Investiguer et supprimer toutes les règles de redirection vers des domaines externes non légitimes
2. Configurer une alerte de sécurité Microsoft 365 sur la création/modification de règles de boîte de réception
3. Bloquer le forwarding automatique vers l'externe (déjà couvert par 3.1.1 — vérifier que la règle de transport est en place)
4. Activer Microsoft Defender for Office 365 pour la détection des règles suspectes
5. Surveiller via le journal d'audit : `Search-UnifiedAuditLog -Operations "New-InboxRule","Set-InboxRule","UpdateInboxRules"`
6. En cas de règle suspecte confirmée : initier la procédure de réponse aux incidents BEC

VALEUR PAR DÉFAUT :

Aucune détection automatique des règles de boîte de réception malveillantes.

Section 4 — MICROSOFT TEAMS

4.1 — Sécurité des Communications Teams

4.1.1 *Restreindre l'accès des invités (Guest Access)* — Élevé

DESCRIPTION :
L'accès invité dans Teams permet à des utilisateurs externes de rejoindre des équipes et d'accéder à des conversations, fichiers et réunions. Sans restriction, des informations sensibles peuvent être partagées accidentellement avec des personnes non autorisées.

AUDIT :

- Teams Admin Center > Paramètres à l'échelle de l'organisation > Accès invité
- PowerShell :

```
Get-CsTeamsClientConfiguration | Select-Object AllowGuestUser
(Get-MgPolicyAuthorizationPolicy).AllowInvitesFrom
```

REMÉDIATION :

1. Teams Admin Center > Accès invité : Configurer les autorisations spécifiques
2. Désactiver pour les invités : appels privés, partage vidéo (selon politique interne)
3. Activer le processus d'approbation pour l'ajout d'invités (via Entra ID)
4. Révision périodique des comptes invités actifs via Access Reviews
5. Définir une expiration automatique des comptes invités (ex: 90 jours)

4.1.2 *Restreindre l'accès externe (Federation)* — Moyen

DESCRIPTION :
L'accès externe (fédération) permet aux utilisateurs Teams de communiquer avec des utilisateurs d'autres organisations Teams ou Skype. Sans liste blanche de domaines autorisés, tout domaine externe peut contacter vos utilisateurs, créant un vecteur de phishing via Teams.

```
Get-CsTenantFederationConfiguration | Select-Object AllowFederatedUsers, AllowedDomains, BlockedDomains
```

REMÉDIATION :

1. Teams Admin Center > Paramètres > Accès externe
2. Choisir entre : Autoriser tous les domaines externes (déconseillé) OU Autoriser uniquement les domaines spécifiques
3. Si autorisation large : activer le blocage des domaines connus malveillants
4. Désactiver l'accès depuis Skype Consumer si non nécessaire

4.1.3 *Sécuriser les réunions Teams* — Moyen

DESCRIPTION :
Les réunions Teams peuvent être rejointes par des participants non authentifiés si elles sont mal configurées. Des attaquants peuvent se joindre à des réunions sensibles ou injecter du contenu malveillant.

```
Get-CsTeamsMeetingPolicy | Select-Object Identity, AllowAnonymousUsersToJoinMeeting, AutoAdmittedUsers, AllowCloudRecording
```

REMÉDIATION :

1. AllowAnonymousUsersToJoinMeeting : Désactivé (ou activé avec salle d'attente obligatoire)
2. AutoAdmittedUsers : EveryoneInCompanyExcludingGuests (les invités passent par la salle d'attente)
3. AllowExternalParticipantGiveRequestControl : Désactivé
4. DesignatedPresenterRoleMode : OrganizerOnlyUserOverride (seul l'organisateur est présentateur par défaut)

4.1.4 *Désactiver l'intégration Email dans les canaux Teams* — Élevé

DESCRIPTION :
L'intégration email dans Teams permet d'envoyer des emails directement dans un canal Teams via une adresse email générée. Cette fonctionnalité contourne les politiques de filtrage des emails et peut permettre l'injection de contenu malveillant dans des canaux Teams sans passer par les protections Exchange/Defender.

```
Get-CsTeamsClientConfiguration | Select-Object AllowEmailIntoChannel
```

REMÉDIATION :

1. Teams Admin Center > Teams > Paramètres Teams > Email integration
2. "Les utilisateurs peuvent envoyer des emails à une adresse email de canal" : Désactivé
3. PowerShell :

```
Set-CsTeamsClientConfiguration -AllowEmailIntoChannel $false
```

4.1.5 *Gouvernance des applications Teams* — Moyen

DESCRIPTION :
Les applications Teams (Microsoft Store, tierces parties, applications personnalisées) peuvent accéder aux données Teams, SharePoint et Exchange via des permissions OAuth. Sans gouvernance, des applications malveillantes ou non vérifiées peuvent être installées par n'importe quel utilisateur et obtenir un accès persistant aux données d'entreprise.

AUDIT :
- Teams Admin Center > Applications Teams > Paramètres d'application à l'échelle de l'organisation

REMÉDIATION :
1. Teams Admin Center > Applications Teams > Gérer les applications > Paramètres d'application à l'échelle de l'organisation
2. Applications tierces : Désactiver les applications tierces globalement, puis activer sélectivement les applications approuvées
3. Applications personnalisées : Restreindre à un groupe d'administrateurs valideurs
4. Créer une liste des applications Microsoft approuvées et une liste des applications tierces autorisées
5. Processus de validation : toute nouvelle application doit faire l'objet d'une revue sécurité avant autorisation

4.1.6 *Activer la protection contre les malwares dans Teams (Safe Attachments)* — Élevé

DESCRIPTION :
Les pièces jointes partagées dans Teams (fichiers dans les conversations et canaux) peuvent contenir des malwares. La protection Safe Attachments pour Teams scanne ces fichiers dans un sandbox avant de les rendre accessibles, comme pour les emails.

```
Get-SafeAttachmentPolicy | Select-Object Name, Enable, EnableForInternalSenders
# Vérifier également dans les paramètres globaux
```

AUDIT :
- Portail Defender > Email & Collaboration > Politiques > Safe Attachments > Paramètres globaux : "Activer Defender pour Office 365 pour SharePoint, OneDrive et Microsoft Teams"

REMÉDIATION :
1. Portail Defender > Safe Attachments > Paramètres globaux
2. Activer "Activer Microsoft Defender pour Office 365 pour SharePoint, OneDrive et Microsoft Teams"
3. Les utilisateurs seront bloqués s'ils tentent de télécharger un fichier détecté comme malveillant

4.1.7 *Activer la protection Safe Links pour Teams* — Élevé

DESCRIPTION :
Les URLs partagées dans les conversations Teams doivent être vérifiées au moment du clic, tout comme les URLs dans les emails. Des attaquants envoient des liens malveillants directement via Teams, contournant potentiellement les protections email si Safe Links n'est pas activé pour Teams.

```
Get-SafeLinksPolicy | Select-Object Name, EnableSafeLinksForTeams, TrackClicks, AllowClickThrough
```

REMÉDIATION :
1. Dans la politique Safe Links : EnableSafeLinksForTeams = $true
2. TrackClicks = $true (suivi des clics pour les rapports)
3. AllowClickThrough = $false (l'utilisateur ne peut pas outrepasser le blocage)

4.1.8 *Contrôler le partage d'écran dans Teams* — Faible

DESCRIPTION :
Le partage d'écran non contrôlé peut conduire au partage accidentel d'informations confidentielles lors de réunions avec des participants externes.

```
Get-CsTeamsMeetingPolicy | Select-Object Identity, ScreenSharingMode, AllowParticipantGiveRequestControl
```

REMÉDIATION :
1. ScreenSharingMode : SingleApplication (partage d'une seule application plutôt que tout l'écran)
2. AllowParticipantGiveRequestControl : Désactivé pour les réunions avec invités externes
3. Former les utilisateurs aux bonnes pratiques de partage d'écran

4.1.9 *Désactiver les 5 fournisseurs de stockage cloud tiers dans Teams* — Moyen

Profile : E3 Level 2

DESCRIPTION :
Teams permet par défaut le partage de fichiers depuis 5 services cloud tiers : **Box, Dropbox, Google Drive, Egnyte, ShareFile**. Ces services contournent les politiques DLP, les étiquettes de sensibilité et l'audit M365. Les fichiers partagés depuis ces services ne bénéficient pas de la protection Safe Attachments et ne sont pas indexés dans Microsoft Purview.

```
Get-CsTeamsClientConfiguration | Select-Object AllowDropBox, AllowBox, AllowGoogleDrive, AllowShareFile, AllowEgnyte | Format-List
# Résultat attendu : Tous à False
```

```
Set-CsTeamsClientConfiguration -AllowDropBox $false -AllowBox $false -AllowGoogleDrive $false -AllowShareFile $false -AllowEgnyte $
```

REMÉDIATION :
Conserver uniquement SharePoint/OneDrive comme sources de fichiers approuvées.

VALEUR PAR DÉFAUT :
Tous les 5 fournisseurs tiers autorisés.

4.1.10 *Empêcher les communications avec les tenants Teams en mode trial* — Élevé

Profile : E3 Level 1

DESCRIPTION :
Les tenants Teams en version d'essai (trial) ont des contrôles de sécurité moins stricts et peuvent être créés facilement par des attaquants pour tenter d'établir des communications avec votre organisation.

```
Get-CsTenantFederationConfiguration | Select-Object AllowTeamsConsumerInbound
```

```
Set-CsTenantFederationConfiguration -AllowTeamsConsumerInbound $false
```

4.1.11 *Bloquer les utilisateurs Teams non gérés d'initier des conversations entrantes* — Élevé

Profile : E3 Level 1

DESCRIPTION :
Des utilisateurs Teams non gérés (comptes personnels, Skype) peuvent initier des conversations avec vos utilisateurs si cette option n'est pas désactivée.

```
Get-CsExternalAccessPolicy -Identity Global | Select-Object EnableTeamsConsumerAccess
```

```
Set-CsExternalAccessPolicy -Identity Global -EnableTeamsConsumerAccess $false
```

REMÉDIATION :
4.2 Sécurité des Réunions Teams — Contrôles Supplémentaires

4.2.1 *Empêcher les utilisateurs en appel entrant (dial-in) de bypasser le lobby* — Moyen

Profile : E3 Level 1

```
Get-CsTeamsMeetingPolicy -Identity Global | Select-Object AllowPSTNUsersToBypassLobby
```

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowPSTNUsersToBypassLobby $false
```

4.2.2 *Désactiver le chat de réunion pour les utilisateurs anonymes* — Moyen

Profile : E3 Level 2

DESCRIPTION :
Le chat visible par des participants anonymes peut être utilisé pour partager des liens malveillants cliqués par des participants internes.

```
Get-CsTeamsMeetingPolicy -Identity Global | Select-Object MeetingChatEnabledType
```

```
Set-CsTeamsMeetingPolicy -Identity Global -MeetingChatEnabledType "EnabledExceptAnonymous"
```

4.2.3 *Restreindre la présentation aux organisateurs et co-organisateurs* — Moyen

Profile : E3 Level 2

```
Get-CsTeamsMeetingPolicy -Identity Global | Select-Object DesignatedPresenterRoleMode
```

```
Set-CsTeamsMeetingPolicy -Identity Global -DesignatedPresenterRoleMode "OrganizerOnlyUserOverride"
```

4.2.4 *Désactiver le chat avec des participants externes post-réunion* — Moyen

Profile : E3 Level 2

```
Get-CsTeamsMeetingPolicy -Identity Global | Select-Object AllowExternalNonTrustedMeetingChat
```

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowExternalNonTrustedMeetingChat $false
```

4.2.5 *Désactiver l'enregistrement automatique des réunions par défaut* — Moyen

Profile : E3 Level 2

```
Get-CsTeamsMeetingPolicy -Identity Global | Select-Object AllowCloudRecording
```

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowCloudRecording $false
```

4.2.6 *Activer le signalement de problèmes de sécurité dans Teams* Moyen

Profile : E3 Level 1

DESCRIPTION :

Permet aux utilisateurs de signaler des messages suspects directement dans Teams — les signalements arrivent dans le portail Microsoft Defender pour analyse. Ce mécanisme de signalement interne accélère la détection des campagnes de phishing ciblant l'organisation via Teams.

```
Get-CsTeamsMessagingPolicy -Identity Global | Select-Object AllowSecurityEndUserReporting
# AllowSecurityEndUserReporting doit être True
```

```
Set-CsTeamsMessagingPolicy -Identity Global -AllowSecurityEndUserReporting $true
```

REMÉDIATION :

Configurer l'adresse de destination : Portail Defender > Settings > Security incident reporting.

VALEUR PAR DÉFAUT :

Signalement de sécurité Teams désactivé.

> **Note :** Le ZAP pour Teams (Zero-Hour Auto Purge) est couvert en **Section 2.4.4** (Microsoft Defender for Office 365).

4.2.7 *Désactiver la publication automatique des enregistrements de réunions Teams* Élevé

Profile : E3 Level 1

DESCRIPTION :

Lorsque l'enregistrement automatique des réunions est activé avec la publication automatique, tous les participants — y compris les invités et utilisateurs externes — reçoivent immédiatement un lien vers l'enregistrement. Cette configuration peut provoquer des fuites involontaires de données sensibles discutées en réunion vers des personnes non autorisées. Un seul invité non identifié dans une réunion peut ainsi obtenir l'enregistrement complet d'une réunion confidentielle.

```
Get-CsTeamsMeetingPolicy -Identity Global | Select-Object Identity, AllowCloudRecording, AutoRecording, NewMeetingRecordingExpirati
# Vérifier : AutoRecording = "Disabled" OU si activé, l'accès post-réunion est contrôlé
# MS.TEAMS.3.1v1 : RecordingStorageMode ne doit pas permettre l'autopublish externe
```

REMÉDIATION :

1. Teams Admin Center > Politiques de réunion > Politique globale
2. Désactiver "Enregistrement automatique des réunions" ou configurer la restriction post-réunion
3. Si l'enregistrement automatique est requis : configurer `DesignatedPresenter = OrganizerAndCoOrganizersOnly`
4. Restreindre l'accès aux enregistrements aux membres authentifiés uniquement :

```
Set-CsTeamsMeetingPolicy -Identity Global `
    -AllowRecordingStorageOrStreamUpload $false
```

REMÉDIATION :

1. Configurer la rétention/expiration automatique des enregistrements (recommandé : 60 jours)
2. Former les organisateurs à la politique d'enregistrement et à la gestion des accès post-réunion

VALEUR PAR DÉFAUT :

Les enregistrements sont publiés automatiquement et accessibles à tous les participants sans restriction.

Section 5 — SHAREPOINT ONLINE ET ONEDRIVE

5.1 — Partage et Permissions

5.1.1 *Restreindre le partage SharePoint/OneDrive à des domaines spécifiques* — Élevé

MITRE ATT&CK : T1213.002 (Data from Cloud Storage: SharePoint) · T1530 (Data from Cloud Storage) · T1048.003 (Exfiltration Over Alternative Protocol: HTTP/HTTPS)

DESCRIPTION :
Par défaut, SharePoint et OneDrive permettent le partage avec n'importe quelle adresse email externe. Restreindre le partage aux domaines partenaires approuvés réduit le risque d'exfiltration accidentelle ou malveillante de données.

AUDIT :

- SharePoint Admin Center > Partage > Paramètres de partage externe
- PowerShell :

```
Get-SPOTenant | Select-Object SharingCapability, SharingDomainRestrictionMode, SharingAllowedDomainList
```

REMÉDIATION :

1. Niveau de partage externe SharePoint : Invités existants uniquement OU Invités nouveaux et existants (selon besoins)
2. Activer la restriction par domaine : Autoriser uniquement les domaines spécifiques
3. OneDrive : même niveau ou plus restrictif que SharePoint
4. Désactiver "Tout le monde" (liens anonymes) pour les données sensibles

5.1.2 *Désactiver les liens de partage anonymes ("Anyone")* — Élevé

DESCRIPTION :
Les liens "Anyone" permettent à toute personne possédant le lien d'accéder au fichier sans authentification. Ces liens peuvent être partagés involontairement ou interceptés, menant à une fuite de données.

```
Get-SPOTenant | Select-Object DefaultSharingLinkType, DefaultLinkPermission
```

REMÉDIATION :

1. SharePoint Admin Center > Paramètres > Partage
2. Désactiver les liens "Toute personne" ou définir une expiration maximale (ex: 7 jours)
3. Lien de partage par défaut : Personnes spécifiques (pas "Personnes de l'organisation")
4. Permissions par défaut des liens : Affichage (pas Modification)

5.1.2b *Configurer une expiration obligatoire sur tous les liens anonymes (30 jours max)* — Critique

Profile : E3 Level 1

DESCRIPTION :
Lorsque les liens anonymes ("Anyone") ne peuvent pas être complètement désactivés pour des raisons métier, une politique d'expiration obligatoire est indispensable. Sans expiration, un lien anonyme créé aujourd'hui reste valide **indéfiniment**, même si l'employé quitte l'entreprise ou si le fichier ne doit plus être partagé. Un attaquant qui intercepte ce lien peut accéder aux données sans limite de temps. Configurer une expiration maximale de 30 jours (idéalement 7 jours) limite drastiquement la fenêtre d'exposition.

```
# Vérifier la durée d'expiration des liens anonymes au niveau tenant
$tenant = Get-SPOTenant
$tenant | Select-Object RequireAnonymousLinksExpireInDays, DefaultLinkPermission, DefaultSharingLinkType

# Résultat attendu :
# RequireAnonymousLinksExpireInDays : entre 1 et 30 (valeur -1 = pas d'expiration = NON CONFORME)
```

AUDIT :

- SharePoint Admin Center > Stratégies > Partage > "Ces liens doivent expirer dans ce nombre de jours"

```
# Définir l'expiration obligatoire à 30 jours maximum (recommandé : 7 jours)
Set-SPOTenant -RequireAnonymousLinksExpireInDays 30

# Idéalement pour les environnements sensibles
Set-SPOTenant -RequireAnonymousLinksExpireInDays 7
```

REMÉDIATION :

1. SharePoint Admin Center > Stratégies > Partage
2. Section "Liens anonymes" > "Ces liens doivent expirer dans ce nombre de jours" = **30** (ou moins)
3. Appliquer également la même politique au niveau de chaque site critique via :

```
# Appliquer sur un site spécifique
Set-SPOSite -Identity "https://contoso.sharepoint.com/sites/Finance" -AnonymousLinkExpirationInDays 7
```

REMÉDIATION :

1. Combiner avec une politique de rappel DLP qui détecte les liens anonymes sans expiration configurée

VALEUR PAR DÉFAUT :
`-1` = Aucune expiration — les liens anonymes sont valides indéfiniment.

> ⚠️ **Point critique (365Inspect — Inspect-SharepointLinkExpiry) :** Ce paramètre est l'un des contrôles les plus fréquemment trouvés non conforme lors des audits M365. La valeur par défaut est systématiquement `-1` (pas d'expiration) et n'est presque jamais modifiée sans audit proactif.

5.1.3 *Activer l'accès conditionnel pour SharePoint (accès non géré)* Élevé

DESCRIPTION :
Les appareils non gérés (personnels) accédant à SharePoint peuvent télécharger et stocker localement des données d'entreprise sans contrôle. La politique d'accès non géré permet de restreindre ces appareils à un accès en lecture seule ou via navigateur uniquement.

```
Get-SPOTenant | Select-Object ConditionalAccessPolicy
```

REMÉDIATION :
1. SharePoint Admin Center > Contrôle des accès > Appareils non gérés
2. Choisir : Autoriser un accès limité (navigateur uniquement, pas de téléchargement)
3. Ou bloquer complètement l'accès depuis des appareils non gérés

5.1.4 *Configurer la durée d'expiration des sessions SharePoint* Faible

DESCRIPTION :
Des sessions SharePoint trop longues sur des appareils partagés ou non sécurisés augmentent le risque d'accès non autorisé si l'utilisateur oublie de se déconnecter.

```
Get-SPOTenant | Select-Object SignInAccelerationDomain, UsePersistentCookiesForExplorerView
```

REMÉDIATION :
1. Activer la déconnexion automatique après inactivité via Accès Conditionnel
2. Pour les appareils non gérés : session max = 1 heure d'inactivité

5.1.5 *Configurer les permissions par défaut des liens en mode Affichage uniquement* Critique

Profile : E3 Level 1
DESCRIPTION :
Lorsqu'un utilisateur crée un lien de partage, la permission par défaut détermine si le destinataire peut modifier ou seulement consulter le fichier. Si la valeur par défaut est "Modification", un utilisateur distrait peut partager involontairement des droits d'écriture sur des fichiers critiques. En définissant "Affichage uniquement" comme défaut, on suit le principe du moindre privilège.

