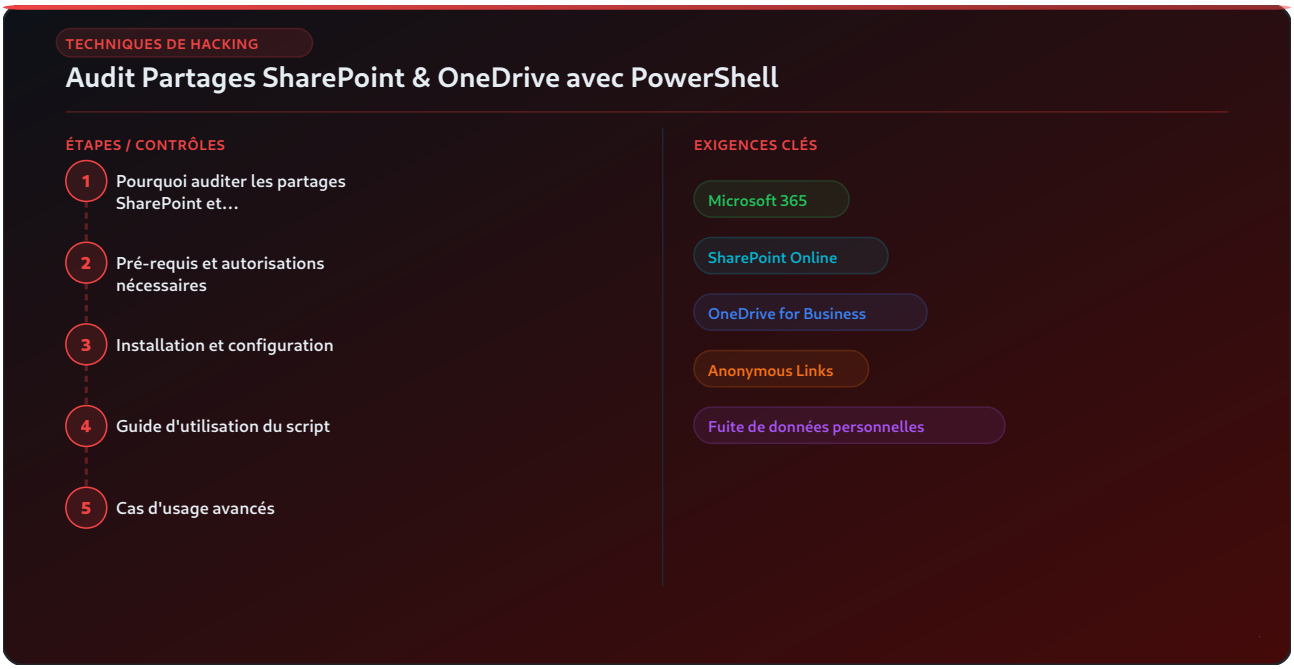
# Audit des Partages SharePoint & OneDrive : Lister les Liens Anonymes avec PowerShell

> Script PowerShell pour auditer tous les partages SharePoint Online et OneDrive : liens anonymes, récursif sur tout le tenant M365. Export CSV/HTML 2026.

La prolifération des liens de partage dans les environnements **Microsoft 365** constitue aujourd'hui l'un des vecteurs de fuite de données les plus sous-estimés des organisations européennes. **SharePoint Online** et **OneDrive for Business** permettent en quelques clics de générer des liens accessibles sans aucune authentification — les fameux "Anyone links" ou **Anonymous Links**. Ces partages, créés pour simplifier la collaboration, s'accumulent silencieusement au fil des mois, exposant des contrats, des données personnelles, des plans stratégiques ou des rapports financiers à n'importe quel internaute disposant de l'URL. Dans un contexte où le règlement **RGPD** impose des mesures techniques appropriées pour protéger les données personnelles, et où la directive **NIS 2** exige des organisations essentielles et importantes une gestion rigoureuse des risques cyber, l'absence d'audit régulier des partages M365 constitue une non-conformité potentiellement coûteuse. Ce guide complet vous présente un script PowerShell professionnel — `Get-ShareAudit.ps1` — capable d'auditer exhaustivement l'intégralité des partages de votre tenant Microsoft 365, de détecter les liens anonymes, d'exporter les résultats et de guider la remédiation. Que vous soyez RSSI, auditeur technique ou administrateur M365, ce script est conçu pour s'intégrer immédiatement dans votre programme de gouvernance.




## Pourquoi auditer les partages SharePoint et OneDrive ?

Les **Anonymous Links** SharePoint sont des liens de type "Anyone with the link" qui permettent à toute personne disposant de l'URL d'accéder au fichier sans s'identifier. Ils sont créés par des utilisateurs métier qui souhaitent partager rapidement un document avec un prestataire externe, un client ou un partenaire — sans passer par les procédures IT. Le problème : une fois créé, ce lien est permanent par défaut, rarement audité, et peut être transmis ou découvert par des tiers non autorisés.

Les risques concrets sont multiples :

**Fuite de données personnelles** : RH, contrats clients, données de santé partagés en Anonymous font l'objet d'une obligation de notification CNIL sous 72h en cas de découverte (RGPD Art. 33)

**Violation NIS 2** : Les entités essentielles (énergie, santé, finances) doivent démontrer la maîtrise de leurs accès et partages de données sensibles

**Propriété intellectuelle exposée** : Code source, brevets, plans produits — des incidents réels ont compromis des entreprises via des liens SharePoint indexés par Google

**Vecteur d'attaque secondaire** : Un attaquant ayant obtenu une URL via phishing peut exfiltrer des données sans déclencher d'alerte IAM car aucune authentification n'est requise

Du point de vue réglementaire, l'article 32 du RGPD impose des *mesures techniques appropriées pour assurer la sécurité des données*. La CNIL considère explicitement que l'absence de contrôle des accès aux données constitue une mesure insuffisante. La directive NIS 2 (transposée en France par la loi du 15 avril 2025) ajoute l'obligation de gérer les risques liés à la chaîne d'approvisionnement numérique — ce qui inclut les partages avec des tiers.

Des cas réels illustrent l'ampleur du problème : en 2024, une entreprise industrielle française a découvert lors d'un pentest que 340 documents internes — dont les spécifications d'un produit en développement — étaient accessibles publiquement via des Anonymous Links SharePoint créés 18 mois plus tôt par des équipes R&D. Pour une collectivité territoriale auditée en 2025, c'est plus de 2 000 fichiers contenant des données personnelles de citoyens qui se trouvaient accessibles sans authentification.

---

## Pré-requis et autorisations nécessaires

Avant d'exécuter `Get-ShareAudit.ps1`, vous devez enregistrer une application dans **Azure Active Directory** et lui accorder les permissions nécessaires. Ce mode "application" (app-only) est recommandé car il ne dépend pas d'un compte utilisateur individuel et peut s'exécuter de manière non interactive.

> ⚡ **Retour terrain**
>
> Dans mes missions de red team, la phase de post-exploitation révèle systématiquement des données que le client pensait protégées. Le cas le plus fréquent : des fichiers Excel de comptabilité ou RH stockés sur des partages réseau accessibles à tous les utilisateurs du domaine, sans restriction. Sur les 30 dernières missions, 27 avaient des partages réseau avec des données sensibles accessibles à n'importe quel utilisateur authentifié. La sensibilité des données n'est pas corrélée à leur niveau de protection réel.

## Enregistrement de l'application Azure AD

Accédez au portail Azure → **Azure Active Directory** → **Inscriptions d'applications** → **Nouvelle inscription**. Nommez l'application (ex : `M365-ShareAudit-Prod`), sélectionnez "Comptes dans ce répertoire organisationnel uniquement", puis créez.