```
$tenant = Get-SPOTenant
$tenant | Select-Object DefaultLinkPermission
# Valeur attendue : View (1 = View, 2 = Edit)
# Si DefaultLinkPermission = 2 (Edit) → NON CONFORME
```

```
Set-SPOTenant -DefaultLinkPermission View
```

REMÉDIATION :
1. SharePoint Admin Center > Stratégies > Partage
2. Section "Liens de fichiers et de dossiers" > Autorisations par défaut : **Affichage**

VALEUR PAR DÉFAUT :
`Edit` (Modification) — les nouveaux liens accordent des droits d'écriture par défaut.

5.1.7 *Restreindre les liens "Anyone" à la permission Affichage uniquement* Critique

Profile : E3 Level 1
DESCRIPTION :
Même lorsque les liens anonymes ("Anyone") sont autorisés pour des raisons métier, leur permission doit être limitée à Affichage uniquement. Un lien "Anyone" en modification permet à n'importe quelle personne possédant le lien de modifier, supprimer ou écraser des fichiers d'entreprise sans authentification.

```
$tenant = Get-SPOTenant
$tenant | Select-Object FileAnonymousLinkType, FolderAnonymousLinkType
# FileAnonymousLinkType = 1 (View) → CONFORME
# FileAnonymousLinkType = 2 (Edit) → NON CONFORME
```

```
Set-SPOTenant -FileAnonymousLinkType View
Set-SPOTenant -FolderAnonymousLinkType View
```

REMÉDIATION :
1. SharePoint Admin Center > Stratégies > Partage
2. Section "Liens Toute personne" > Permissions : **Affichage**

VALEUR PAR DÉFAUT :
`Edit` — les liens anonymes accordent la modification par défaut.

5.1.8 *Exiger une ré-authentification périodique pour les codes de vérification email (≤ 30 jours)* Élevé

Profile : E3 Level 1

DESCRIPTION :

Les utilisateurs externes accédant à SharePoint via un code de vérification email reçoivent un cookie de session persistant. Sans expiration configurée, ce cookie reste valide indéfiniment. Configurer une expiration à 30 jours ou moins force la ré-authentification périodique des invités, limitant la fenêtre d'exploitation d'un cookie volé.

```
$tenant = Get-SPOTenant
$tenant | Select-Object EmailAttestationRequired, EmailAttestationReAuthDays
# EmailAttestationRequired = True ET EmailAttestationReAuthDays ≤ 30 → CONFORME
# EmailAttestationRequired = False → NON CONFORME
```

```
Set-SPOTenant -EmailAttestationRequired $true
Set-SPOTenant -EmailAttestationReAuthDays 30
```

REMÉDIATION :

1. SharePoint Admin Center > Stratégies > Partage
2. Section "Autres paramètres" > "Les personnes qui utilisent un code de vérification doivent s'authentifier de nouveau après" = **30 jours**

VALEUR PAR DÉFAUT :

Ré-authentification désactivée — les cookies invités ne expirent jamais.

5.1.10 *Exiger l'authentification moderne pour SharePoint* Critique

Profile : E3 Level 1

DESCRIPTION :

SharePoint Online doit être configuré pour exiger l'authentification moderne (OAuth 2.0/OIDC). Les clients utilisant l'authentification basique contournent le MFA et l'Accès Conditionnel.

```
Get-SPOTenant | Select-Object LegacyAuthProtocolsEnabled
```

AUDIT :

Doit retourner : `False`

```
Set-SPOTenant -LegacyAuthProtocolsEnabled $false
```

5.1.11 *Activer l'intégration SharePoint/OneDrive avec Azure AD B2B* Élevé

Profile : E3 Level 1

DESCRIPTION :

L'intégration Azure AD B2B pour SharePoint et OneDrive permet d'utiliser les politiques d'accès conditionnel Entra ID pour les invités accédant aux fichiers partagés. Sans cette intégration, les invités contournent les politiques CA lors de l'accès aux liens de partage SharePoint.

```
Get-SPOTenant | Select-Object EnableAzureADB2BIntegration
```

AUDIT :

Doit retourner : `True`

```
Set-SPOTenant -EnableAzureADB2BIntegration $true
```

5.1.12 *Empêcher les invités SharePoint de partager des éléments qu'ils ne possèdent pas* Élevé

Profile : E3 Level 2

DESCRIPTION :

Par défaut, les invités peuvent repartager des fichiers ou dossiers qui ont été partagés avec eux, potentiellement avec d'autres personnes non autorisées. Cela crée des chaînes de partage incontrôlables.

```
Get-SPOTenant | Select-Object PreventExternalUsersFromResharing
```

AUDIT :

Doit retourner : `True`

```
Set-SPOTenant -PreventExternalUsersFromResharing $true
```

5.1.13 *Restreindre le partage externe SharePoint à un groupe de sécurité spécifique* Élevé

Profile : E3 Level 2

DESCRIPTION :

Plutôt que d'autoriser tous les utilisateurs à partager en externe, restreindre cette capacité à un groupe de sécurité dédié (ex: "SPO-External-Sharing-Authorized"). Seuls les membres approuvés peuvent créer des liens de partage externe. Cela permet un contrôle granulaire par utilisateur et une traçabilité complète des partages externes.

```
Get-SPOTenant | Select-Object SharingAllowedDomainList, SharingBlockedDomainList, SharingDomainRestrictionMode, ExternalUserExpirat
# Vérifier aussi :
Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/groupSettings" -Method GET | ConvertTo-Json -Depth 3
```

AUDIT :

- SharePoint Admin Center > Stratégies > Partage > "Autoriser uniquement les utilisateurs de groupes de sécurité spécifiques à partager en externe"

REMÉDIATION :

1. SharePoint Admin Center > Stratégies > Partage
2. Activer "Autoriser uniquement les utilisateurs d'un groupe de sécurité spécifique"
3. Créer un groupe "SPO-External-Sharing-Authorized" avec les utilisateurs approuvés
4. Revue trimestrielle des membres du groupe
5. Documenter le processus d'ajout/retrait du groupe

VALEUR PAR DÉFAUT :

Tous les utilisateurs peuvent partager en externe (dans les limites du niveau de partage tenant).

5.1.14 *Configurer l'expiration automatique de l'accès guest à SharePoint/OneDrive* Élevé

Profile : E3 Level 1

DESCRIPTION :

Les accès guest SharePoint/OneDrive ne doivent pas durer indéfiniment. Une expiration automatique force la révision et le renouvellement des accès, garantissant que les ex-prestataires ou anciens partenaires perdent automatiquement l'accès.

```
Get-SPOTenant | Select-Object ExternalUserExpirationRequired, ExternalUserExpireInDays
```

```
Set-SPOTenant -ExternalUserExpirationRequired $true -ExternalUserExpireInDays 60
```

REMÉDIATION :

CIS recommande 60 jours ou moins. Adapter selon la politique interne.

5.1.15 *Bloquer le téléchargement de fichiers infectés depuis SharePoint* Élevé

Profile : E3 Level 2

DESCRIPTION :

Par défaut, SharePoint peut permettre le téléchargement de fichiers détectés comme infectés (comportement attendu : afficher un avertissement mais permettre le téléchargement). La CIS recommande de bloquer complètement le téléchargement de fichiers infectés.

```
Get-SPOTenant | Select-Object DisallowInfectedFileDownload
```

AUDIT :

Doit retourner : `True`

```
Set-SPOTenant -DisallowInfectedFileDownload $true
```

5.1.16 *Restreindre la synchronisation OneDrive aux appareils gérés* Élevé

Profile : E3 Level 2

DESCRIPTION :

La synchronisation OneDrive sur des appareils non gérés (BYOD, appareils personnels) copie les données d'entreprise localement sur des machines sans contrôle Intune. En cas de compromission ou de perte de l'appareil, ces données sont exposées.

```
Get-SPOTenant | Select-Object BlockMacSync, OneDriveForGuestsEnabled
# Vérifier également la stratégie Intune pour la sync OneDrive
```

```
# Restreindre la sync aux domaines Entra ID approuvés (appareils joints)
Set-SPOTenant -TenantRestrictionsDomains @("votre-tenant-id")
```

REMÉDIATION :

Ou via Intune : déployer la configuration OneDrive pour n'autoriser la sync que sur les appareils conformes.

5.1.17 *Bloquer les scripts personnalisés sur les sites SharePoint* Moyen

Licence requise : SharePoint Online

DESCRIPTION :

Les scripts personnalisés (custom scripts) permettent d'exécuter du JavaScript et du code sur les sites SharePoint. Si un site SharePoint contient un script malveillant (XSS, injection), il s'exécute dans le contexte des utilisateurs qui visitent le site avec leurs credentials M365.

```
# Vérifier la politique globale des scripts personnalisés
Get-SPOTenant | Select-Object DenyAddAndCustomizePages
# DenyAddAndCustomizePages doit être True (scripts désactivés)

# Vérifier les sites spécifiques autorisant les scripts
Get-SPOSite -Limit All | Where-Object { $_.DenyAddAndCustomizePages -eq "Disabled" } | Select-Object Url, Title
```

```
# Désactiver les scripts sur tous les sites
Set-SPOTenant -DenyAddAndCustomizePages $true
# Pour un site spécifique :
Set-SPOSite -Identity "https://contoso.sharepoint.com/sites/DevSite" -DenyAddAndCustomizePages Enabled
```

VALEUR PAR DÉFAUT :

Scripts personnalisés désactivés globalement, mais certains sites anciens peuvent avoir des exceptions.

Section 6 — PROTECTION DE L'INFORMATION ET CONFORMITÉ

6.1 — Microsoft Purview (anciennement Compliance Center)

6.1.1 *Activer l'Audit Unifié (Unified Audit Log)* — Critique

MITRE ATT&CK : T1562.008 (Impair Defenses: Disable Cloud Logs) · T1070.003 (Indicator Removal: Clear Command History) · T1490 (Inhibit System Recovery)

DESCRIPTION :
L'Audit Log unifié enregistre l'ensemble des activités administratives et utilisateur dans M365 (emails, fichiers, connexions, modifications de configuration). Sans ce journal, toute investigation forensic après incident est impossible. Depuis 2023, l'audit est activé par défaut pour les nouveaux tenants, mais doit être vérifié.

```
Get-AdminAuditLogConfig | Select-Object UnifiedAuditLogIngestionEnabled
```

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

REMÉDIATION :
1. Vérifier que la rétention est de 90 jours (standard) ou 180/365 jours (avec licences E5/Audit Premium)
2. Exporter les journaux vers un SIEM externe pour rétention longue durée
3. Configurer des alertes sur les activités critiques

6.1.2 *Configurer des politiques de rétention des données* — Élevé

DESCRIPTION :
Les politiques de rétention permettent de conserver les données pendant la durée légale requise et de les supprimer automatiquement ensuite. Sans politiques de rétention, l'organisation risque soit de supprimer des preuves nécessaires aux investigations, soit de conserver indéfiniment des données inutiles augmentant les risques.

AUDIT :
- Microsoft Purview > Gestion du cycle de vie des données > Stratégies de rétention
- Vérifier l'existence de politiques couvrant Exchange, SharePoint, OneDrive, Teams

REMÉDIATION :
1. Créer des politiques de rétention selon les exigences légales du secteur (ex: 5 ans pour données financières, 3 ans pour emails standard)
2. Appliquer aux emplacements : Exchange, SharePoint, OneDrive, Teams Channel Messages, Teams Chats
3. Configurer la suppression automatique après la période de rétention

6.1.3 *Activer la prévention des pertes de données (DLP)* — Élevé

DESCRIPTION :
Les politiques DLP détectent et empêchent le partage d'informations sensibles (numéros de carte bancaire, NIR, IBAN, données personnelles RGPD) via email, SharePoint, Teams ou OneDrive.

AUDIT :
- Microsoft Purview > Prévention des pertes de données > Stratégies
- Vérifier les politiques actives et leurs périmètres

REMÉDIATION :
1. Créer des politiques DLP pour les types d'informations sensibles pertinents (RGPD France, données financières, données de santé)
2. Actions recommandées : Bloquer le partage externe, notifier l'utilisateur, alerter l'administrateur
3. Activer en mode simulation d'abord pour mesurer le volume de faux positifs
4. Couvrir : Exchange, SharePoint, OneDrive, Teams, Endpoints (si Defender for Endpoint)

6.1.4 *Activer les étiquettes de sensibilité (Sensitivity Labels)* — Moyen

Licence requise : Microsoft 365 E3 ou supérieur avec AIP P1

DESCRIPTION :
Les étiquettes de sensibilité permettent de classifier les documents et emails selon leur niveau de confidentialité (Public, Interne, Confidentiel, Strictement Confidentiel). Ces étiquettes peuvent déclencher automatiquement des protections (chiffrement, marquage visuel, restrictions d'accès).

AUDIT :
- Microsoft Purview > Protection des informations > Étiquettes

REMÉDIATION :
1. Créer une taxonomie d'étiquettes adaptée à l'organisation (ex: Public / Interne / Confidentiel / Secret)
2. Configurer les étiquettes avec : marquage visuel (en-tête, pied de page), chiffrement pour les niveaux élevés, restrictions de partage externe
3. Déployer le client AIP ou l'étiquetage intégré dans les apps M365
4. Activer l'étiquetage automatique pour certains types de données

6.1.5 *Activer Microsoft Purview Communication Compliance* Moyen

Licence requise : Microsoft 365 E5 Compliance

DESCRIPTION :

Communication Compliance permet de détecter les communications à risque : harcèlement, divulgation d'informations confidentielles, mots clés réglementaires. Essentiel pour les secteurs financiers et régulés.

AUDIT :

- Microsoft Purview > Communication Compliance

REMÉDIATION :

1. Créer des politiques de surveillance pour les canaux de communication (Email, Teams)
2. Configurer les mots clés et classifieurs appropriés au secteur
3. Désigner des réviseurs indépendants des personnes surveillées

6.1.6 *Configurer Microsoft Purview Insider Risk Management* Élevé

Licence requise : Microsoft 365 E5 Compliance ou Microsoft 365 E5

DESCRIPTION :

L'Insider Risk Management de Microsoft Purview détecte les comportements anormaux des utilisateurs internes qui pourraient indiquer une exfiltration de données, une sabotage volontaire ou une compromission de compte. Les indicateurs surveillés incluent : téléchargements massifs avant la démission, partages externes anormaux, accès à des données hors périmètre habituel, utilisation d'appareils USB non autorisés. Ce contrôle est particulièrement critique pour les organisations avec des données sensibles ou soumises à des exigences RGPD/NIS2.

Séquence de détection :

```
Déclencheur (ex: préavis HR) → Indicateurs comportementaux (téléchargements > seuil)
→ Score de risque → Alerte investigateur → Action (Legal Hold, restriction accès)
```

AUDIT :

- Microsoft Purview > Insider Risk Management > Tableau de bord
- Vérifier l'existence d'au moins une politique de gestion des risques internes active
- Vérifier que les connecteurs HR sont configurés (si disponibles)

```
# Vérifier via Graph API (nécessite permissions Compliance)
# Microsoft Purview > Insider Risk Management > Policies
# Vérifier : au moins 1 politique active couvrant "Data leaks" ou "Data theft by departing users"
```

REMÉDIATION :

1. Microsoft Purview > Insider Risk Management > Créer une politique
2. Configurer en priorité les politiques :
3. **Fuites de données** : détection téléchargements/partages anormaux
4. **Vol de données par les utilisateurs partants** : déclenché par signal HR (préavis, résiliation)
5. Configurer les seuils d'alerte adaptés à l'organisation (éviter les faux positifs)
6. Désigner un groupe d'investigateurs IR indépendants (séparation des responsabilités)
7. Connecter le connecteur HR RH Microsoft 365 pour les signaux de départ d'employés
8. Activer l'intégration avec Microsoft Defender for Cloud Apps pour enrichir les signaux

VALEUR PAR DÉFAUT :

Insider Risk Management non configuré — aucune détection des comportements internes à risque.

Section 7 — SÉCURITÉ DES APPAREILS (INTUNE/MICROSOFT ENDPOINT MANAGER)

7.1 — Gestion des Appareils

7.1.1 *Exiger le chiffrement des appareils (BitLocker)* — Critique

DESCRIPTION :
Le chiffrement des disques durs protège les données en cas de perte ou vol d'un appareil. Sans BitLocker, toutes les données M365 synchronisées localement sont accessibles par quiconque obtient physiquement l'appareil.

AUDIT :
- Intune > Appareils > Politiques de conformité
- Vérifier l'existence d'une politique exigeant BitLocker

REMÉDIATION :
1. Intune > Sécurité des points de terminaison > Chiffrement de disque > Créer une politique
2. Exiger BitLocker activé sur tous les appareils Windows
3. Configurer le dépôt automatique des clés BitLocker dans Entra ID
4. Politique de conformité : appareil non conforme (BitLocker absent) = accès bloqué

7.1.2 *Exiger un code PIN/mot de passe sur les appareils mobiles* — Élevé

DESCRIPTION :
Les smartphones accédant aux données M365 (email, Teams, OneDrive) doivent être protégés par un code PIN ou biométrie. Un téléphone sans verrouillage d'écran expose directement les données d'entreprise.

AUDIT :
- Intune > Appareils > Politiques de conformité > iOS/Android
- Vérifier les exigences de verrouillage d'écran

REMÉDIATION :
1. Politique de conformité iOS : PIN minimum 6 caractères, biométrie acceptée
2. Politique de conformité Android : PIN minimum 6 caractères, chiffrement exigé
3. App Protection Policies (MAM) pour les appareils non gérés accédant aux apps M365

7.1.3 *Configurer les App Protection Policies (MAM)* — Élevé

DESCRIPTION :
Les politiques de protection des applications (MAM) permettent de sécuriser les données M365 sur des appareils non gérés (BYOD) sans nécessiter l'inscription MDM. Elles isolent les données d'entreprise dans un conteneur sécurisé.

AUDIT :
- Intune > Applications > Stratégies de protection des applications

REMÉDIATION :
1. Créer des politiques MAM pour iOS et Android ciblant les apps M365 (Outlook, Teams, OneDrive, SharePoint)
2. Configurer : Copier/Coller restreint entre apps gérées et non gérées, Capture d'écran désactivée, Chiffrement des données app, Wipe sélectif des données d'entreprise si non conformité

7.1.4 *Activer Windows Hello for Business* — Moyen

DESCRIPTION :
Windows Hello for Business remplace les mots de passe par une authentification biométrique ou PIN local, et utilise des clés cryptographiques liées à l'appareil. C'est une authentification résistante au phishing car elle ne transmet pas de credentials réseau.

AUDIT :
- Intune > Appareils > Profils de configuration > Windows Hello for Business

REMÉDIATION :
1. Intune > Appareils > Inscription > Inscription Windows > Windows Hello for Business
2. Activer Windows Hello for Business pour tous les appareils
3. Exiger un PIN de 6 chiffres minimum (8 recommandé)
4. Activer la biométrie (empreinte digitale, reconnaissance faciale)

7.1.5 *Marquer les appareils sans politique de conformité comme Non conformes*

Élevé

Profile : E3 Level 2

DESCRIPTION :

Par défaut, les appareils sans politique de conformité assignée sont marqués "Conformes" dans Intune — ce qui peut permettre un accès aux ressources protégées par Accès Conditionnel (CA) sans aucun contrôle de conformité. La configuration recommandée est "Non conforme" pour forcer l'assignation d'une politique à chaque appareil.

```
$Uri = 'https://graph.microsoft.com/v1.0/deviceManagement/settings'
(Invoke-MgGraphRequest -Uri $Uri -Method GET).secureByDefault
# Valeur attendue : True
```

AUDIT :

Ou via Intune > Appareils > Conformité > Paramètres de conformité > "Appareils sans politique de conformité" = Non conforme.

REMÉDIATION :

1. Intune Admin Center > Appareils > Conformité > Paramètres de conformité
2. "Marquer les appareils sans politique de conformité assignée comme" → **Non conforme**
3. Déployer ensuite des politiques de conformité pour chaque plateforme (Windows, iOS, Android, macOS)

7.1.6 *Bloquer l'inscription d'appareils personnels (BYOD) par défaut*

Élevé

Profile : E3 Level 2

DESCRIPTION :

Les restrictions d'inscription permettent de bloquer l'inscription d'appareils personnels dans Intune. Un attaquant ayant compromis un compte et contourné l'Accès Conditionnel peut inscrire un appareil personnel pour obtenir un point d'ancrage persistant, simuler une conformité, et réaliser une reconnaissance ou un mouvement latéral.