Dans les **Autorisations d'API**, ajoutez les permissions d'*application* (et non déléguées) suivantes :

**Microsoft Graph — Sites.Read.All** : Lecture de tous les sites SharePoint Online

**Microsoft Graph — Files.Read.All** : Lecture de tous les fichiers et leurs métadonnées de partage

**Microsoft Graph — User.Read.All** : Énumération des utilisateurs pour accéder à leurs OneDrive

**SharePoint — Sites.FullControl.All** : Requis uniquement si vous utilisez PnP.PowerShell en mode app-only

Cliquez **Accorder le consentement administrateur** — cette étape nécessite le rôle Global Administrator. Ensuite, dans **Certificates & secrets**, créez un nouveau secret client avec une durée de 12 mois. Notez immédiatement la valeur (elle ne sera plus visible).

## Rôles administrateur requis

L'opérateur qui enregistre l'application doit détenir le rôle **Global Administrator** ou **Application Administrator** + **Privileged Role Administrator**. En mode lecture seule via **Microsoft Graph API**, le rôle **Global Reader** suffit pour consentir aux permissions de lecture.

Pour l'usage courant (exécution du script sans modification de configuration), l'opération nécessite simplement le ClientId et le ClientSecret — aucun rôle supplémentaire n'est requis côté script.

### Principe du moindre privilège

Si votre politique de sécurité interdit les permissions `Sites.FullControl.All`, utilisez le mode fallback **Microsoft Graph** avec `Sites.Read.All` + `Files.Read.All` uniquement. Le script détecte automatiquement la disponibilité de PnP.PowerShell et bascule vers Graph si nécessaire.

---

## Installation et configuration

Le script supporte deux moteurs d'accès à l'API Microsoft 365 : **PnP.PowerShell** (préféré) et **Microsoft.Graph** (fallback automatique). Les deux approches offrent une couverture complète mais avec des nuances.

### PnP.PowerShell vs Microsoft Graph

**PnP.PowerShell** : Cmdlets natives SharePoint, plus expressives ( `Get-PnPFileSharingLink`, `Get-PnPTenantSite` ), gestion intégrée du throttling. Nécessite le module PnP.PowerShell ≥ 2.0.

**Microsoft Graph API** : API REST universelle, disponible sur toutes les plateformes (Linux, macOS via PowerShell 7), ne nécessite pas PnP. Légèrement plus verbeux mais identique en termes de données.

### Installation du module PnP.PowerShell

```
 # Installation pour l'utilisateur courant (recommandé)
Install-Module PnP.PowerShell -MinimumVersion 2.0 -Scope CurrentUser -Force

# Vérification
Get-Module PnP.PowerShell -ListAvailable | Select-Object Name, Version

# Installation optionnelle : Microsoft.Graph (fallback)
Install-Module Microsoft.Graph -Scope CurrentUser -Force
```

### Clonage du dépôt

```
 git clone https://github.com/ayinedjimi/sharepoint-onedrive-share-audit.git
cd sharepoint-onedrive-share-audit

# Débloquer le script sous Windows
Unblock-File .\Get-ShareAudit.ps1

# Vérifier la signature (optionnel – PowerShell execution policy)
Get-AuthenticodeSignature .\Get-ShareAudit.ps1
```

### Configuration de la politique d'exécution

```
 # Autoriser les scripts locaux signés (recommandé en production)
Set-ExecutionPolicy RemoteSigned -Scope CurrentUser

# Ou pour un usage ponctuel :
powershell.exe -ExecutionPolicy Bypass -File .\Get-ShareAudit.ps1 -TenantId "..." ...
```

## Guide d'utilisation du script

Le script `Get-ShareAudit.ps1` s'articule autour de 7 paramètres principaux. Voici les scénarios d'utilisation les plus courants.

### Audit basique — SharePoint uniquement

```
.\Get-ShareAudit.ps1 `
    -TenantId "contoso.onmicrosoft.com" `
    -ClientId "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
    -ClientSecret "VotreSecretClient123!"
```

Ce mode analyse tous les sites **SharePoint Online** du tenant et exporte les résultats dans le répertoire courant sous forme de fichiers `ShareAudit_YYYYMMDD_HHmmss.csv` et `ShareAudit_YYYYMMDD_HHmmss.html`.