```
$Uri = 'https://graph.microsoft.com/beta/deviceManagement/deviceEnrollmentConfigurations'
$Config = (Invoke-MgGraphRequest -Uri $Uri -Method GET).value |
    Where-Object { $_.id -match 'DefaultPlatformRestrictions' -and $_.priority -eq 0 }
$Config | Select-Object -ExpandProperty windowsRestriction | Select-Object personalDeviceEnrollmentBlocked
# Valeur attendue : True pour toutes les plateformes
```

REMÉDIATION :

1. Intune > Appareils > Inscription des appareils > Restriction de plateforme
2. Politique de priorité par défaut > Modifier les paramètres de plateforme
3. Colonne "Appareils personnels" → **Bloquer** pour toutes les plateformes (Windows, iOS, Android, macOS)

7.1.7 *Activer Intune Multi-Admin Approval (MAA) pour les actions critiques*

Élevé

Licence requise : Microsoft Intune Plan 1

DESCRIPTION :

Le Multi-Admin Approval (MAA) d'Intune exige qu'une seconde approbation d'un autre administrateur soit obtenue avant d'exécuter des actions critiques (suppression massive d'appareils, modification de politiques de conformité, déploiement de scripts). Cela protège contre les erreurs humaines, les comptes admin compromis et les insider threats.

```
# Vérifier les politiques MAA Intune
$maaApprovals = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/beta/deviceManagement/approvalWorkflowProviders" -Method GE
if ($maaApprovals.value.Count -gt 0) {
    Write-Host "✅ Intune MAA configuré — $($maaApprovals.value.Count) politiques" -ForegroundColor Green
    $maaApprovals.value | Select-Object displayName, isEnabled | Format-Table
} else {
    Write-Host "❌ Intune MAA non configuré" -ForegroundColor Red
}
```

REMÉDIATION :

1. Intune Admin Center > Administration des locataires > Approbations multi-administrateur
2. Créer des workflows d'approbation pour : Scripts, Applications, Politiques de conformité
3. Configurer les approbateurs : au moins 2 admins distincts
4. Les demandes expirent après 72h sans approbation

VALEUR PAR DÉFAUT :

Aucun MAA configuré — toutes les actions admin s'exécutent instantanément.

7.1.8 *Vérifier que l'autorité MDM est définie sur Intune*

Élevé

Licence requise : Microsoft Intune

DESCRIPTION :

L'autorité MDM détermine quelle solution gère les appareils mobiles. Si elle est définie sur "SCCM" ou "None" au lieu d'"Intune", les politiques Intune ne s'appliquent pas aux appareils mobiles, laissant les appareils iOS/Android sans gestion.

```
$mdmAuthority = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/beta/organization" -Method GET
$mdmAuthority.value[0] | Select-Object mobileDeviceManagementAuthority
# Valeur attendue : intune
```

REMÉDIATION :

- Intune Admin Center > Administration des locataires > Autorité MDM
- Définir sur "Intune" si ce n'est pas déjà le cas

VALEUR PAR DÉFAUT :

Intune si déployé via M365, mais peut être défini sur SCCM en environnement hybride.

7.1.9 *Configurer le nettoyage automatique des appareils inactifs Intune* — Moyen

Licence requise : Microsoft Intune

DESCRIPTION :
Les appareils inscrits dans Intune mais inactifs depuis longtemps (ex: appareils d'anciens employés, appareils remplacés) consomment des licences et faussent les rapports de conformité. Une règle de nettoyage automatique supprime ces appareils après un délai configurable.

```
$cleanupRule = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/beta/deviceManagement/managedDeviceCleanupSettings" -Method
$cleanupRule | Select-Object deviceInactivityBeforeRetirementInDays
# Valeur attendue : entre 30 et 90 jours
```

REMÉDIATION :

1. Intune Admin Center > Appareils > Règles de nettoyage des appareils
2. Activer la règle de nettoyage automatique
3. Seuil d'inactivité recommandé : **90 jours**

VALEUR PAR DÉFAUT :
Aucune règle de nettoyage — les appareils inactifs restent indéfiniment.

7.2 — Microsoft Defender for Endpoint — Durcissement

7.2.1 *Activer la protection anti-falsification (Tamper Protection)* — Critique

DESCRIPTION :
La Tamper Protection empêche les attaquants (et les malwares) de désactiver ou modifier les composants de Microsoft Defender Antivirus via le registre, PowerShell ou des outils tiers. Sans Tamper Protection, un attaquant ayant accès local ou via SYSTEM peut silencieusement désactiver la protection en temps réel avant d'exécuter son payload. C'est l'une des premières actions que les ransomwares modernes tentent.

MITRE ATT&CK : T1562.001 (Impair Defenses: Disable or Modify Tools)

```
# Via Microsoft Graph (Intune)
$configs = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/beta/deviceManagement/deviceConfigurations" -Method GET
$configs.value | Where-Object { $_.oDataType -match "windows10EndpointProtection" } |
    Select-Object displayName, @{N="TamperProtection"; E={ $_.defenderTamperProtection }}
# Valeur attendue : enable
```

AUDIT :
Ou dans Defender Portal > Paramètres > Fonctionnalités avancées > Tamper Protection = Activé

REMÉDIATION :

1. Intune > Sécurité des points de terminaison > Antivirus > Créer une politique Windows Antivirus
2. Activer **Tamper Protection** = Activé
3. Appliquer à tous les groupes d'appareils Windows
4. Vérifier via Defender Portal > Paramètres > Protection contre les falsifications

VALEUR PAR DÉFAUT :
Désactivée sur les appareils non gérés par Intune/MDE.

7.2.2 *Configurer les règles de réduction de la surface d'attaque (ASR Rules)* — Critique

DESCRIPTION :
Les règles ASR (Attack Surface Reduction) bloquent des comportements spécifiques utilisés par les malwares : macros Office injectant du shellcode, lancement de processus fils depuis Office/Adobe, création de processus via WMI, vol de credentials depuis LSASS, etc. Ces règles sont la couche de défense la plus efficace contre les vecteurs d'attaque modernes (phishing, living-off-the-land).

MITRE ATT&CK : T1566 (Phishing) · T1055 (Process Injection) · T1059 (Command and Scripting Interpreter) · T1003.001 (LSASS Memory)

```
# Vérifier les règles ASR configurées via MDE
Get-MpPreference | Select-Object AttackSurfaceReductionRules_Ids, AttackSurfaceReductionRules_Actions
# Les GUID des règles critiques et leurs actions (0=Off, 1=Block, 2=Audit, 6=Warn)
```

AUDIT :
Defender Portal > Gestion de la configuration > Politiques de sécurité des points de terminaison > Règles ASR

REMÉDIATION :
Configurer via Intune (Endpoint Security > Attack Surface Reduction) les règles critiques en mode **Block** :

> **Déploiement recommandé :** démarrer en mode **Audit** pendant 2 semaines pour identifier les faux positifs, puis basculer en **Block**.

VALEUR PAR DÉFAUT :
Toutes les règles ASR désactivées.

7.2.3 *Activer la protection réseau (Network Protection)* Élevé

DESCRIPTION :
La Network Protection étend les capacités de SmartScreen à tout le trafic réseau sortant, bloquant les connexions vers des domaines malveillants, serveurs C2 connus et URLs de phishing — même depuis des applications non-navigateur (PowerShell, cmd.exe, malwares custom). C'est une couche critique contre les attaques de type C2 callback.

MITRE ATT&CK : T1071 (Application Layer Protocol) · T1041 (Exfiltration Over C2 Channel)

```
Get-MpPreference | Select-Object EnableNetworkProtection
# 0 = Disabled | 1 = Enabled (Block) | 2 = Audit
# Valeur attendue : 1 (Block)
```

```
# Via Intune — Endpoint Security > Attack Surface Reduction > Network Protection = Block
Set-MpPreference -EnableNetworkProtection Enabled  # Pour test local uniquement
```

REMÉDIATION :

1. Intune > Sécurité des points de terminaison > Réduction de la surface d'attaque
2. Créer une politique > Protection réseau = **Activé (mode Bloquer)**
3. Déployer sur tous les groupes d'appareils Windows gérés

VALEUR PAR DÉFAUT :
Désactivée.

7.2.4 *Configurer l'investigation et la réponse automatisées (AIR) en mode complet* Élevé

DESCRIPTION :
L'Automated Investigation and Response (AIR) de Microsoft Defender for Endpoint analyse automatiquement les alertes, collecte des preuves et peut remédier automatiquement aux menaces. En mode "Approbation requise" (semi-automatique), les actions de remédiation attendent une validation humaine. En mode "Automatique complet", MDE remédie directement aux menaces non critiques, réduisant le temps de réponse de heures à minutes.

MITRE ATT&CK : M1038 (Execution Prevention) · M1040 (Behavior Prevention on Endpoint)

AUDIT :

1. Defender Portal > Paramètres > Points de terminaison > Groupes d'appareils
2. Vérifier le niveau d'automatisation de chaque groupe : valeur attendue = **Complet**

REMÉDIATION :

1. Defender Portal (security.microsoft.com) > Paramètres > Système > Groupes d'appareils
2. Pour chaque groupe : modifier le niveau d'automatisation = **Complet - corriger les menaces automatiquement**
3. S'assurer que tous les appareils sont rattachés à un groupe avec automatisation complète

VALEUR PAR DÉFAUT :
Semi-automatique (approbation requise pour la remédiation).

7.2.5 *Activer Microsoft Defender Antivirus en mode protection en temps réel* Critique

DESCRIPTION :
La protection en temps réel de Microsoft Defender Antivirus scanne les fichiers à l'ouverture, à l'écriture et à l'exécution. Sa désactivation — même temporaire — crée une fenêtre d'exposition critique. Des GPO ou scripts malveillants peuvent la désactiver. Surveiller son état via Intune garantit une couverture continue.

```
# Vérifier via Intune — Rapport de conformité antivirus
Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/beta/deviceManagement/managedDevices?`$filter=operatingSystem eq 'Windows'"
    Select-Object -ExpandProperty value | Select-Object deviceName, isEncrypted, complianceState
# Ou via Defender Portal > Rapports > Appareils à risque
```

REMÉDIATION :

1. Intune > Sécurité des points de terminaison > Antivirus > Créer une politique Microsoft Defender Antivirus
2. Activer : Protection en temps réel = **Oui**, Protection fournie par le cloud = **Oui**, Soumission automatique d'échantillons = **Oui**
3. Configurer une alerte sur les appareils ayant la protection en temps réel désactivée

VALEUR PAR DÉFAUT :
Activée par défaut, mais peut être désactivée localement sans Intune.

Section 8 — MICROSOFT SECURE SCORE ET MONITORING

8.1 — Secure Score et Alertes

8.1.1 *Atteindre et maintenir un Secure Score ≥ 50%* — Élevé

DESCRIPTION :
Le Microsoft Secure Score est un indicateur de la posture de sécurité du tenant M365. Un score bas indique de nombreuses mesures de sécurité non implémentées. Le score doit être mesuré régulièrement et les améliorations priorisées.

AUDIT :

- Portail Microsoft Defender > Secure Score
- Documenter le score actuel et la tendance

REMÉDIATION :

1. Portail Defender > Secure Score > Actions recommandées
2. Prioriser les actions par : Impact élevé, Facilité d'implémentation
3. Assigner des responsables pour chaque action
4. Définir un objectif de score cible (ex: +10 points par trimestre)
5. Exclure les recommandations non applicables (avec justification documentée)

8.1.2 *Configurer les alertes de sécurité obligatoires Exchange/Defender* — Critique

DESCRIPTION :
La CISA impose l'activation d'un ensemble minimum d'alertes dans M365 pour les organisations. Ces alertes couvrent les principaux vecteurs d'attaque : compromission de comptes d'envoi, activités de connecteurs suspects, transferts d'emails malveillants, etc.

AUDIT :

- Microsoft Purview > Alertes > Stratégies d'alerte
- Vérifier que les alertes suivantes sont actives et ont des destinataires configurés :

Liste des alertes CISA obligatoires :

```
1. Patterns d'envoi d'emails suspects détectés
2. Activité suspecte du connecteur
3. Activité suspecte de transfert d'emails
4. Les messages ont été retardés
5. Tenant restreint de l'envoi d'emails non provisionnés
6. Tenant restreint de l'envoi d'emails
7. Un clic sur une URL potentiellement malveillante a été détecté
```

REMÉDIATION :

1. Microsoft Purview > Alertes > Stratégies d'alerte
2. Activer chacune des alertes listées ci-dessus
3. Configurer les destinataires : adresse email SOC ou RSSI
4. Tester les alertes via des simulations d'activités suspectes

8.1.3 *Configurer des alertes de sécurité personnalisées* — Élevé

DESCRIPTION :
Des alertes proactives permettent de détecter rapidement les incidents de sécurité : connexions suspectes, activation de règles de transfert malveillantes, tentatives de connexion depuis des pays inhabituels, alertes administratives critiques.

AUDIT :

- Microsoft Purview > Alertes > Stratégies d'alerte
- Portail Defender > Incidents & Alertes

REMÉDIATION :

1. Activer les politiques d'alerte par défaut (déjà disponibles dans M365)
2. Créer des alertes personnalisées pour :
3. Connexion depuis un pays jamais vu
4. Création de règle de transfert d'emails
5. Téléchargement massif de fichiers (> 50 fichiers en < 5 min)
6. Activation/désactivation MFA sur un compte admin
7. Connexion sur les comptes break glass
8. Attribution du rôle Global Administrator
9. Configurer les destinataires des notifications (SOC, RSSI)

8.1.4 *Activer Microsoft Defender for Identity (si AD hybride)* Élevé

Licence requise : Microsoft 365 E5 ou Defender for Identity standalone

DESCRIPTION :

Defender for Identity surveille le trafic Active Directory on-premises et dans le cloud pour détecter les comportements suspects : Golden Ticket, Pass-the-Hash, reconnaissance LDAP, escalade de privilèges.

AUDIT :

- Portail Defender > Paramètres > Identités
- Vérifier que les capteurs sont installés sur tous les contrôleurs de domaine

REMÉDIATION :

1. Créer un compte de service dédié pour Defender for Identity
2. Installer les capteurs sur tous les Domain Controllers
3. Configurer les notifications et intégration SIEM
4. Réviser les alertes hebdomadairement

8.1.5 *Activer Microsoft Defender for Cloud Apps (CASB)* Élevé

Licence requise : Microsoft 365 E5 Security

DESCRIPTION :

Defender for Cloud Apps (anciennement MCAS) est un Cloud Access Security Broker qui permet la visibilité et le contrôle des applications cloud utilisées dans l'organisation (Shadow IT), la détection d'anomalies comportementales, et la protection contre les menaces avancées.

AUDIT :

- Portail Defender > Cloud Apps > Tableau de bord

REMÉDIATION :

1. Connecter les applications cloud principales (M365, Salesforce, Box, etc.)
2. Activer Cloud Discovery pour identifier le Shadow IT
3. Configurer des politiques d'anomalie détectant : voyage impossible, téléchargements massifs, activités depuis des adresses IP anonymes
4. Intégrer avec Accès Conditionnel pour le contrôle d'application en temps réel

8.1.6 *Activer et configurer la protection des comptes prioritaires* Élevé

Profile : E5 Level 1

Licence requise : Microsoft Defender for Office 365 Plan 2

DESCRIPTION :

La protection des comptes prioritaires offre une surveillance et une protection renforcées pour les utilisateurs à haute valeur : dirigeants, DSI, DRH, responsables financiers, comptes IT admin. Ces comptes sont les cibles privilégiées du whaling (spear-phishing ciblant les cadres dirigeants).

AUDIT :

1. Microsoft Defender > Paramètres > Email & collaboration > Protection des comptes prioritaires
2. Vérifier que la protection est activée
3. Microsoft Defender > Paramètres > Email & collaboration > Balises utilisateur
4. Vérifier que les comptes critiques sont tagués "Compte prioritaire"

REMÉDIATION :

1. Defender > Paramètres > Email & collaboration > Protection des comptes prioritaires → Activer
2. Defender > Paramètres > Email & collaboration > Balises utilisateur → Ajouter les dirigeants, admins IT, équipe financière comme "Comptes prioritaires"
3. Configurer des alertes email pour les activités des comptes prioritaires

8.1.7 *Appliquer le preset de sécurité Strict aux comptes prioritaires* Élevé

Profile : E5 Level 1

Licence requise : Microsoft Defender for Office 365 Plan 2

DESCRIPTION :

Les comptes prioritaires (dirigeants, IT admins) doivent bénéficier de la protection preset "Stricte" de Defender for Office 365 — le niveau le plus agressif couvrant : anti-spam, anti-malware, anti-phishing avec protection contre l'usurpation, Safe Attachments et Safe Links.

Note : Les presets ne peuvent pas cibler des **balises** Priority Account — utiliser des groupes de sécurité à la place.

AUDIT :

- Defender > Email & collaboration > Politiques et règles > Politiques de menaces > Politiques de sécurité prédéfinies
- Vérifier que "Strict Preset Security Policy" inclut les groupes contenant les comptes prioritaires

REMÉDIATION :

1. Defender > Email & collaboration > Politiques et règles > Politiques de sécurité prédéfinies
2. Cliquer "Gérer les paramètres de protection" pour la protection Stricte
3. Ajouter le groupe des comptes prioritaires aux sections EOP Protection et Defender Protection
4. Configurer la protection contre l'usurpation d'identité (usurpation d'utilisateurs internes et de domaines partenaires)

8.1.8 *Configurer des alertes d'activité pour les comptes d'accès d'urgence (Break Glass)* Critique

Profile : E5 Level 1

DESCRIPTION :

Les comptes Break Glass ne doivent être utilisés qu'en cas d'urgence absolue (blocage de tous les autres admins). Toute connexion avec ces comptes doit déclencher immédiatement une alerte à l'équipe sécurité — il peut s'agir d'une urgence légitime ou d'une compromission critique.

AUDIT :

- Microsoft Defender > Politiques et règles > Gestion des alertes > Politiques d'alertes
- Vérifier l'existence d'une alerte sur "Connexion" pour les UPNs des comptes Break Glass

REMÉDIATION :

1. Microsoft Defender > Politiques et règles > Gestion des alertes
2. Créer une politique d'alerte : Activité = "Connexion réussie", Utilisateurs = [UPN des comptes Break Glass]
3. Configurer une notification immédiate vers le RSSI et l'équipe SOC
4. Tester l'alerte trimestriellement en se connectant avec un compte Break Glass en conditions contrôlées

8.1.9 *Détecter les credentials admins exposés sur des endpoints vulnérables (XSPM)* Élevé

MITRE ATT&CK : T1552 (Unsecured Credentials) · T1078.004 (Valid Accounts: Cloud) · T1555 (Credentials from Password Stores)

Licence requise : Microsoft Defender XDR P2

DESCRIPTION :

Microsoft Defender Exposure Management (XSPM) détecte lorsque des credentials d'utilisateurs hautement privilégiés (Global Admins, Security Admins) ont été utilisés sur des endpoints vulnérables ou compromis. Si un admin se connecte sur un poste non patché ou infecté, ses credentials peuvent être exposés via un credential dump. Ce contrôle croise les données Defender avec les données d'identité Entra.

```
# Via l'API Defender Exposure Management
$exposedCredentials = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/beta/security/exposureManagement/attackPaths?`$filter
if ($exposedCredentials) {
    $exposedCredentials.value | Select-Object displayName, risk | Format-Table
} else {
    Write-Host "Vérifier dans le portail Microsoft Defender > Gestion de l'exposition > Chemins d'attaque"
}
```

AUDIT :

- Microsoft Defender XDR > Gestion de l'exposition > Chemins d'attaque > Filtrer par admins privilégiés

REMÉDIATION :

1. Identifier les endpoints vulnérables utilisés par des admins privilégiés
2. Patcher immédiatement ou isoler ces endpoints via Intune
3. Forcer une réinitialisation MFA et mot de passe pour les admins concernés
4. Déployer Windows Credential Guard sur tous les postes d'administration

VALEUR PAR DÉFAUT :

Non configuré — nécessite Defender XDR P2.

8.1.10 *Implémenter la détection de dérive de configuration (Configuration Drift)* Moyen

Licence requise : Entra ID P1

DESCRIPTION :

La dérive de configuration (configuration drift) survient lorsque des paramètres de sécurité sont modifiés sans suivi. Un export JSON de l'état de référence (baseline) permet de détecter les changements non autorisés. Maester propose un mécanisme de comparaison JSON automatisé via CI/CD.

```
# Exporter l'état de référence des politiques CA
$baseline = Get-MgIdentityConditionalAccessPolicy -All | ConvertTo-Json -Depth 5
$baseline | Out-File "C:\Security\CA_Baseline_$(Get-Date -Format 'yyyy-MM-dd').json"

# Comparer avec une baseline existante
$current = Get-MgIdentityConditionalAccessPolicy -All | ConvertTo-Json -Depth 5
$reference = Get-Content "C:\Security\CA_Baseline_reference.json"
if ($current -ne $reference) {
    Write-Host "⚠️ DRIFT DÉTECTÉ : les politiques CA ont changé depuis la baseline" -ForegroundColor Yellow
}
```

REMÉDIATION :

1. Créer une baseline JSON mensuelle de la configuration de sécurité (CA, auth methods, PIM)
2. Intégrer la comparaison dans un pipeline CI/CD ou une tâche planifiée
3. Alerter sur toute dérive non autorisée
4. Maester peut être exécuté en mode monitoring continu pour ce contrôle

VALEUR PAR DÉFAUT :

Aucun mécanisme de détection de dérive — les changements de config passent inaperçus.

Section 9 — POWER PLATFORM ET AUTRES SERVICES

9.1 — Power Platform

9.1.1 *Restreindre la création d'environnements de production et sandbox aux administrateurs* — Moyen

DESCRIPTION :
Par défaut, n'importe quel utilisateur avec une licence M365 peut créer des environnements Power Apps, des flux Power Automate et des applications Canvas. Des données sensibles peuvent être exportées via des connecteurs non contrôlés.

AUDIT :

- Power Platform Admin Center > Paramètres > Gouvernance > Environnements

REMÉDIATION :

1. Power Platform Admin Center > Paramètres > Gouvernance
2. Restreindre la création d'environnements aux administrateurs Power Platform uniquement
3. Désactiver les connecteurs à haut risque (connecteurs tierces parties non approuvés) via Data Loss Prevention policies
4. Activer la journalisation des activités Power Platform

9.1.2 *Restreindre la création d'environnements d'essai (trial) aux administrateurs* — Élevé

DESCRIPTION :
Les environnements d'essai créés par les utilisateurs échappent aux politiques DLP et de gouvernance de l'organisation, pouvant contenir des flux et applications qui manipulent des données sensibles sans contrôle.

AUDIT :

- Power Platform Admin Center > Paramètres > Environnements d'essai

REMÉDIATION :

1. Power Platform Admin Center > Paramètres > Gouvernance
2. "Qui peut créer des environnements d'essai" : Uniquement les administrateurs spécifiques

9.1.3 *Activer l'isolation des tenants Power Platform* — Élevé

DESCRIPTION :
L'isolation des tenants Power Platform empêche les connecteurs Power Apps/Power Automate de l'organisation de se connecter à des tenants Entra ID externes non approuvés, et empêche des tenants externes de se connecter au tenant de l'organisation. Cela bloque l'exfiltration de données via des flux inter-tenants malveillants.

AUDIT :

- Power Platform Admin Center > Sécurité > Identité et accès > Isolation des tenants

REMÉDIATION :

1. Power Platform Admin Center > Sécurité > Isolation des tenants
2. Activer "Restreindre les connexions inter-tenants"
3. Configurer une liste d'autorisation (allowlist) pour les tenants partenaires légitimes
4. PowerShell :

```
# Activer tenant isolation
$tenantSettings = Get-TenantSettings
$tenantSettings.powerPlatform.governance.disableTenantIsolation = $false
Set-TenantSettings -RequestBody $tenantSettings
```

9.1.4 *Activer la Content Security Policy (CSP) pour les Power Apps* — Moyen

DESCRIPTION :
La Content Security Policy (CSP) pour les Power Apps (model-driven et canvas) empêche les attaques XSS en définissant quelles sources de contenu sont autorisées à s'exécuter dans l'application. Sans CSP, du code JavaScript malveillant pourrait être injecté dans les applications Power Apps.

AUDIT :

- Power Platform Admin Center > Environnements > Paramètres > Produit > Confidentialité + Sécurité
- Vérifier que CSP est activé pour les applications model-driven et canvas

REMÉDIATION :

1. Pour chaque environnement : Power Platform Admin Center > Environnements > Sélectionner l'environnement > Paramètres > Produit > Confidentialité + Sécurité
2. Activer CSP pour les applications model-driven
3. Activer CSP pour les applications canvas

9.1.5 *Restreindre la création de sites Power Pages aux administrateurs* Moyen

DESCRIPTION :
Power Pages permet de créer des portails web accessibles publiquement depuis les données Dataverse. Un portail mal configuré créé par un utilisateur non averti peut exposer des données sensibles sur Internet.

```
$tenantSettings = Get-TenantSettings
$tenantSettings.powerPlatform.powerPages.disablePortalsCreationByNonAdminUsers
```

AUDIT :
Doit retourner `True`

```
$tenantSettings = Get-TenantSettings
$tenantSettings.powerPlatform.powerPages.disablePortalsCreationByNonAdminUsers = $true
Set-TenantSettings -RequestBody $tenantSettings
```

9.1.6 *Désactiver le partage Power Apps avec "Tout le monde"* Moyen

DESCRIPTION :
La fonctionnalité "Partager avec tout le monde" dans Power Apps peut exposer une application à l'ensemble des utilisateurs de l'organisation, y compris ceux qui n'ont pas besoin d'y accéder. Cela viole le principe du moindre privilège.

```
$tenantSettings = Get-TenantSettings
$tenantSettings.powerPlatform.powerApps.disableShareWithEveryone
```

AUDIT :
Doit retourner `True`

```
$tenantSettings = Get-TenantSettings
$tenantSettings.powerPlatform.powerApps.disableShareWithEveryone = $true
Set-TenantSettings -RequestBody $tenantSettings
```

9.1.7 *Configurer les politiques DLP Power Platform* Moyen

DESCRIPTION :
Les politiques DLP de Power Platform contrôlent quels connecteurs peuvent être utilisés ensemble dans un flux ou une application. Cela prévient la création de flux qui exportent des données M365 vers des services non approuvés.

AUDIT :

- Power Platform Admin Center > Politiques de données > Politiques DLP

REMÉDIATION :

1. Créer une politique DLP couvrant tous les environnements
2. Déplacer les connecteurs M365 (SharePoint, Excel, Outlook) dans le groupe "Business"
3. Déplacer les connecteurs à risque dans le groupe "Non-Business" ou "Blocked"
4. Les connecteurs dans des groupes différents ne peuvent pas être utilisés dans le même flux

Section 10 — MICROSOFT FABRIC (POWER BI)

10.1 — Paramètres du Tenant Fabric

10.1.1 *Restreindre l'accès invité à Microsoft Fabric* — Élevé

Profile : E3 Level 1

DESCRIPTION :

L'accès des invités Entra ID à Microsoft Fabric doit être restreint. Des utilisateurs invités ayant accès à Fabric peuvent consulter des tableaux de bord contenant des données commerciales sensibles (chiffres d'affaires, KPIs, données RH, etc.) qui n'étaient pas destinées à une audience externe.

AUDIT :

- Portail Power BI Admin > Paramètres du tenant > Paramètres d'exportation et de partage
- Vérifier "Autoriser Azure Active Directory les utilisateurs invités à accéder à Microsoft Fabric"

REMÉDIATION :

1. Portail Fabric Admin (app.powerbi.com/admin-portal) > Paramètres du tenant
2. "Autoriser les utilisateurs invités Azure AD à accéder à Microsoft Fabric" : Désactivé
3. Si des invités ont besoin d'accès : créer des groupes de sécurité dédiés avec accès explicitement approuvé

10.1.2 *Restreindre les invitations d'utilisateurs externes dans Fabric* — Élevé

Profile : E3 Level 1

DESCRIPTION :

Fabric peut inviter des utilisateurs externes directement, contournant potentiellement les restrictions d'invitation d'invités configurées dans Entra ID. Cette fonctionnalité doit être désactivée pour centraliser la gestion des invités dans Entra ID.

AUDIT :

- Portail Fabric Admin > Paramètres du tenant > "Inviter des utilisateurs externes dans votre organisation"

REMÉDIATION :

1. Portail Fabric Admin > Paramètres du tenant
2. "Inviter des utilisateurs externes dans votre organisation" : Désactivé
3. Toutes les invitations doivent passer par le processus Entra ID standard

10.1.3 *Restreindre l'accès guest au contenu Fabric* — Élevé

Profile : E3 Level 1

DESCRIPTION :

Même si les invités peuvent accéder à Fabric, l'accès au contenu (rapports, tableaux de bord, datasets) doit être restreint aux ressources explicitement partagées, sans accès global au tenant Fabric.

AUDIT :

- Portail Fabric Admin > "Autoriser les utilisateurs invités Azure AD à accéder à Microsoft Fabric"
- Différent du contrôle 10.1.1 — ceci contrôle l'accès au contenu spécifique

REMÉDIATION :

1. Portail Fabric Admin > Paramètres du tenant
2. "Les utilisateurs invités peuvent accéder aux rapports Fabric via un lien" : Désactivé (ou restreint à un groupe approuvé)

10.1.4 *Restreindre la publication sur Internet (Publish to Web)* — Critique

Profile : E3 Level 1

DESCRIPTION :

La fonctionnalité "Publier sur le web" de Power BI/Fabric crée un lien public accessible à n'importe quelle personne sur Internet, sans authentification. Des rapports contenant des données sensibles peuvent être publiés accidentellement. Cette fonctionnalité doit être désactivée ou restreinte aux administrateurs uniquement.

AUDIT :

- Portail Fabric Admin > Paramètres du tenant > "Publier sur le web"

REMÉDIATION :

1. Portail Fabric Admin > Paramètres du tenant
2. "Publier sur le web" : Désactivé
3. Si nécessaire pour des cas légitimes : restreindre à un groupe de sécurité approuvé avec processus de validation

10.1.5 *Désactiver les visuels R et Python interactifs* — Moyen

Profile : E3 Level 2

DESCRIPTION :

Les visuels R et Python dans Fabric exécutent du code sur les postes clients ou dans le cloud. Du code R/Python malveillant intégré dans un rapport peut exfiltrer des données, exécuter des commandes système, ou servir de vecteur d'attaque.

AUDIT :

- Portail Fabric Admin > Paramètres du tenant > "Interagir avec et partager des visuels R et Python"

REMÉDIATION :

1. Portail Fabric Admin > Paramètres du tenant
2. "Interagir avec et partager des visuels R et Python" : Désactivé

10.1.6 *Activer l'application des étiquettes de sensibilité dans Fabric* Élevé

Profile : E3 Level 1

DESCRIPTION :

Les étiquettes de sensibilité Microsoft Purview doivent pouvoir être appliquées aux contenus Fabric (rapports, datasets, tableaux de bord). Cela permet la classification des données et le déclenchement de politiques de protection associées (chiffrement, restrictions d'accès).

AUDIT :

- Portail Fabric Admin > Paramètres du tenant > Protection des informations
- "Permettre aux utilisateurs d'appliquer des étiquettes de sensibilité au contenu" : Activé

REMÉDIATION :

1. Portail Fabric Admin > Protection des informations
2. Activer "Permettre aux utilisateurs d'appliquer des étiquettes de sensibilité au contenu"
3. Activer "Appliquer des étiquettes de sensibilité depuis des sources de données aux données dans Fabric"

10.1.7 *Restreindre les liens partageables dans Fabric* Élevé

Profile : E3 Level 1

DESCRIPTION :

Les liens partageables dans Fabric peuvent donner accès à des rapports à toute personne de l'organisation ou externe. Ces liens doivent être restreints pour éviter la diffusion non contrôlée de données analytiques sensibles.

AUDIT :

- Portail Fabric Admin > Paramètres du tenant > "Créer des liens partageables vers du contenu avec accès activé"

REMÉDIATION :

1. Portail Fabric Admin > Paramètres du tenant
2. Désactiver les liens partageables avec "Toute personne dans l'organisation"
3. Maintenir uniquement les liens pour des utilisateurs spécifiques

10.1.8 *Restreindre le partage de données externes dans Fabric* Élevé

Profile : E3 Level 1

DESCRIPTION :

Fabric peut se connecter à des sources de données externes et potentiellement envoyer des données vers l'extérieur. Cette fonctionnalité doit être restreinte pour éviter l'exfiltration non intentionnelle de données d'entreprise.

AUDIT :

- Portail Fabric Admin > "Autoriser les connexions de données externes spécifiques"

REMÉDIATION :

1. Portail Fabric Admin > Paramètres du tenant > "Activation du partage externe de données"
2. Désactiver ou restreindre à un groupe d'utilisateurs approuvés

10.1.9 *Activer BlockResourceKeyAuthentication dans Fabric* Élevé

Profile : E3 Level 1

DESCRIPTION :

L'authentification par clé de ressource (ResourceKey) dans Power BI Embedded permet d'accéder à des rapports sans authentification Entra ID. Si cette méthode est utilisée avec des clés exposées, n'importe qui ayant la clé peut accéder aux rapports. Bloquer cette méthode force l'utilisation d'OAuth 2.0.

AUDIT :

- Portail Fabric Admin > Paramètres du tenant > "Bloquer l'authentification par clé de ressource"

REMÉDIATION :

1. Portail Fabric Admin > Paramètres du tenant
2. "Bloquer l'authentification par clé de ressource" : Activé

10.1.10 *Restreindre l'accès aux APIs Fabric par les principaux de service* Élevé

Profile : E3 Level 1

DESCRIPTION :

Les principaux de service (Service Principals) peuvent accéder aux APIs Fabric avec des permissions très larges. Sans restriction, des applications tierces ou des scripts automatisés peuvent lire, modifier ou exporter l'ensemble des données analytiques de l'organisation.

AUDIT :

- Portail Fabric Admin > Paramètres du tenant > "Permettre aux principaux de service d'utiliser les APIs Power BI"

REMÉDIATION :

1. Portail Fabric Admin > Paramètres du tenant
2. "Permettre aux principaux de service d'utiliser les APIs Power BI" : Désactivé ou restreint à des groupes de sécurité spécifiques
3. Pour chaque principal de service autorisé : documenter le cas d'usage et effectuer une révision trimestrielle

10.1.11 *Empêcher les principaux de service de créer et utiliser des profils* — Moyen

Profile : E3 Level 1

DESCRIPTION :

Les profils de principal de service dans Fabric peuvent être utilisés pour contourner les restrictions d'accès normales. Restreindre cette capacité limite les vecteurs d'abus potentiels par des applications mal configurées ou compromises.

AUDIT :

- Portail Fabric Admin > "Permettre aux principaux de service de créer et d'utiliser des profils"

REMÉDIATION :

1. Portail Fabric Admin > Paramètres du tenant
2. "Permettre aux principaux de service de créer et d'utiliser des profils" : Désactivé

10.1.12 *Restreindre la création d'espaces de travail Fabric par les principaux de service* — Moyen

Profile : E3 Level 1

DESCRIPTION :

Des principaux de service capables de créer des espaces de travail, connexions et pipelines de déploiement peuvent contourner les workflows de gouvernance et créer des environnements shadow IT dans Fabric.

AUDIT :

- Portail Fabric Admin > "Capacité des principaux de service à créer des espaces de travail, connexions et pipelines"

REMÉDIATION :

1. Portail Fabric Admin > Paramètres du tenant
2. Désactiver la capacité des principaux de service à créer des espaces de travail automatiquement
3. Exiger une validation humaine pour toute création d'espace de travail via API

10.1.13 *Restreindre le partage de datasets Power BI entre espaces de travail (Cross-Workspace)* — Élevé

Profile : E3 Level 1

DESCRIPTION :

La fonctionnalité "Partage de datasets entre espaces de travail" (Cross-Workspace Dataset Sharing) permet aux utilisateurs de connecter des rapports Power BI à des datasets situés dans d'autres espaces de travail auxquels ils n'ont pas nécessairement accès direct. Sans restriction, cette fonctionnalité peut permettre à un utilisateur d'accéder indirectement à des données sensibles via un dataset partagé, contournant les permissions configurées sur l'espace de travail source.

AUDIT :

- Portail d'administration Fabric > Paramètres du tenant > "Autoriser la connexion XMLA et l'utilisation de datasets dans Power BI Desktop"
- Portail d'administration Fabric > Paramètres du tenant > "Partager des datasets avec des utilisateurs extérieurs à votre organisation"

```
# Vérifier via API Fabric Admin
$headers = @{ Authorization = "Bearer $token" }
Invoke-RestMethod -Uri "https://api.fabric.microsoft.com/v1/admin/tenantsettings" -Headers $headers |
    Select-Object -ExpandProperty tenantSettings |
    Where-Object { $_.settingName -match "CrossWorkspace|DatasetShare|XMLA" } |
    Format-Table settingName, enabled, canSpecifySecurityGroups
```

REMÉDIATION :

1. Portail Fabric Admin > Paramètres du tenant > Partage
2. Désactiver "Permettre aux utilisateurs de partager des datasets avec d'autres utilisateurs"
3. Si nécessaire pour des cas légitimes : restreindre à des groupes de sécurité spécifiques
4. Activer le chiffrement RLS (Row-Level Security) sur tous les datasets sensibles
5. Revoir trimestriellement les datasets avec des permissions cross-workspace actives

VALEUR PAR DÉFAUT :

Le partage de datasets entre espaces de travail est activé par défaut dans Fabric.

Section 11 — MICROSOFT 365 APPS — SÉCURITÉ DES APPLICATIONS OFFICE

11.1 — Macros et Code Actif

11.1.1 *Exiger la signature des macros (Require Macro Signing)* — Critique

Déploiement : Intune (Settings Catalog) / GPO AD

MITRE ATT&CK : T1137 (Office Application Startup) · T1204.002 (User Execution: Malicious File) · T1059.005 (Command and Scripting: Visual Basic)

DESCRIPTION :

Les macros VBA non signées représentent l'un des vecteurs d'infection les plus courants dans les campagnes de ransomware et d'espionnage. En exigeant une signature numérique valide pour l'exécution des macros, l'organisation s'assure que seules les macros approuvées et développées en interne peuvent s'exécuter. Les macros dans les documents reçus par email ou téléchargés seront bloquées.

Paramètre GPO :

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security Settings\
→ Exiger la signature des macros = Activé
```

DESCRIPTION :

Ou via Intune : Settings Catalog > Microsoft Office 2016 > Security Settings > Require Macro Signing

```
# Via registre sur poste client
Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\Office\16.0\Common\Security" -Name "RequireAddinSig" -ErrorAction Silentl
# Valeur attendue : 1
```

REMÉDIATION :

1. Intune > Appareils > Profils de configuration > Créer > Windows 10 et ultérieur > Settings Catalog
2. Rechercher "Require Macro Signing" pour chaque application Office concernée
3. Activer et assigner au groupe d'appareils
4. Établir un processus de signature des macros internes (certificat de signature de code interne)

Les macros existantes non signées seront bloquées. Inventaire préalable indispensable.

11.1.2 *Bloquer les macros VBA dans les fichiers Office depuis Internet (MOTW)* — Critique

Déploiement : Intune / GPO AD

MITRE ATT&CK : T1204.002 (User Execution: Malicious File) · T1566.001 (Phishing: Spearphishing Attachment) · T1059.005 (Visual Basic)

DESCRIPTION :

Windows marque les fichiers téléchargés depuis Internet avec une balise "Mark of the Web" (MOTW). Office doit bloquer l'exécution des macros dans tous les fichiers portant cette balise. Depuis 2022, Microsoft a renforcé ce blocage par défaut, mais il peut avoir été désactivé par des GPOs ou des utilisateurs.

Paramètre GPO :

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security Settings\
→ Block macros from running in Office files from the Internet = Enabled
```

```
# Vérifier que le blocage MOTW est actif pour Excel
Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\Office\16.0\Excel\Security" -Name "BlockContentExecutionFromInternet" -Er
# Valeur attendue : 1
```

REMÉDIATION :

1. Intune > Settings Catalog > "Block macros from running in Office files from the Internet" = Enabled
2. Appliquer pour Word, Excel, PowerPoint, Outlook, Visio

11.1.3 *Bloquer les objets OLE actifs dans PowerPoint* — Élevé

Déploiement : Intune / GPO AD

DESCRIPTION :

Les objets OLE (Object Linking and Embedding) embarqués dans des présentations PowerPoint peuvent exécuter du code externe, charger des applications tierces, ou établir des connexions réseau non sécurisées. La baseline v2512 désactive les actions OLE interactives.

Paramètre GPO :

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2016\PowerPoint Options\Security\
→ OLE Active Content = No OLE content will be activated
```

REMÉDIATION :

1. Intune > Settings Catalog > Microsoft PowerPoint 2016 > Security > OLE Active Content > Désactivé

11.1.4 *Bloquer l'exécution de DDE dans Excel* — Critique

Déploiement : Intune / GPO AD

DESCRIPTION :

DDE (Dynamic Data Exchange) est un protocole hérité permettant à Excel de requêter des données depuis d'autres applications ou processus systèmes, y compris cmd.exe et PowerShell. Des documents Excel malveillants exploitent DDE pour exécuter du code arbitraire sans macro VBA, contournant les protections anti-macro.

Paramètre GPO :

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\
→ Don't allow Dynamic Data Exchange (DDE) server launch in Excel = Enabled
```

```
Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\Office\16.0\Excel\Security" -Name "DisableDDEServerLaunch" -ErrorAction S
# Valeur attendue : 1
```

11.1.5 *Bloquer les formats de fichiers Office hérités (Legacy File Block)* — Élevé

Déploiement : Intune / GPO AD

DESCRIPTION :

Les anciens formats Office (.doc, .xls, .ppt pre-2007) contiennent souvent des vulnérabilités connues et non corrigées dans leurs parsers. Bloquer l'ouverture de ces formats réduit la surface d'attaque pour les exploits de format de fichier.

Paramètre GPO :

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security Settings\
→ Legacy File Block = Prevent opening/saving
```

11.1.6 *Désactiver JScript hérité dans Internet Explorer / Zones restreintes Office* — Élevé

Déploiement : Intune / GPO AD

DESCRIPTION :

Le moteur JScript hérité de Microsoft (distinct de V8/Node.js) est utilisé dans la zone Internet d'Internet Explorer et dans certains contextes Office pour exécuter des scripts embarqués dans des documents. Ce moteur présente de nombreuses vulnérabilités CVE critiques. La baseline v2512 désactive JScript dans la zone Internet et la zone Sites restreints pour Office.

Paramètre GPO :

```
Computer Configuration\Administrative Templates\Microsoft Office 2016\Security Settings\
→ Block Legacy JScript Execution = Enabled
```

11.1.7 *Désactiver les add-ins Office non gérés (DisableAllAddIns)* — Élevé

Déploiement : Intune (Settings Catalog) / GPO AD

DESCRIPTION :

Les add-ins Office non gérés (COM add-ins, VSTO add-ins, Web Add-ins tiers non approuvés) représentent un vecteur d'attaque significatif. Des malwares avancés utilisent des add-ins malveillants pour persister dans le système, intercepter des communications Outlook, exfiltrer des données, ou contourner les contrôles de sécurité. Le Microsoft Security Compliance Toolkit v2512 recommande de désactiver tous les add-ins non approuvés et de n'autoriser que les add-ins déployés via le Catalogue d'Applications centralisé (Admin Center).

Paramètre GPO :

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security Settings\
→ Disable All Add-ins = Enabled (Force désactivation de tous les add-ins non gérés)

User Configuration\Administrative Templates\Microsoft Outlook 2016\Miscellaneous\
→ Do not allow Outlook object model scripts to run for shared folders = Enabled
```

```
# Vérifier via Intune — Settings Catalog policy pour Office Add-ins
# Microsoft Intune Admin Center > Devices > Configuration > Policies
# Filtrer par "Office Add-in" ou "DisableAllAddIns"

# Via registry sur les postes (si GPO)
Get-ItemProperty "HKCU:\Software\Microsoft\Office\16.0\Common\General" -Name "DisableAllAddIns" -ErrorAction SilentlyContinue
# Valeur attendue : DisableAllAddIns = 1
```

REMÉDIATION :

1. Intune > Devices > Configuration > Settings Catalog > Créer une politique pour les Apps M365
2. Ajouter le paramètre "Disable All Add-ins" = Enabled
3. Déployer les add-ins légitimes via le Catalogue d'Applications centralisé (Admin Center > Settings > Integrated apps)
4. Créer une liste blanche des add-ins approuvés dans le portail M365
5. Auditer les add-ins actuellement installés sur les postes via Intune Device Reports

VALEUR PAR DÉFAUT :

Les utilisateurs peuvent installer tout add-in disponible dans l'Office Store sans restriction.

11.2 — Protocoles et Connexions Sécurisées

11.2.1 *Bloquer les protocoles non-HTTPS dans les applications Office* — Élevé

Déploiement : Intune / GPO AD

DESCRIPTION :

La baseline v2512 introduit la politique "Block Insecure Protocols" qui bloque tous les protocoles non-HTTPS (HTTP, FTP, etc.) lors de l'ouverture de documents ou de la résolution de liens dans les applications M365. Cela élimine les chemins de déclassement (downgrade) et les connexions non sécurisées pouvant être interceptées.

Paramètre GPO :

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security Settings\
→ Block Insecure Protocols = Enabled
```

11.2.2 *Bloquer les liens externes dans les classeurs Excel (File Block External Links)* — Élevé

Déploiement : Intune / GPO AD

DESCRIPTION :

Les classeurs Excel avec liens vers des fichiers externes bloqués par File Block ne doivent pas pouvoir rafraîchir ces liens. Cela empêche l'ingestion de données depuis des sources non approuvées ou potentiellement malveillantes, et prévient les techniques de reconnaissance utilisant des liens OLE/Excel vers des serveurs attaquants.

Paramètre GPO :

```
User Configuration\Administrative Templates\Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings\
→ File Block includes external link files = Enabled
```

11.2.3 *Bloquer le fallback FPRPC dans les applications Office* — Moyen

Déploiement : Intune / GPO AD

DESCRIPTION :

Le protocole FrontPage Server Extensions RPC (FPRPC) est un protocole d'accès aux fichiers vieillissant, non conçu pour les exigences sécurité modernes. La baseline v2512 désactive le fallback vers FPRPC pour garantir l'utilisation exclusive de méthodes d'accès aux fichiers modernes et authentifiées.

Paramètre GPO :

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security Settings\
→ Restrict Apps from FPRPC Fallback = Enabled
```

11.2.4 *Désactiver les composants OLE Graph hérités (MSGraph.Application)* — Moyen

Déploiement : Intune / GPO AD

DESCRIPTION :

MSGraph.Application et MSGraph.Chart sont des composants OLE Graph classiques qui constituent une interface d'automatisation historiquement risquée. La baseline v2512 remplace leur exécution par un rendu d'image statique, éliminant l'exposition au moteur d'automation sous-jacent.

Paramètre GPO :

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security Settings\
→ Block OLE Graph = Enabled
```

11.2.5 *Désactiver le composant OrgChart Add-in hérité* — Moyen

Déploiement : Intune / GPO AD

DESCRIPTION :

L'add-in OrgChart hérité utilise des frameworks d'automatisation obsolètes. La baseline le désactive et remplace son rendu par une image statique, réduisant l'exposition aux vulnérabilités des frameworks d'automation.

Paramètre GPO :

```
User Configuration\Administrative Templates\Microsoft Office 2016\Security Settings\
→ Block OrgChart = Enabled
```

11.3 — Journaux et Télémétrie Office

11.3.1 *Activer la journalisation des erreurs Office via Intune* — Moyen

Déploiement : Intune / GPO AD

DESCRIPTION :

Les journaux d'erreur et d'utilisation des applications Office permettent de détecter des comportements anormaux (tentatives d'exploitation, crashes répétés sur des fichiers spécifiques) et de corréler avec des indicateurs de compromission.

AUDIT :

- Intune > Politiques de configuration > Vérifier l'activation des journaux Office
- Ou via Registre :

```
Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\Office\16.0\Common" -Name "SendCustomerData" -ErrorAction SilentlyContinu
```

REMÉDIATION :

1. Activer le journal d'audit Office via Intune (Settings Catalog > Office)
2. Configurer l'envoi des journaux vers Microsoft Defender for Endpoint ou le SIEM

11.3.2 *Activer la protection contre les documents malveillants (Protected View renforcé)* Élevé

Déploiement : Intune / GPO AD

DESCRIPTION :

La Protected View d'Office ouvre les documents potentiellement dangereux en mode lecture seule dans un bac à sable, sans activer les macros, les objets OLE, ni les connexions réseau. Forcer l'activation de Protected View pour les fichiers Internet, les pièces jointes Outlook, et les emplacements potentiellement dangereux est une mesure de sécurité critique.

Paramètre GPO :

```
User Configuration\Administrative Templates\Microsoft Word/Excel/PowerPoint\Options\Security\Trust Center\
→ Enable Protected View for files originating from the Internet = Enabled
→ Enable Protected View for files in potentially unsafe locations = Enabled
→ Enable Protected View for Outlook attachments = Enabled
```

Section 12 — GESTION ADMINISTRATIVE

12.1 — Paramètres du Tenant

12.1.1 *Restreindre l'accès au portail d'administration M365* — Élevé

DESCRIPTION :
L'accès au portail Microsoft 365 Admin Center doit être restreint aux administrateurs uniquement. Les utilisateurs standards n'ont pas besoin d'y accéder.

```
Get-MsolCompanyInformation | Select-Object UsersPermissionToReadOtherUsersEnabled, UsersPermissionToUserConsentToAppEnabled
```

REMÉDIATION :
1. M365 Admin Center > Paramètres > Org Settings > Services
2. Désactiver l'accès au portail d'admin pour les non-administrateurs
3. Créer une politique CA : Bloquer l'accès à "Microsoft Admin Portals" pour les non-admins

12.1.2 *Désactiver le consentement des utilisateurs aux applications tierces* — Élevé

DESCRIPTION :
Par défaut, les utilisateurs peuvent donner leur consentement à des applications tierces pour accéder à leurs données M365 (emails, fichiers, contacts). Des applications malveillantes exploitent cela pour obtenir un accès persistant (OAuth Phishing).

```
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions | Select-Object AllowedToCreateApps, AllowedToCreateSecurityGroups, Al
Get-MgPoliciesPermissionGrantPolicies
```

REMÉDIATION :
1. Entra ID > Applications d'entreprise > Paramètres utilisateur
2. "Les utilisateurs peuvent donner leur consentement aux applications accédant aux données de l'entreprise" → Non
3. Activer le workflow de consentement administrateur pour que les utilisateurs puissent demander l'approbation
4. Réviser les applications ayant déjà reçu des consentements larges

12.1.3 *Activer les restrictions de création de tenants* — Moyen

DESCRIPTION :
Sans restrictions, les utilisateurs peuvent créer de nouveaux tenants Entra ID avec leur adresse email professionnelle pour contourner les contrôles de sécurité de l'organisation.

```
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions.AllowedToCreateTenants
```

```
$permissionsObject = (Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions
$permissionsObject.AllowedToCreateTenants = $false
Update-MgPolicyAuthorizationPolicy -DefaultUserRolePermissions $permissionsObject
```

12.1.4 *Restreindre l'enregistrement d'appareils par les utilisateurs* — Moyen

DESCRIPTION :
Limiter quels utilisateurs peuvent enregistrer des appareils dans Entra ID empêche l'enregistrement non autorisé d'appareils personnels qui pourraient obtenir des tokens d'accès ou contourner des politiques CA basées sur les appareils.

AUDIT :
- Entra ID > Appareils > Paramètres d'appareil > Les utilisateurs peuvent joindre des appareils à Azure AD

REMÉDIATION :
1. Entra ID > Appareils > Paramètres d'appareil
2. "Les utilisateurs peuvent joindre des appareils à Azure AD" : Sélectionné (groupe restreint) au lieu de Tous
3. Nombre maximum d'appareils par utilisateur : 5 (ou selon politique interne)

12.1.5 *Vérifier la configuration des domaines personnalisés* — Moyen

DESCRIPTION :
Les domaines personnalisés non vérifiés ou mal configurés peuvent être utilisés pour l'usurpation d'identité. Tous les domaines associés au tenant doivent avoir leurs enregistrements DNS correctement configurés.

AUDIT :
- M365 Admin Center > Paramètres > Domaines
- Vérifier le statut de chaque domaine (Sain / Avertissements)

REMÉDIATION :
1. Résoudre tous les avertissements DNS sur les domaines personnalisés
2. S'assurer que SPF, DKIM et DMARC sont configurés pour TOUS les domaines
3. Supprimer les domaines inutilisés du tenant

12.1.6 *Restreindre l'accès au Microsoft Office Store pour les utilisateurs* Élevé

Profile : E3 Level 1

DESCRIPTION :

Par défaut, les utilisateurs peuvent accéder à l'Office Store et installer des applications et compléments Microsoft 365 de leur propre initiative. Ces applications non gérées peuvent accéder aux données M365 (emails, fichiers, contacts), introduire des risques de sécurité et contourner les politiques DLP.

```
$Uri = "https://graph.microsoft.com/beta/admin/appsAndServices/settings"
Invoke-MgGraphRequest -Uri $Uri
# Valeurs attendues : isAppAndServicesTrialEnabled = false, isOfficeStoreEnabled = false
```

```
$uri = "https://graph.microsoft.com/beta/admin/appsAndServices"
$body = @{
    Settings = @{
        isAppAndServicesTrialEnabled = $false
        isOfficeStoreEnabled = $false
    }
} | ConvertTo-Json
Invoke-MgGraphRequest -Method PATCH -Uri $uri -Body $body
```

REMÉDIATION :

Ou via M365 Admin Center > Paramètres > Paramètres Org > Services > Applications et services.

12.1.7 *Activer la protection phishing interne pour Microsoft Forms* Élevé

Profile : E3 Level 1

DESCRIPTION :

Microsoft Forms dispose d'une protection anti-phishing interne qui détecte lorsque des formulaires sont utilisés pour des attaques de phishing en interne (collecte de credentials, informations sensibles). Des attaquants ayant compromis un compte peuvent créer des formulaires de phishing pour cibler d'autres employés.

```
$uri = 'https://graph.microsoft.com/beta/admin/forms/settings'
(Invoke-MgGraphRequest -Uri $uri).isInOrgFormsPhishingScanEnabled
# Valeur attendue : True
```

```
$uri = 'https://graph.microsoft.com/beta/admin/forms/settings'
$body = @{ isInOrgFormsPhishingScanEnabled = $true } | ConvertTo-Json
Invoke-MgGraphRequest -Method PATCH -Uri $uri -Body $body
```

12.1.8 *Activer Customer Lockbox pour les accès Microsoft au tenant* Moyen

Profile : E5 Level 2

Licence requise : Microsoft 365 E5 ou Microsoft 365 E5 Compliance

DESCRIPTION :

Customer Lockbox garantit que Microsoft ne peut pas accéder aux données client sans approbation explicite. Quand le support Microsoft doit accéder aux données pour résoudre un incident, une demande d'approbation est envoyée à l'administrateur du tenant. Sans Customer Lockbox, Microsoft peut accéder aux données avec uniquement une notification interne.

```
Get-OrganizationConfig | Select-Object CustomerLockBoxEnabled
# Valeur attendue : True
```

```
Set-OrganizationConfig -CustomerLockBoxEnabled $true
```

REMÉDIATION :

Ou via M365 Admin Center > Paramètres > Paramètres Org > Sécurité et confidentialité > Customer Lockbox.

12.1.9 *Restreindre les services de stockage tiers dans Microsoft 365 Web* Moyen

Profile : E3 Level 2

DESCRIPTION :

Par défaut, les applications web M365 (Word, Excel, PowerPoint Online) permettent d'ouvrir et sauvegarder des fichiers depuis des services tiers comme Dropbox, Box ou Google Drive. Cela peut conduire à des fuites de données sensibles vers des espaces non contrôlés par l'organisation.

```
$SP = Get-MgServicePrincipal -Filter "appId eq 'c1f33bc0-bdb4-4248-ba9b-096807ddb43e'"
if ((-not $SP) -or $SP.AccountEnabled) {
    Write-Host "NON CONFORME - Stockages tiers autorisés"
} else {
    Write-Host "CONFORME - Stockages tiers bloqués"
}
```

```
$SP = Get-MgServicePrincipal -Filter "appId eq 'c1f33bc0-bdb4-4248-ba9b-096807ddb43e'"
if (-not $SP) { $SP = New-MgServicePrincipal -AppId "c1f33bc0-bdb4-4248-ba9b-096807ddb43e" }
Update-MgServicePrincipal -ServicePrincipalId $SP.Id -AccountEnabled:$false
```

12.1.10 *Désactiver le partage externe de Sway* Moyen

Profile : E3 Level 1

DESCRIPTION :

Sway est un outil de création de présentations interactives. Par défaut, les utilisateurs peuvent partager leurs Sways publiquement avec des personnes extérieures à l'organisation. Des Sways peuvent contenir des informations stratégiques, des données RH ou des plans commerciaux qui ne doivent pas être accessibles publiquement.

AUDIT :

1. M365 Admin Center > Paramètres > Paramètres Org > Services
2. Rechercher "Sway"
3. Vérifier que "Permettre aux personnes de votre organisation de partager leurs Sways avec des personnes extérieures" est décoché

REMÉDIATION :

1. M365 Admin Center > Paramètres > Paramètres Org > Services > Sway
2. Décocher "Permettre aux personnes de votre organisation de partager leurs Sways avec des personnes extérieures à votre organisation"

12.1.11 *Restreindre ou désactiver Microsoft Bookings* Moyen

Profile : E3 Level 2

DESCRIPTION :

Microsoft Bookings permet aux utilisateurs externes de réserver des créneaux avec les employés de l'organisation, exposant publiquement les calendriers et les coordonnées du personnel. Ce service peut également permettre la création de boîtes partagées Bookings non gérées, augmentant la surface d'attaque.

```
Get-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default | Select-Object BookingsMailboxCreationEnabled
Get-OrganizationConfig | Select-Object BookingsEnabled
# Valeurs attendues : les deux à False
```

```
Set-OwaMailboxPolicy "OwaMailboxPolicy-Default" -BookingsMailboxCreationEnabled:$false
Set-OrganizationConfig -BookingsEnabled $false
```

13.0 — RÉPONSE AUX INCIDENTS ET PLANS DE CONTINUITÉ

13.1.1 *Documenter les procédures de réponse aux incidents M365* — Moyen

DESCRIPTION :
L'absence de procédures documentées pour les incidents M365 (compromission de compte, ransomware via email, fuite de données) retarde significativement la réponse et augmente l'impact de l'incident.

AUDIT :
- Vérifier l'existence d'un plan de réponse aux incidents documenté spécifique M365
- Vérifier que les procédures incluent : isolation de compte compromis, révocation de sessions, analyse forensic M365

REMÉDIATION :
1. Documenter les procédures pour les scénarios : Compte admin compromis, Règle de transfert malveillante, Ransomware via SharePoint, Business Email Compromise (BEC)
2. Tester les procédures via des exercices de simulation (tabletop exercises) annuels
3. Maintenir les contacts Microsoft DART (Detection and Response Team) pour les incidents critiques

13.1.2 *Activer la journalisation avancée (Audit Premium)* — Moyen

Licence requise : Microsoft 365 E5 ou Microsoft 365 E5 Compliance

DESCRIPTION :
L'Audit Premium de Microsoft Purview offre une rétention des journaux de 1 an (voire 10 ans), une bande passante d'API accrue pour les enquêtes forensics, et des événements d'audit supplémentaires critiques pour les investigations (MailItemsAccessed, SearchQueryInitiatedExchange, etc.).

```
Get-Mailbox -Identity user@domain.com | Select-Object AuditEnabled, DefaultAuditSet
```

REMÉDIATION :
1. Assigner la licence Microsoft Purview Audit (Premium) aux utilisateurs prioritaires (dirigeants, IT, finance)
2. Activer l'audit MailItemsAccessed pour détecter les accès à des emails spécifiques lors d'investigations
3. Configurer l'exportation vers un SIEM pour rétention à long terme

13.1.3 *Maintenir des playbooks de réponse aux incidents BEC et ransomware* — Élevé

Profile : E3 Level 1

DESCRIPTION :
La compromission de messagerie d'entreprise (BEC) et les ransomwares sont les deux principales menaces M365. Sans playbooks documentés et testés, le temps de réponse en cas d'incident est multiplié par 3 à 5 et les erreurs critiques (mauvaises réinitialisations, non-préservation des preuves) sont fréquentes. Les playbooks doivent être spécifiques à M365 et inclure les actions PowerShell/API nécessaires.

AUDIT :
- Documentation de l'organisation > Existence de playbooks IR M365 (BEC, ransomware, phishing, accès admin compromis)
- Vérifier la date du dernier test/simulation (< 12 mois)
- Vérifier la liste des comptes Break Glass et leur procédure d'activation

REMÉDIATION :
1. Créer un playbook BEC couvrant :
2. Détection via Defender for Office 365 Alert
3. Révocation immédiate des sessions (`Revoke-MgUserSignInSession`)
4. Reset MFA et MDP
5. Investigation des règles de transfert et délégations suspectes
6. Analyse des emails exfiltrés via eDiscovery
7. Créer un playbook Ransomware couvrant :
8. Isolation de l'appareil compromis via Intune
9. Blocage de compte M365
10. Restauration OneDrive/SharePoint via versioning (180 jours)
11. Analyse de propagation via Microsoft 365 Defender
12. Tester les playbooks annuellement via simulation tabletop
13. Référence : Microsoft Incident Response Playbooks — https://aka.ms/IRplaybooks

VALEUR PAR DÉFAUT :
Aucun playbook IR spécifique M365 n'est fourni par défaut.

13.1.4 *Activer et tester la sauvegarde M365 (backup tiers ou natif)* Élevé

Profile : E3 Level 1

Licence requise : Microsoft 365 Backup (module add-on) ou solution tierce

DESCRIPTION :

Microsoft n'est pas responsable de la sauvegarde des données M365 — sa responsabilité est la disponibilité de la plateforme, pas la récupération en cas de suppression accidentelle, de ransomware ou d'erreur administrative. Les outils natifs (corbeille, versioning) ont des limitations (30–93 jours). Une solution de sauvegarde dédiée est nécessaire pour les SLA de récupération critiques.

```
# Vérifier si Microsoft 365 Backup est configuré
$backupPolicy = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/beta/admin/m365Apps/installation/backupPolicies" -Method GE
$backupPolicy | ConvertTo-Json
```

AUDIT :

- Vérifier aussi : solution tierce active (Veeam, Acronis, Druva, Barracuda, AvePoint)
- Tester la restauration d'une boîte mail et d'un site SharePoint < 12 mois

REMÉDIATION :

1. Option 1 — Microsoft 365 Backup (natif) :
2. Microsoft 365 Admin Center > Settings > Microsoft 365 Backup
3. Configurer les politiques de sauvegarde pour Exchange, SharePoint, OneDrive
4. RTO/RPO : restauration en minutes pour les 180 derniers jours
5. Option 2 — Solution tierce : déployer et configurer selon la politique de l'organisation
6. Documenter le processus de restauration et le tester annuellement
7. Vérifier que les sauvegardes sont stockées hors du tenant (protection contre suppression admin)

VALEUR PAR DÉFAUT :

Aucune sauvegarde dédiée M365 par défaut.

Section 14 — MICROSOFT COPILOT FOR M365

14.1 — Gouvernance et Sécurité de Microsoft Copilot for M365

14.1.1 *Évaluer le périmètre d'oversharing avant le déploiement Copilot*

Critique

Profile : E5 / Copilot for M365 Add-on

Licence requise : Microsoft 365 Copilot + Purview DSPM for AI (add-on)

DESCRIPTION :

Copilot accède aux données via le Microsoft Graph — toutes les données accessibles par l'utilisateur sont potentiellement accessibles à Copilot. En entreprise, il est courant que des données sensibles (RH, financier, juridique) soient accessibles à des utilisateurs qui n'auraient pas dû y avoir accès. Avant tout déploiement Copilot, un audit d'oversharing doit être réalisé via Microsoft Purview DSPM for AI (Data Security Posture Management).

```
# Vérifier les sites SharePoint avec "Tout le monde sauf les utilisateurs externes"
$sites = Get-PnPTenantSite -Detailed
$sites | Where-Object { $_.SharingCapability -eq "ExternalUserAndGuestSharing" } | Select-Object Url, Title

# Identifier les fichiers partagés avec "Tout le monde"
# À exécuter via Purview Content Explorer ou DSPM for AI
```

AUDIT :

- Microsoft Purview > DSPM for AI > Rapport d'oversharing
- Vérifier que les sites SharePoint sensibles n'ont pas de permissions "Tout le monde"

REMÉDIATION :

1. Déployer Microsoft Purview DSPM for AI et générer le rapport d'oversharing
2. Identifier les 10 sites/bibliothèques les plus à risque et restreindre les permissions
3. Supprimer les partages "Tout le monde" et "Tout le monde sauf les utilisateurs externes"
4. Activer la restriction d'accès aux sites SharePoint selon les étiquettes de sensibilité
5. Déployer une politique "SharePoint Advanced Management" pour audit continu
6. Ne pas activer Copilot avant que le score DSPM soit acceptable

VALEUR PAR DÉFAUT :

Aucune évaluation d'oversharing — Copilot peut exposer toutes les données accessibles à l'utilisateur.

14.1.2 *Configurer les politiques DLP spécifiques à Copilot*

Critique

Profile : E5 / Copilot for M365 Add-on

Licence requise : Microsoft 365 Copilot + Purview DLP

DESCRIPTION :

Les politiques DLP (Data Loss Prevention) doivent être étendues pour couvrir les interactions Copilot. Sans DLP spécifique, Copilot peut inclure dans ses réponses des données sensibles (numéros de carte, données santé, données personnelles RGPD) qui se retrouvent dans des prompts partagés ou des résumés.

```
# Vérifier les politiques DLP actives et leurs emplacements
Connect-IPPSSession
$policies = Get-DlpCompliancePolicy | Where-Object { $_.Mode -eq "Enable" }
$policies | Select-Object Name, Mode, ExchangeLocation, SharePointLocation | Format-Table

# Vérifier si les politiques couvrent Copilot (Microsoft365CopilotWorkloads)
$policies | Where-Object { $_.Workload -match "Copilot" } | Select-Object Name
```

REMÉDIATION :

1. Microsoft Purview > Prévention des pertes de données > Stratégies > Nouvelle stratégie
2. Créer une stratégie DLP dédiée "Copilot" couvrant :
3. Exchange Online + Teams + SharePoint + OneDrive + Copilot interactions
4. Définir des règles pour détecter et bloquer : numéros de carte bancaire, NIR, données santé, mots de passe
5. Configurer les actions : bloquer, notifier l'utilisateur, log dans le portail de conformité
6. Activer la surveillance des interactions Copilot via Purview Communication Compliance

VALEUR PAR DÉFAUT :

Aucune politique DLP spécifique à Copilot configurée.

14.1.3 *Activer la journalisation et l'audit des interactions Copilot* Élevé

Profile : E5 / Copilot for M365 Add-on

Licence requise : Microsoft 365 Copilot + Purview Audit Premium

DESCRIPTION :

Toutes les interactions Copilot (prompts et réponses) doivent être journalisées pour permettre l'investigation en cas d'incident (fuite de données, usage inapproprié, accès non autorisé). Les logs Copilot sont stockés dans Microsoft Purview et disponibles via Audit Premium.

```
# Vérifier l'état de l'audit unifié
Connect-IPPSSession
Get-AdminAuditLogConfig | Select-Object UnifiedAuditLogIngestionEnabled

# Rechercher les événements Copilot dans les logs
$startDate = (Get-Date).AddDays(-30)
$endDate = Get-Date
Search-UnifiedAuditLog -StartDate $startDate -EndDate $endDate -RecordType CopilotInteraction -ResultSize 10 |
    Select-Object CreationDate, UserIds, Operations | Format-Table
```

REMÉDIATION :

1. Vérifier que le journal d'audit unifié est actif (voir contrôle 8.1.1)
2. Microsoft Purview > Audit > Recherche d'audit > Filtrer par "Copilot"
3. Configurer des alertes sur les interactions Copilot anormales (volume élevé, données sensibles)
4. Activer Microsoft Purview Communication Compliance pour surveillance continue
5. Exporter les logs Copilot vers le SIEM pour corrélation

VALEUR PAR DÉFAUT :

Journalisation des interactions Copilot non activée par défaut.

14.1.4 *Contrôler les plugins et extensions Copilot tiers* Élevé

Profile : E5 / Copilot for M365 Add-on

Licence requise : Microsoft 365 Copilot + App Governance

DESCRIPTION :

Les plugins Copilot (connecteurs tiers, extensions d'agents Copilot) peuvent accéder à des données sensibles et les transmettre à des services externes. Sans gouvernance, les utilisateurs peuvent installer des plugins non approuvés qui créent des risques de fuite de données ou d'injection de prompts malveillants.

```
# Vérifier les consentements d'applications tiers pour Copilot
$apps = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/servicePrincipals?`$filter=tags/any(t:t eq 'WindowsAzureActive
$apps.value | Select-Object displayName, appId | Format-Table

# Lister les agents Copilot déployés
# Microsoft 365 Admin Center > Copilot > Agents
```

REMÉDIATION :

1. Microsoft 365 Admin Center > Settings > Integrated apps > Gérer les plugins Copilot
2. Désactiver les plugins tiers non approuvés par le service IT
3. Créer une liste d'applications Copilot approuvées
4. Activer Microsoft App Governance pour surveiller les comportements des plugins
5. Configurer le consentement administrateur obligatoire pour tous les nouveaux plugins Copilot (voir contrôle 1.5.x)

VALEUR PAR DÉFAUT :

Tous les plugins disponibles dans le store peuvent être installés par les utilisateurs.

14.1.5 *Appliquer les étiquettes de sensibilité aux contenus générés par Copilot* Élevé

Profile : E5 / Copilot for M365 Add-on

Licence requise : Microsoft 365 Copilot + AIP/Purview P2

DESCRIPTION :

Les documents créés ou modifiés par Copilot doivent hériter de l'étiquette de sensibilité la plus élevée des sources utilisées. Sans cette configuration, Copilot peut créer un document non classifié en se basant sur des contenus Confidentiels — le document résultant ne sera pas protégé.

```
# Vérifier les politiques d'étiquettes auto-appliquées
Connect-IPPSSession
Get-AutoSensitivityLabelPolicy | Select-Object Name, Mode, ApplySensitivityLabel | Format-Table

# Vérifier si Copilot est configuré pour hériter des étiquettes
Get-LabelPolicy | Select-Object Name, Settings | Format-Table
```

REMÉDIATION :

1. Microsoft Purview > Protection des informations > Étiquettes de sensibilité > Paramètres Copilot
2. Activer "Copilot doit utiliser l'étiquette la plus restrictive parmi les contenus référencés"
3. Configurer des politiques d'étiquetage automatique pour les contenus générés par IA
4. Former les utilisateurs à vérifier les étiquettes des documents générés par Copilot

VALEUR PAR DÉFAUT :

Copilot ne propage pas les étiquettes de sensibilité automatiquement.

14.1.6 *Gouverner les licences Copilot et restreindre l'accès aux groupes autorisés*

Moyen

Profile : E5 / Copilot for M365 Add-on

Licence requise : Microsoft 365 Copilot (add-on)

DESCRIPTION :

Les licences Copilot doivent être assignées de manière contrôlée via des groupes d'approbation, et non distribués massivement. Un utilisateur avec Copilot peut accéder et synthétiser en secondes des volumes de données auxquels il aurait normalement accès mais ne consulterait jamais. Une gouvernance stricte des licences réduit la surface d'exposition.

```
# Lister les utilisateurs avec licence Copilot
Get-MgUser -All | Where-Object {
    $_.AssignedLicenses.SkuId -contains "639dec6b-bb19-468b-871c-c5c441c4b0cb" # SKU Copilot M365
} | Select-Object DisplayName, UserPrincipalName | Format-Table

# Vérifier le nombre total de licences utilisées
(Get-MgSubscribedSku | Where-Object { $_.SkuPartNumber -like "*COPILOT*" }).ConsumedUnits
```

REMÉDIATION :

1. Microsoft 365 Admin Center > Facturation > Licences > Microsoft 365 Copilot
2. Créer un groupe de sécurité "Copilot-Autorisés" pour l'assignation des licences
3. Définir un processus d'approbation (manager + IT) pour les nouvelles demandes Copilot
4. Revoir trimestriellement la liste des utilisateurs Copilot et retirer les licences inutilisées
5. Lier l'activation Copilot à la completion d'une formation sur l'utilisation responsable de l'IA

VALEUR PAR DÉFAUT :

Les licences peuvent être assignées sans processus d'approbation.

14.1.7 *Détecter et bloquer les attaques par injection de prompt (Prompt Injection) dans Copilot*

Élevé

MITRE ATT&CK : T1059 (Command and Scripting Interpreter) · T1534 (Internal Spearphishing) · T1656 (Impersonation)

Licence requise : Microsoft 365 Copilot + Purview Communication Compliance

DESCRIPTION :

Les attaques par injection de prompt ciblent Copilot for M365 de deux façons : (1) **Injection directe** — un utilisateur malveillant formule un prompt conçu pour contourner les garde-fous de Copilot et accéder à des données auxquelles il n'aurait normalement pas accès ; (2) **Injection indirecte** — un document SharePoint ou un email contient des instructions cachées (texte blanc sur fond blanc, métadonnées) qui manipulent Copilot lorsqu'il traite ce contenu pour exfiltrer des informations. Ces attaques sont difficiles à détecter sans surveillance spécifique.

```
# Rechercher des interactions Copilot anormales dans les logs d'audit
Connect-IPPSSession
$startDate = (Get-Date).AddDays(-30)
Search-UnifiedAuditLog -StartDate $startDate -EndDate (Get-Date) `
    -RecordType CopilotInteraction -ResultSize 100 |
    Select-Object CreationDate, UserIds, Operations, AuditData |
    Where-Object { $_.AuditData -match "SharePoint|OneDrive" } |
    Format-Table

# Rechercher des documents SharePoint avec du texte masqué (indicateur d'injection)
# Purview > Content Search > filtrer par type de document et contenu suspect
```

REMÉDIATION :

1. Activer Microsoft Purview Communication Compliance avec politique de surveillance Copilot
2. Configurer des alertes sur les prompts contenant des patterns suspects (ex: "ignore previous instructions", "act as", injections en base64)
3. Activer la protection Purview Information Barriers pour prévenir les accès croisés non autorisés
4. Sensibiliser les utilisateurs aux risques d'injection via des documents SharePoint/email malveillants
5. Mettre en place une révision périodique des interactions Copilot à haut volume ou hors périmètre habituel
6. Activer Microsoft Defender XDR pour la détection des comportements Copilot anormaux

VALEUR PAR DÉFAUT :

Aucune protection spécifique contre les injections de prompt dans Copilot.

14.1.8 *Détecter les comptes zombies avec licences M365 actives (License Hygiene)* Moyen

MITRE ATT&CK : T1078 (Valid Accounts) · T1078.004 (Valid Accounts: Cloud) · T1531 (Account Access Removal)

Licence requise : Microsoft 365 (toute édition)

DESCRIPTION :

Les comptes "zombies" (utilisateurs désactivés ou partis depuis > 30 jours) qui conservent des licences M365 actives représentent un double problème : (1) **Risque de sécurité** — un compte désactivé peut être réactivé par un attaquant ou un insider, conservant ses accès et données ; (2) **Coût inutile** — chaque licence non recyclée représente un surcoût mensuel. Les licences Copilot (≈ 30$/user/mois) sont particulièrement importantes à récupérer. Une bonne hygiène de licences est aussi un signal de maturité en cybersécurité.

```
# Identifier comptes désactivés avec des licences actives
$disabledWithLicenses = Get-MgUser -All -Filter "accountEnabled eq false" `
    -Property "displayName,userPrincipalName,accountEnabled,assignedLicenses,signInActivity" |
    Where-Object { $_.AssignedLicenses.Count -gt 0 } |
    Select-Object DisplayName, UserPrincipalName,
        @{N="Licences";E={$_.AssignedLicenses.Count}},
        @{N="DernièreConnexion";E={$_.SignInActivity.LastSignInDateTime}}
$disabledWithLicenses | Format-Table
Write-Host "Total comptes zombies avec licences: $($disabledWithLicenses.Count)" -ForegroundColor Red

# Identifier comptes avec licence Copilot inactifs depuis > 90 jours
$copilotSku = "639dec6b-bb19-468b-871c-c5c441c4b0cb"
$staleDate = (Get-Date).AddDays(-90)
Get-MgUser -All -Property "displayName,userPrincipalName,assignedLicenses,signInActivity" |
    Where-Object {
        $_.AssignedLicenses.SkuId -contains $copilotSku -and
        ($_.SignInActivity.LastSignInDateTime -lt $staleDate -or $_.SignInActivity.LastSignInDateTime -eq $null)
    } | Select-Object DisplayName, UserPrincipalName | Format-Table
```

REMÉDIATION :

1. Supprimer immédiatement les licences des comptes désactivés
2. Mettre en place un processus de départ automatisé (offboarding) : désactivation → retrait licence → archivage → suppression (90 jours)
3. Configurer une Access Review automatique trimestrielle pour les comptes inactifs depuis > 90 jours
4. Récupérer en priorité les licences Premium (Copilot, E5, Entra ID P2)
5. Intégrer la revue de licences dans le processus RH de départ

VALEUR PAR DÉFAUT :

Les licences sont conservées sur les comptes désactivés jusqu'à suppression manuelle.

14.1.9 *Désactiver ou restreindre la recherche Web dans Copilot pour M365* Élevé

DESCRIPTION :

La recherche Web dans Copilot permet à l'outil d'interroger Bing lors d'une interaction. Des prompts contenant des données internes sensibles (noms de projets confidentiels, clients, données financières) peuvent ainsi être partiellement exposés à des moteurs de recherche externes ou au traitement Bing. Dans les environnements haute sécurité, cette fonctionnalité doit être désactivée ou limitée aux utilisateurs autorisés.

AUDIT :

- Microsoft 365 Admin Center > Paramètres > Copilot > Recherche Web
- Ou via Microsoft 365 Apps Admin Center > Paramètres de confidentialité Copilot

REMÉDIATION :

1. Microsoft 365 Admin Center > Paramètres > Microsoft Copilot
2. Désactiver "Autoriser les utilisateurs à utiliser la recherche Web dans Copilot"
3. Si recherche web nécessaire pour certains groupes : créer une stratégie ciblée
4. Informer les utilisateurs de la désactivation et des raisons de sécurité

VALEUR PAR DÉFAUT :

Recherche Web activée — les prompts peuvent interroger Bing.

14.1.10 *Gouverner la création d'agents Copilot personnalisés par les utilisateurs* Élevé

DESCRIPTION :

Microsoft 365 Copilot permet aux utilisateurs de créer des "agents" (Custom Copilot) qui peuvent accéder à des sources de données spécifiques, exécuter des actions et être partagés avec d'autres utilisateurs. Sans gouvernance, un utilisateur peut créer un agent malveillant ou mal configuré qui exfiltre des données via des prompts, partage des informations sensibles avec des utilisateurs non autorisés, ou interagit avec des API externes non approuvées.

AUDIT :

- Microsoft 365 Admin Center > Paramètres > Copilot > Agents et plugins
- Vérifier qui peut créer et publier des agents

REMÉDIATION :

1. Restreindre la création d'agents Copilot aux utilisateurs/groupes approuvés
2. Exiger une approbation IT avant la publication d'un agent à d'autres utilisateurs
3. Activer l'audit des agents créés dans Microsoft Purview
4. Revoir trimestriellement les agents publiés dans l'organisation

VALEUR PAR DÉFAUT :

Tous les utilisateurs Copilot peuvent créer et partager des agents.

14.1.11 *Configurer la rétention et l'audit des interactions Copilot (prompts et réponses)* Élevé

DESCRIPTION :
Les interactions Copilot (prompts et réponses) doivent être journalisées dans Microsoft Purview pour permettre l'investigation forensic en cas d'incident : fuite de données, utilisation inappropriée, ou injection de prompt réussie. Sans journalisation, il est impossible de déterminer quelles données ont été exposées lors d'un incident impliquant Copilot.

```
# Vérifier que les événements Copilot sont dans l'audit log
Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-7) -EndDate (Get-Date) `
    -RecordType CopilotInteraction -ResultSize 10 | Select-Object CreationDate, UserIds, Operations
# Résultat attendu : événements présents si Copilot est utilisé
```

REMÉDIATION :
1. S'assurer que l'Unified Audit Log est activé (contrôle 6.1.1)
2. Microsoft Purview > Audit > Vérifier que "CopilotInteraction" est dans les événements journalisés
3. Créer une politique de rétention Purview couvrant les interactions Copilot (12 mois minimum)
4. Configurer des alertes sur les interactions avec des fichiers hautement sensibles (label Confidentiel)

VALEUR PAR DÉFAUT :
Interactions Copilot dans l'audit log si UAL activé — mais pas de politique de rétention spécifique.

Section 15 — ATTACK PATH & IDENTITY EXPOSURE

15.1 — Chemins d'Escalade vers les Privilèges Globaux

15.1.1 *Auditer les chemins d'escalade vers Global Administrator (Attack Path)*

Critique

DESCRIPTION :
Un chemin d'attaque vers Global Administrator existe quand une identité non-privilégiée peut atteindre ce rôle en une ou plusieurs étapes : via une App Registration avec permissions `RoleManagement.ReadWrite.Directory`, via un group owner d'un groupe assigné au rôle GA, via un SP avec credentials non sécurisés et droits élevés, ou via une Workload Identity Federation mal configurée. Ces chemins sont souvent invisibles dans les audits de configuration classiques.

```
# Identifier les identités pouvant s'escalader vers Global Admin
# Étape 1 : Apps avec RoleManagement.ReadWrite.Directory
$dangerous = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/servicePrincipals?`$expand=appRoleAssignments" -Method GE
$escalationPaths = @()

# Étape 2 : Propriétaires de groupes assignés à des rôles
$gaRole = Get-MgDirectoryRole -Filter "DisplayName eq 'Global Administrator'"
$gaGroups = Get-MgDirectoryRoleMember -DirectoryRoleId $gaRole.Id -All | Where-Object { $_.'@odata.type' -eq '#microsoft.graph.grou
foreach ($group in $gaGroups) {
    $owners = Get-MgGroupOwner -GroupId $group.Id
    $escalationPaths += $owners | ForEach-Object {
        [PSCustomObject]@{ Type = "GroupOwner→GA"; Identity = $_.AdditionalProperties.displayName; Via = $group.AdditionalPropertie
    }
}
$escalationPaths | Format-Table
Write-Host "⚠️ Chemins d'escalade vers GA identifiés : $($escalationPaths.Count)"
```

REMÉDIATION :

1. Pour chaque chemin d'escalade identifié : évaluer la légitimité et corriger
2. Supprimer les App Registrations non nécessaires avec permissions de gestion des rôles
3. Convertir les assignations de groupes directs en PIM for Groups
4. Activer Microsoft Security Exposure Management pour la détection continue des attack paths
5. Revoir trimestriellement les chemins d'escalade avec l'équipe SecOps

VALEUR PAR DÉFAUT :
Aucune détection automatique des chemins d'escalade — visibles uniquement via audit manuel ou outils spécialisés.

15.1.2 *Détecter les scénarios de contournement des politiques CA (CA Policy Bypass)*

Critique

DESCRIPTION :
Les politiques CA peuvent être contournées via : des exclusions trop larges (groupes entiers exclus), des applications non couvertes (toutes les apps cloud ≠ toutes les apps réellement utilisées), des protocoles legacy non bloqués, ou des comptes service exclus sans justification. Un attaquant qui identifie ces angles morts peut s'y engouffrer. Microsoft propose un outil d'analyse des lacunes CA dans le portail Entra.

```
# Analyser les lacunes CA : utilisateurs exclus de la politique MFA principale
$mfaPolicy = Get-MgIdentityConditionalAccessPolicy -All | Where-Object {
    $_.State -eq "enabled" -and
    $_.Conditions.Users.IncludeUsers -contains "All" -and
    $_.GrantControls.BuiltInControls -contains "mfa"
}
foreach ($policy in $mfaPolicy) {
    $excludedUsers = $policy.Conditions.Users.ExcludeUsers.Count
    $excludedGroups = $policy.Conditions.Users.ExcludeGroups.Count
    Write-Host "Politique: $($policy.DisplayName)"
    Write-Host "  Utilisateurs exclus : $excludedUsers"
    Write-Host "  Groupes exclus      : $excludedGroups"
    if ($excludedUsers + $excludedGroups -gt 5) {
        Write-Host "  ⚠️ Nombre d'exclusions élevé — risque de lacune CA" -ForegroundColor Yellow
    }
}
# Portail : Entra ID > Protection > CA > Insights & Reporting > What If
```

REMÉDIATION :

1. Utiliser l'outil "What If" CA pour simuler des scénarios d'accès suspects
2. Réduire les exclusions au strict minimum (seulement Break Glass + comptes de service documentés)
3. Vérifier que les applications critiques (Exchange, SharePoint, Teams, Azure Portal) sont toutes couvertes
4. Activer le mode "Rapport seul" pour tester les nouvelles politiques avant activation
5. Revoir toutes les exclusions CA mensuellement

VALEUR PAR DÉFAUT :
Aucun outil de détection des lacunes CA — les bypass sont identifiables uniquement par revue manuelle.

15.1.3 *Auditer les scénarios d'abus de relations cross-tenant (Cross-Tenant Trust Abuse)* Élevé

DESCRIPTION :
Les relations B2B cross-tenant peuvent être exploitées si la politique d'accès cross-tenant est trop permissive : un tenant partenaire compromis peut utiliser sa relation de confiance pour pivoter vers votre tenant. Les paramètres de "trust MFA" (faire confiance au MFA du tenant partenaire) sont particulièrement risqués si le tenant partenaire a une posture MFA faible.

```
# Vérifier les paramètres de confiance cross-tenant
$xtapDefault = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/policies/crossTenantAccessPolicy/default" -Method GET
Write-Host "Trust MFA externe : $($xtapDefault.inboundTrust.isMfaAccepted)"
Write-Host "Trust Compliant Device externe : $($xtapDefault.inboundTrust.isCompliantDeviceAccepted)"
if ($xtapDefault.inboundTrust.isMfaAccepted -eq $true) {
    Write-Host "⚠️ CRITIQUE : Vous faites confiance au MFA de tenants externes inconnus" -ForegroundColor Red
}

# Vérifier les partenaires avec trust MFA spécifique
$partners = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/policies/crossTenantAccessPolicy/partners" -Method GET
$partners.value | Where-Object { $_.inboundTrust.isMfaAccepted -eq $true } |
    Select-Object tenantId, displayName | Format-Table
```

REMÉDIATION :
1. Désactiver le trust MFA par défaut pour les tenants inconnus
2. Activer le trust MFA uniquement pour des partenaires de confiance spécifiques et documentés
3. Revoir trimestriellement les partenaires avec relations de confiance actives
4. Pour les partenaires critiques : exiger leur conformité à votre politique MFA (pas de trust aveugle)

VALEUR PAR DÉFAUT :
Confiance MFA externe désactivée par défaut, mais configurable — risque si mal paramétré.

16.1 — Détection des Menaces Identité

16.1.1 *Activer et configurer les alertes Defender for Identity mappées MITRE ATT&CK*

Critique

Licence requise : Microsoft 365 E5 ou Defender for Identity add-on

DESCRIPTION :

Microsoft Defender for Identity détecte les attaques sur les identités (pass-the-hash, pass-the-ticket, Kerberoasting, LDAP recon, DCSync, Golden Ticket). Sans alertes configurées et transmises au SOC, ces attaques sont invisibles même si toutes les politiques de configuration sont correctes. En 2026, les incidents M365 les plus graves (BEC, ransomware, APT) passent tous par la couche identité.

```
# Vérifier les alertes Defender for Identity actives
$alerts = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/security/alerts_v2?`$filter=serviceSource eq 'microsoftDefen
Write-Host "Alertes Defender for Identity (7 derniers jours) : $($alerts.value.Count)"

# Vérifier la couverture des capteurs (pour environnements hybrides)
# Portail MDI : security.microsoft.com > Settings > Identities > Sensors
```

REMÉDIATION :

1. Activer Microsoft Defender for Identity dans le portail Defender XDR
2. Pour environnements hybrides : déployer les capteurs MDI sur tous les Domain Controllers
3. Configurer les notifications email pour toutes les alertes de sévérité Haute et Critique
4. Intégrer les alertes MDI dans Microsoft Sentinel via le connecteur MDI
5. Créer des règles d'analytics Sentinel pour les tactiques MITRE clés : T1078 (Valid Accounts), T1110 (Brute Force), T1003 (Credential Dumping)

VALEUR PAR DÉFAUT :

Defender for Identity non configuré — les attaques sur les identités sont invisibles.

16.1.2 *Activer les Use Cases Microsoft Sentinel pour BEC, Token Theft et Consent Grant*

Élevé

Licence requise : Microsoft Sentinel (Log Analytics)

DESCRIPTION :

Microsoft Sentinel propose des règles d'analytics prêtes à l'emploi (OOTB) pour les scénarios d'attaque M365 les plus courants. Sans ces règles activées, les indicateurs d'attaque sont dans les logs mais personne ne les corrèle : un vol de token, une campagne BEC ou un consent phishing réussi passent inaperçus pendant des semaines.

```
# Les règles Sentinel ne sont pas vérifiables via Graph — utiliser le portail
# Sentinel > Analytics > Vérifier les règles actives pour :
$keyRules = @(
    "Suspicious application consent similar to O365 Attack Toolkit",
    "Rare application consent",
    "Mail forwarding rules to external domains",
    "Token-stealing sign-in patterns",
    "Azure AD Identity Protection risky sign-ins",
    "Sign-ins from IPs matching known malicious actors"
)
Write-Host "Règles clés à vérifier dans Sentinel Analytics :"
$keyRules | ForEach-Object { Write-Host "  - $_" }
```

REMÉDIATION :

1. Microsoft Sentinel > Gestion des contenus > Hub de contenus > Microsoft 365 Defender
2. Installer la solution "Microsoft 365 Defender" (inclut les règles BEC, Token Theft, etc.)
3. Activer les règles d'analytics OOTB pour M365 Identity
4. Configurer la fréquence de détection : 5 minutes pour les alertes critiques
5. Créer des playbooks d'auto-réponse (Logic Apps) pour les alertes haute sévérité

VALEUR PAR DÉFAUT :

Aucune règle d'analytics activée — les logs sont collectés mais non analysés.

16.1.3 *Activer UEBA (User and Entity Behavior Analytics) dans Microsoft Sentinel* Élevé

Licence requise : Microsoft Sentinel + Entra ID P2

DESCRIPTION :

L'UEBA (User and Entity Behavior Analytics) dans Sentinel construit des profils comportementaux pour chaque utilisateur et entité (appareil, IP, application). Toute déviation statistiquement significative génère une alerte avec score de risque. C'est la détection des "unknown unknowns" — les comportements anormaux qui ne correspondent à aucune règle connue mais indiquent une compromission (utilisateur se connectant à 3h du matin, accédant à des fichiers inhabituels, depuis une IP jamais vue).

AUDIT :

- Microsoft Sentinel > Configuration > Paramètres > UEBA
- Vérifier que UEBA est activé et que les sources de données sont connectées

REMÉDIATION :

1. Microsoft Sentinel > Configuration > Paramètres > UEBA
2. Activer UEBA pour le tenant
3. Connecter les sources : Entra ID Sign-in Logs, Audit Logs, Defender for Endpoint
4. Définir les groupes sensibles pour la surveillance renforcée (Direction, Finance, IT)
5. Configurer des alertes sur les scores UEBA > 8/10

VALEUR PAR DÉFAUT :

UEBA désactivé — aucune analyse comportementale des utilisateurs.

17.1 — Processus et Runbooks SOC

17.1.1 *Documenter et tester les runbooks SOC pour les incidents M365*

Élevé

DESCRIPTION :
Un tenant M365 sans runbooks SOC est une organisation qui découvrira comment répondre à un incident pendant l'incident. Les runbooks doivent couvrir les scénarios les plus probables : compromission de compte admin, BEC (virement frauduleux), ransomware cloud, exfiltration SharePoint, consent phishing réussi. Ils doivent être testés annuellement via des exercices tabletop.

AUDIT :

- Demander les runbooks SOC M365 à l'équipe sécurité
- Vérifier la date du dernier test (tabletop ou exercice réel)
- Vérifier que les runbooks couvrent les scénarios : compromission admin, BEC, ransomware cloud, consent phishing

REMÉDIATION :

1. Créer des runbooks pour chaque scénario d'incident M365 critique
2. Chaque runbook doit inclure : détection, confinement, éradication, récupération, communication
3. Tester les runbooks via tabletop exercise annuel minimum
4. Intégrer les runbooks dans Microsoft Sentinel comme playbooks Logic Apps
5. Former l'équipe SOC sur les spécificités M365 (Graph API, PowerShell, portail Defender)

VALEUR PAR DÉFAUT :
Aucun runbook SOC M365 — réponse aux incidents improvisée.

17.1.2 *Automatiser la rotation des secrets App Registration (< 90 jours)*

Élevé

DESCRIPTION :
Les secrets clients des App Registrations ont souvent des durées de vie excessives (jusqu'à 2 ans), parfois créés avec des valeurs maximales par habitude. Un secret expiré ou volé non détecté reste utilisable jusqu'à sa date d'expiration. La rotation automatique via Azure Key Vault ou des scripts planifiés garantit qu'aucun secret n'a une durée de vie supérieure à 90 jours.

```
# Secrets App Registration avec expiration > 90 jours ou déjà expirés
$cutoff90 = (Get-Date).AddDays(90)
Get-MgApplication -All | ForEach-Object {
    $app = $_
    $app.PasswordCredentials | ForEach-Object {
        [PSCustomObject]@{
            App        = $app.DisplayName
            SecretName = $_.DisplayName
            Created    = $_.StartDateTime
            Expires    = $_.EndDateTime
            Status     = if ($_.EndDateTime -lt (Get-Date)) { "❌ EXPIRÉ" }
                         elseif ($_.EndDateTime -gt $cutoff90) { "⚠️ DURÉE > 90j" }
                         else { "✅ OK" }
        }
    }
} | Where-Object { $_.Status -ne "✅ OK" } | Format-Table
```

REMÉDIATION :

1. Créer un script planifié (Azure Automation Runbook) pour détecter les secrets expirant dans 30 jours
2. Envoyer une alerte au propriétaire de l'application 30 jours avant expiration
3. Migrer vers Azure Key Vault + Managed Identity pour les applications Azure
4. Pour les apps impossibles à migrer : rotation automatique via Automation Account
5. Définir une politique : durée maximale des secrets = 90 jours

VALEUR PAR DÉFAUT :
Secrets avec durée de vie jusqu'à 2 ans — aucune rotation automatique.

17.1.3 *Réaliser un exercice Purple Team annuel sur le tenant M365*

Moyen

DESCRIPTION :
Un Purple Team exercise combine des attaques simulées (Red Team) avec une analyse en temps réel de la détection (Blue Team) sur le tenant M365. Les scénarios typiques : MFA Fatigue attack, AiTM phishing, consent phishing, exfiltration SharePoint via API, privilege escalation via App Registration. Ces exercices révèlent les lacunes de détection que les audits de configuration ne trouvent pas.

AUDIT :

- Demander le rapport du dernier Purple Team exercise M365
- Vérifier que les scénarios MITRE ATT&CK couvrent au minimum : Initial Access (T1566), Credential Access (T1078), Persistence (T1098), Exfiltration (T1048)

REMÉDIATION :

1. Planifier un Purple Team exercise M365 annuel (ou semestriel pour les organisations à risque élevé)
2. Utiliser des outils de simulation : Microsoft Attack Simulator (pour phishing), AADInternals (pour tests AD), Maester (pour validation de posture)
3. Documenter tous les écarts de détection identifiés et les corriger dans les 30 jours
4. Mettre à jour les règles Sentinel et les runbooks SOC après chaque exercice

VALEUR PAR DÉFAUT :
Aucun exercice Purple Team — lacunes de détection non identifiées.

Section 18 — RISQUE HUMAIN & INSIDER THREAT

18.1 — Sensibilisation et Simulation

18.1.1 *Déployer des simulations de phishing régulières avec métriques de taux de clic*

Élevé

Licence requise : Microsoft Defender for Office 365 P2 (Attack Simulator)

DESCRIPTION :
Microsoft Attack Simulator (intégré dans Defender for Office 365 P2) permet de lancer des campagnes de phishing simulées ciblant les utilisateurs. Sans simulation régulière, le taux de clic réel sur les phishing est inconnu, et les utilisateurs vulnérables ne sont pas identifiés. L'objectif est un taux de clic < 5% après formation et une amélioration mesurable d'une campagne à l'autre.

AUDIT :

- Portail Defender > Entraînement à la simulation d'attaque
- Vérifier la date de la dernière simulation et le taux de clic moyen

REMÉDIATION :

1. Portail Defender > Entraînement à la simulation d'attaque > Créer une simulation
2. Fréquence recommandée : une simulation par trimestre minimum
3. Cibler en priorité : Direction, Finance, RH, IT (comptes à haut risque)
4. Assigner automatiquement une formation aux utilisateurs qui cliquent
5. Partager les métriques avec la direction (taux de clic, évolution, comparaison sectorielle)

VALEUR PAR DÉFAUT :
Aucune simulation de phishing configurée.

18.1.2 *Activer et configurer Insider Risk Management (Microsoft Purview)*

Élevé

Licence requise : Microsoft 365 E5 Compliance ou add-on

DESCRIPTION :
Microsoft Purview Insider Risk Management détecte les comportements anormaux pouvant indiquer un risque interne : téléchargements massifs avant une démission, envois de fichiers vers des emails personnels, accès inhabituels à des projets sensibles, utilisation de clés USB. En 2026, les départs d'employés vers des concurrents accompagnés d'exfiltration de données sont l'une des menaces internes les plus fréquentes.

AUDIT :

- Microsoft Purview > Insider Risk Management > Vue d'ensemble
- Vérifier si des politiques de risque sont actives et si des alertes ont été générées

REMÉDIATION :

1. Microsoft Purview > Insider Risk Management > Politiques > Créer
2. Activer la politique "Fuite de données par des utilisateurs qui quittent l'entreprise"
3. Connecter les données RH (dates de départ) via le connecteur RH Purview
4. Définir des indicateurs : exfiltration email, téléchargements SharePoint, activité USB
5. Configurer des seuils d'alerte adaptés au contexte de l'organisation

VALEUR PAR DÉFAUT :
Insider Risk Management non configuré — risques internes non détectés.

18.1.3 *Surveiller le Shadow IT via Microsoft Defender for Cloud Apps (MCAS)*

Moyen

Licence requise : Microsoft 365 E5 ou Defender for Cloud Apps add-on

DESCRIPTION :
Le Shadow IT — applications cloud utilisées par les employés sans approbation IT — représente un vecteur de fuite de données majeur. Des utilisateurs copiant des données M365 vers Dropbox, Slack personnel, ou des outils IA non approuvés créent des canaux d'exfiltration non surveillés. Microsoft Defender for Cloud Apps découvre ces usages via les logs réseau et les signaux Microsoft 365.

AUDIT :

- Portail Defender > Cloud Apps > Cloud Discovery > Tableau de bord
- Vérifier le nombre d'applications découvertes et leur niveau de risque

REMÉDIATION :

1. Activer Cloud Discovery dans Defender for Cloud Apps
2. Intégrer les logs réseau (proxy, pare-feu) ou utiliser l'intégration Defender for Endpoint
3. Identifier les applications à risque élevé et les bloquer via Conditional Access App Control
4. Créer une politique d'utilisation acceptable pour les applications cloud (liste approuvée)
5. Générer un rapport mensuel Shadow IT pour la direction sécurité

VALEUR PAR DÉFAUT :
Shadow IT non surveillé — fuite de données via applications non approuvées invisible.

Annexe : Checklist (253 controles)

#	Recommandation	Niveau	Oui	Non	N/A
Section 1 — GESTION DES IDENTITÉS ET DES ACCÈS					
1.1.1	Activer MFA pour tous les comptes Administrateurs	Critique	☐	☐	☐
1.1.2	Activer MFA pour tous les utilisateurs	Élevé	☐	☐	☐
1.1.3	Désactiver MFA via SMS comme méthode principale	Moyen	☐	☐	☐
1.1.4	Exiger une MFA Résistante au Phishing pour les Rôles Privilégiés	Critique	☐	☐	☐
1.1.5	Désactiver SMS, Appel Vocal et Email OTP comme méthodes MFA	Critique	☐	☐	☐
1.1.6	Activer Number Matching pour Microsoft Authenticator	Élevé	☐	☐	☐
1.1.7	Finaliser la migration des méthodes d'authentification (Authentication Methods Migration)	Élevé	☐	☐	☐
1.1.8	Bloquer l'authentification héritée (Legacy Authentication)	Critique	☐	☐	☐
1.2.1	Utiliser des licences à empreinte applicative réduite pour les comptes admin	Élevé	☐	☐	☐
1.2.2	Bloquer la connexion aux boîtes mail partagées (Shared Mailboxes)	Élevé	☐	☐	☐
1.2.3	Restreindre les groupes publics aux groupes approuvés par l'organisation	Moyen	☐	☐	☐
1.2.4	Configurer le délai d'expiration de session pour les appareils non gérés (≤ 3 heures)	Élevé	☐	☐	☐
1.3.1	Activer les Paramètres de Sécurité par Défaut ou l'Accès Conditionnel	Critique	☐	☐	☐
1.3.2	Politique CA : Exiger un appareil conforme ou hybride Azure AD	Élevé	☐	☐	☐
1.3.3	Politique CA : Bloquer les pays à risque	Élevé	☐	☐	☐
1.3.4	Politique CA : Protéger l'accès à Azure/Entra ID Management	Critique	☐	☐	☐
1.3.5	Politique CA : Fréquence de reconnexion et sessions persistantes	Moyen	☐	☐	☐
1.3.6	Bloquer le flux Device Code (Device Code Flow) — Storm-2372	Critique	☐	☐	☐
1.3.7	Bloquer le flux d'authentification legacy (Other Clients)	Critique	☐	☐	☐
1.3.8	Politique CA : Auth résistante au phishing pour les administrateurs (FIDO2/Passkey)	Élevé	☐	☐	☐
1.3.9	Politique CA : Restreindre l'accès aux réseaux conformes uniquement (Compliant Network)	Élevé	☐	☐	☐
1.4.1	Bloquer les utilisateurs détectés comme à haut risque	Critique	☐	☐	☐
1.4.2	Bloquer les connexions détectées comme à haut risque	Critique	☐	☐	☐
1.5.1	Restreindre l'enregistrement d'applications aux administrateurs uniquement	Élevé	☐	☐	☐
1.5.2	Restreindre le consentement aux applications tierces aux administrateurs uniquement	Critique	☐	☐	☐
1.5.3	Activer le workflow de consentement administrateur	Élevé	☐	☐	☐
1.5.4	Exiger des Éditeurs Vérifiés (Verified Publishers) pour les applications tierces	Élevé	☐	☐	☐
1.6.1	Envoyer les journaux de sécurité Entra ID vers un SIEM	Critique	☐	☐	☐
1.7.1	Restreindre l'accès des invités aux objets de l'annuaire	Élevé	☐	☐	☐
1.7.2	Restreindre qui peut inviter des utilisateurs invités	Élevé	☐	☐	☐
1.7.3	Restreindre les invitations aux domaines externes approuvés	Élevé	☐	☐	☐
1.8.1	Activer Privileged Identity Management (PIM)	Critique	☐	☐	☐
1.8.2	Limiter le nombre d'Administrateurs Globaux	Critique	☐	☐	☐
1.8.3	Utiliser des rôles à granularité fine plutôt que Global Admin	Critique	☐	☐	☐
1.8.4	Provisionner les administrateurs avec des comptes cloud uniquement	Critique	☐	☐	☐
1.8.5	Exiger une approbation pour l'activation du rôle Global Administrator	Critique	☐	☐	☐
1.8.6	Configurer des alertes sur les activations de rôles privilégiés	Élevé	☐	☐	☐
1.8.7	Créer des comptes d'urgence (Break Glass Accounts)	Critique	☐	☐	☐
1.8.8	Utiliser des comptes admin dédiés (sans messagerie)	Élevé	☐	☐	☐
1.8.9	Activer les révisions d'accès pour les utilisateurs invités (Guests)	Élevé	☐	☐	☐
1.8.10	Exiger une approbation pour l'activation du rôle Privileged Role Administrator	Critique	☐	☐	☐
1.8.11	Activer les révisions d'accès (Access Reviews) pour les rôles admin	Élevé	☐	☐	☐
1.8.12	Détecter les comptes administrateurs inactifs depuis plus de 90 jours	Élevé	☐	☐	☐
1.8.13	Vérifier que les administrateurs privilégiés ne sont pas exclus des politiques CA critiques	Critique	☐	☐	☐
1.8.14	Détecter les comptes AD synchronisés dans des rôles cloud privilégiés	Critique	☐	☐	☐
1.8.15	Enforcer l'authentification Passwordless (FIDO2 / Windows Hello for Business) pour les comptes privilégiés	Critique	☐	☐	☐
1.9.1	Créer un groupe dynamique pour les utilisateurs invités	Élevé	☐	☐	☐
1.9.2	Désactiver la création de groupes de sécurité par les utilisateurs	Élevé	☐	☐	☐
1.9.3	Limiter le nombre maximum d'appareils par utilisateur (≤ 20)	Élevé	☐	☐	☐
1.9.4	Ne pas ajouter le Global Administrator comme admin local lors de la jointure Entra	Critique	☐	☐	☐
1.9.5	Restreindre la jointure d'appareils à Entra ID	Moyen	☐	☐	☐
1.9.6	Masquer l'option "Rester connecté" (Stay signed in)	Moyen	☐	☐	☐
1.9.7	Désactiver les connexions de compte LinkedIn	Moyen	☐	☐	☐
1.10.1	Configurer les paramètres d'accès cross-tenant (XTAP)	Élevé	☐	☐	☐
1.10.2	Implémenter les Tenant Restrictions v2 (TRv2)	Élevé	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
1.10.3	Activer l'Évaluation Continue des Accès (CAE)	Élevé	☐	☐	☐
1.10.4	Auditer les accès B2B et réaliser des Access Reviews régulières	Moyen	☐	☐	☐
1.11.1	Auditer les ressources d'access packages avec rôles obsolètes	Élevé	☐	☐	☐
1.11.2	Détecter les access packages référençant des groupes supprimés	Élevé	☐	☐	☐
1.11.3	Identifier les politiques d'access packages inactives ou orphelines	Moyen	☐	☐	☐
1.11.4	Valider les approbateurs des workflows d'access packages	Élevé	☐	☐	☐
1.11.5	Détecter les catalogues sans access packages associés	Faible	☐	☐	☐
1.12.1	Activer la Protection des Tokens (Token Protection) pour Exchange, SharePoint et Teams	Critique	☐	☐	☐
1.12.2	Activer les Actions Protégées (Protected Actions) pour les opérations Entra critiques	Critique	☐	☐	☐
1.13.1	Déployer Microsoft Entra Internet Access (Secure Web Gateway cloud-natif)	Moyen	☐	☐	☐
1.13.2	Remplacer le VPN traditionnel par Microsoft Entra Private Access (ZTNA)	Moyen	☐	☐	☐
1.14.1	Automatiser l'offboarding (Leaver) via Lifecycle Workflows Entra ID	Élevé	☐	☐	☐
1.14.2	Configurer les Lifecycle Workflows pour les Joiners (onboarding + TAP automatique)	Moyen	☐	☐	☐
1.15.1	Implémenter des Restricted Management AUs pour protéger les comptes critiques	Élevé	☐	☐	☐
1.15.2	Déléguer la gestion des utilisateurs par Unités Administratives sans droits globaux	Moyen	☐	☐	☐
1.16.1	Activer et traiter les Recommandations de Sécurité Entra ID	Élevé	☐	☐	☐
1.16.2	Surveiller la santé de la synchronisation Entra Connect (Connect Health)	Élevé	☐	☐	☐
1.17.1	Activer PIM pour les Groupes d'Accès Privilégiés (PIM for Groups)	Élevé	☐	☐	☐
1.17.2	Migrer les comptes de service avec mots de passe vers Managed Identities ou Workload Federation	Élevé	☐	☐	☐
1.18.1	Auditer les Federated Identity Credentials (OIDC) pour CI/CD	Critique	☐	☐	☐
1.18.2	Restreindre les permissions des App Registrations utilisées par les pipelines CI/CD	Élevé	☐	☐	☐
Section 2 — MICROSOFT DEFENDER FOR OFFICE 365					
2.1.1	Activer les politiques de sécurité Standard et Stricte	Critique	☐	☐	☐
2.1.2	Ajouter les comptes sensibles à la politique Stricte	Critique	☐	☐	☐
2.2.1	Configurer les politiques Anti-Phishing	Critique	☐	☐	☐
2.2.2	Configurer DMARC, DKIM et SPF	Critique	☐	☐	☐
2.2.3	Activer la Protection contre l'usurpation (Anti-Spoofing)	Critique	☐	☐	☐
2.3.1	Activer Safe Attachments	Critique	☐	☐	☐
2.3.2	Activer Safe Links	Critique	☐	☐	☐
2.3.3	Configurer la politique Anti-Malware avec types de fichiers étendus	Élevé	☐	☐	☐
2.4.1	Configurer les politiques Anti-Spam	Élevé	☐	☐	☐
2.4.2	Configurer l'impersonation utilisateurs ciblés (Targeted User Impersonation Protection)	Élevé	☐	☐	☐
2.4.3	Configurer l'impersonation domaines owned et partenaires clés	Élevé	☐	☐	☐
2.4.4	Activer ZAP (Zero-Hour Auto Purge) pour Microsoft Teams	Moyen	☐	☐	☐
2.4.5	Configurer la DLP avec un périmètre complet (EXO + OD + SPO + Teams + Devices)	Élevé	☐	☐	☐
Section 3 — EXCHANGE ONLINE ET MESSAGERIE					
3.1.1	Désactiver le transfert automatique des emails vers des domaines externes	Critique	☐	☐	☐
3.1.2	Activer l'audit de la boîte mail (Mailbox Auditing)	Élevé	☐	☐	☐
3.1.3	Désactiver SMTP AUTH au niveau de l'organisation	Élevé	☐	☐	☐
3.1.4	Configurer les connexions sécurisées TLS pour les emails entrants	Moyen	☐	☐	☐
3.1.5	Désactiver les protocoles POP3 et IMAP4	Élevé	☐	☐	☐
3.1.6	Implémenter les avertissements d'expéditeur externe	Élevé	☐	☐	☐
3.1.7	Désactiver les listes d'autorisation IP dans les politiques anti-spam	Élevé	☐	☐	☐
3.1.8	Activer la purge automatique Zero-Hour (ZAP)	Élevé	☐	☐	☐
3.1.9	Ne pas ajouter de domaines dans les listes d'autorisation anti-spam	Critique	☐	☐	☐
3.1.10	Activer le chiffrement des emails sensibles (OME)	Moyen	☐	☐	☐
3.1.11	Valider DMARC p=reject (pas seulement p=none)	Critique	☐	☐	☐
3.1.12	Valider SPF avec hard fail (-all) et non soft fail (~all)	Élevé	☐	☐	☐
3.1.13	Vérifier les 7 alertes obligatoires Microsoft (MS.EXO.16.1)	Élevé	☐	☐	☐
3.1.14	Activer les conseils de sécurité "First Contact" et Mailbox Intelligence	Moyen	☐	☐	☐
3.1.15	Bloquer les règles de transport bypass pour la simulation de phishing (PhishSim)	Élevé	☐	☐	☐
3.1.16	Configurer ARC (Authenticated Received Chain) pour les flux d'emails complexes	Moyen	☐	☐	☐
3.1.17	Auditer les délégations de boîte mail (Send As, Full Access, Send on Behalf)	Élevé	☐	☐	☐
3.2.1	Restreindre le partage de calendriers avec des domaines externes	Moyen	☐	☐	☐
3.2.2	Interdire le partage de dossiers de contacts avec des domaines externes	Élevé	☐	☐	☐
3.2.3	Restreindre le partage de calendriers aux domaines de confiance spécifiés (whitelist)	Élevé	☐	☐	☐
3.2.4	Désactiver les réponses automatiques d'absence du bureau (OOF) vers les domaines externes	Moyen	☐	☐	☐
3.2.5	Bloquer la connexion directe aux boîtes aux lettres partagées	Critique	☐	☐	☐
3.2.6	Vérifier qu'aucune règle de transport n'autorise des domaines entiers	Critique	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
3.2.7	Désactiver AuditBypassEnabled sur toutes les boîtes aux lettres	Critique	☐	☐	☐
3.2.8	Configurer des limites d'envoi dans la politique anti-spam sortant	Élevé	☐	☐	☐
3.2.9	Désactiver la liste sûre du filtre de connexion	Élevé	☐	☐	☐
3.2.10	Activer les notifications pour les malwares envoyés par des utilisateurs internes	Élevé	☐	☐	☐
3.2.11	Détecter et bloquer les règles de boîte de réception malveillantes (Inbox Rules)	Critique	☐	☐	☐
Section 4 — MICROSOFT TEAMS					
4.1.1	Restreindre l'accès des invités (Guest Access)	Élevé	☐	☐	☐
4.1.2	Restreindre l'accès externe (Federation)	Moyen	☐	☐	☐
4.1.3	Sécuriser les réunions Teams	Moyen	☐	☐	☐
4.1.4	Désactiver l'intégration Email dans les canaux Teams	Élevé	☐	☐	☐
4.1.5	Gouvernance des applications Teams	Moyen	☐	☐	☐
4.1.6	Activer la protection contre les malwares dans Teams (Safe Attachments)	Élevé	☐	☐	☐
4.1.7	Activer la protection Safe Links pour Teams	Élevé	☐	☐	☐
4.1.8	Contrôler le partage d'écran dans Teams	Faible	☐	☐	☐
4.1.9	Désactiver les 5 fournisseurs de stockage cloud tiers dans Teams	Moyen	☐	☐	☐
4.1.10	Empêcher les communications avec les tenants Teams en mode trial	Élevé	☐	☐	☐
4.1.11	Bloquer les utilisateurs Teams non gérés d'initier des conversations entrantes	Élevé	☐	☐	☐
4.2.1	Empêcher les utilisateurs en appel entrant (dial-in) de bypasser le lobby	Moyen	☐	☐	☐
4.2.2	Désactiver le chat de réunion pour les utilisateurs anonymes	Moyen	☐	☐	☐
4.2.3	Restreindre la présentation aux organisateurs et co-organisateurs	Moyen	☐	☐	☐
4.2.4	Désactiver le chat avec des participants externes post-réunion	Moyen	☐	☐	☐
4.2.5	Désactiver l'enregistrement automatique des réunions par défaut	Moyen	☐	☐	☐
4.2.6	Activer le signalement de problèmes de sécurité dans Teams	Moyen	☐	☐	☐
4.2.7	Désactiver la publication automatique des enregistrements de réunions Teams	Élevé	☐	☐	☐
Section 5 — SHAREPOINT ONLINE ET ONEDRIVE					
5.1.1	Restreindre le partage SharePoint/OneDrive à des domaines spécifiques	Élevé	☐	☐	☐
5.1.2	Désactiver les liens de partage anonymes ("Anyone")	Élevé	☐	☐	☐
5.1.2b	Configurer une expiration obligatoire sur tous les liens anonymes (30 jours max)	Critique	☐	☐	☐
5.1.3	Activer l'accès conditionnel pour SharePoint (accès non géré)	Élevé	☐	☐	☐
5.1.4	Configurer la durée d'expiration des sessions SharePoint	Faible	☐	☐	☐
5.1.5	Configurer les permissions par défaut des liens en mode Affichage uniquement	Critique	☐	☐	☐
5.1.7	Restreindre les liens "Anyone" à la permission Affichage uniquement	Critique	☐	☐	☐
5.1.8	Exiger une ré-authentification périodique pour les codes de vérification email (≤ 30 jours)	Élevé	☐	☐	☐
5.1.10	Exiger l'authentification moderne pour SharePoint	Critique	☐	☐	☐
5.1.11	Activer l'intégration SharePoint/OneDrive avec Azure AD B2B	Élevé	☐	☐	☐
5.1.12	Empêcher les invités SharePoint de partager des éléments qu'ils ne possèdent pas	Élevé	☐	☐	☐
5.1.13	Restreindre le partage externe SharePoint à un groupe de sécurité spécifique	Élevé	☐	☐	☐
5.1.14	Configurer l'expiration automatique de l'accès guest à SharePoint/OneDrive	Élevé	☐	☐	☐
5.1.15	Bloquer le téléchargement de fichiers infectés depuis SharePoint	Élevé	☐	☐	☐
5.1.16	Restreindre la synchronisation OneDrive aux appareils gérés	Élevé	☐	☐	☐
5.1.17	Bloquer les scripts personnalisés sur les sites SharePoint	Moyen	☐	☐	☐
Section 6 — PROTECTION DE L'INFORMATION ET CONFORMITÉ					
6.1.1	Activer l'Audit Unifié (Unified Audit Log)	Critique	☐	☐	☐
6.1.2	Configurer des politiques de rétention des données	Élevé	☐	☐	☐
6.1.3	Activer la prévention des pertes de données (DLP)	Élevé	☐	☐	☐
6.1.4	Activer les étiquettes de sensibilité (Sensitivity Labels)	Moyen	☐	☐	☐
6.1.5	Activer Microsoft Purview Communication Compliance	Moyen	☐	☐	☐
6.1.6	Configurer Microsoft Purview Insider Risk Management	Élevé	☐	☐	☐
Section 7 — SÉCURITÉ DES APPAREILS (INTUNE/MICROSOFT ENDPOINT MANAGER)					
7.1.1	Exiger le chiffrement des appareils (BitLocker)	Critique	☐	☐	☐
7.1.2	Exiger un code PIN/mot de passe sur les appareils mobiles	Élevé	☐	☐	☐
7.1.3	Configurer les App Protection Policies (MAM)	Élevé	☐	☐	☐
7.1.4	Activer Windows Hello for Business	Moyen	☐	☐	☐
7.1.5	Marquer les appareils sans politique de conformité comme Non conformes	Élevé	☐	☐	☐
7.1.6	Bloquer l'inscription d'appareils personnels (BYOD) par défaut	Élevé	☐	☐	☐
7.1.7	Activer Intune Multi-Admin Approval (MAA) pour les actions critiques	Élevé	☐	☐	☐
7.1.8	Vérifier que l'autorité MDM est définie sur Intune	Élevé	☐	☐	☐
7.1.9	Configurer le nettoyage automatique des appareils inactifs Intune	Moyen	☐	☐	☐

#	Recommandation	Niveau	Oui	Non	N/A
7.2.1	Activer la protection anti-falsification (Tamper Protection)	🔴 Critique	☐	☐	☐
7.2.2	Configurer les règles de réduction de la surface d'attaque (ASR Rules)	🔴 Critique	☐	☐	☐
7.2.3	Activer la protection réseau (Network Protection)	🟠 Élevé	☐	☐	☐
7.2.4	Configurer l'investigation et la réponse automatisées (AIR) en mode complet	🟠 Élevé	☐	☐	☐
7.2.5	Activer Microsoft Defender Antivirus en mode protection en temps réel	🔴 Critique	☐	☐	☐
Section 8 — MICROSOFT SECURE SCORE ET MONITORING					
8.1.1	Atteindre et maintenir un Secure Score ≥ 50%	🟠 Élevé	☐	☐	☐
8.1.2	Configurer les alertes de sécurité obligatoires Exchange/Defender	🔴 Critique	☐	☐	☐
8.1.3	Configurer des alertes de sécurité personnalisées	🟠 Élevé	☐	☐	☐
8.1.4	Activer Microsoft Defender for Identity (si AD hybride)	🟠 Élevé	☐	☐	☐
8.1.5	Activer Microsoft Defender for Cloud Apps (CASB)	🟠 Élevé	☐	☐	☐
8.1.6	Activer et configurer la protection des comptes prioritaires	🟠 Élevé	☐	☐	☐
8.1.7	Appliquer le preset de sécurité Strict aux comptes prioritaires	🟠 Élevé	☐	☐	☐
8.1.8	Configurer des alertes d'activité pour les comptes d'accès d'urgence (Break Glass)	🔴 Critique	☐	☐	☐
8.1.9	Détecter les credentials admins exposés sur des endpoints vulnérables (XSPM)	🟠 Élevé	☐	☐	