### Audit complet avec OneDrive et filtre anonymes

```
.\Get-ShareAudit.ps1 `
    -TenantId "contoso.onmicrosoft.com" `
    -ClientId "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
    -ClientSecret "VotreSecretClient123!" `
    -IncludeOneDrive `
    -AnonymousOnly `
    -OutputPath "C:\Audits\M365\2026-05" `
    -Verbose
```

Le paramètre `-IncludeOneDrive` ajoute les MySites de tous les utilisateurs, ce qui peut significativement allonger la durée d'audit sur les tenants de grande taille (plusieurs centaines d'utilisateurs). Le switch `-AnonymousOnly` filtre les résultats pour ne conserver que les **Anonymous Links**, réduisant le volume de données à analyser.

### Interprétation des résultats CSV

Le fichier CSV contient les colonnes suivantes :

**SiteUrl / SiteTitle** : URL et nom du site source

**SiteType** : `SharePoint` ou `OneDrive`

**ItemPath / ItemName** : Chemin complet et nom de l'élément partagé

**ShareType** : `Anyone` (anonyme), `Company` (tenant uniquement), `Specific` (utilisateurs nommés)

**CreatedBy / CreatedDate** : Auteur et date de création du lien

**ExpirationDate** : Date d'expiration ( `vide` = jamais expiré)

**IsAnonymous / IsExpired** : Booléens pour filtrage rapide dans Excel

**ShareUrl** : URL directe du lien de partage

Pour analyser rapidement les résultats sous Excel : ouvrez le CSV → Données → Filtres automatiques → filtrez la colonne `IsAnonymous` sur `True`. Les lignes rouges dans le rapport HTML correspondent aux **Anonymous Links**.

---

## Cas d'usage avancés

### Audit ciblé par site

Pour auditer un site spécifique sans parcourir l'intégralité du tenant, vous pouvez adapter le script en modifiant la liste de sites retournée par `Get-AllSharePointSites`, ou utiliser directement **PnP.PowerShell** :

```
Connect-PnPOnline -Url "https://contoso.sharepoint.com/sites/Finance" `
                  -ClientId $ClientId -ClientSecret $ClientSecret

# Récupérer tous les liens de partage d'une bibliothèque
$items = Get-PnPListItem -List "Documents" -Fields "FileRef","FileLeafRef"
foreach ($item in $items) {
    $links = Get-PnPFileSharingLink -FileUrl $item["FileRef"] -ErrorAction SilentlyContinue
    if ($links) {
        $links | Where-Object { $_.Link.Scope -like "*anonymous*" } |
            Select-Object @{N="Fichier";E={$item["FileLeafRef"]}}, `
                          @{N="URL";E={$_.Link.WebUrl}}, `
                          @{N="Expiration";E={$_.ExpirationDateTime}}
    }
}
```

### Détection des liens expirés mais encore actifs

Certains tenants ne purgent pas automatiquement les liens expirés. Pour identifier les liens dont la date d'expiration est dépassée mais qui sont toujours présents en base :

```
 # Après exécution du script principal
$expired = Import-Csv "ShareAudit_20260521.csv" -Delimiter ";" |
    Where-Object {
        $_.ExpirationDate -ne "" -and
        [datetime]$_.ExpirationDate -lt (Get-Date)
    }

Write-Host "$($expired.Count) liens expirés trouvés"
$expired | Export-Csv "liens-expires.csv" -NoTypeInformation -Encoding UTF8 -Delimiter ";"
```

### Intégration dans un pipeline CI/CD

Pour une intégration dans **Azure DevOps** ou **GitHub Actions**, vous pouvez encapsuler le script dans une tâche PowerShell et exposer le nombre de liens anonymes comme métrique de conformité :

```
# GitHub Actions — audit hebdomadaire automatique
name: M365 Share Audit
on:
  schedule:
    - cron: '0 6 * * 1'  # Chaque lundi à 6h UTC
  workflow_dispatch:

jobs:
  audit:
    runs-on: windows-latest
    steps:
      - uses: actions/checkout@v4
      - name: Install PnP.PowerShell
        run: Install-Module PnP.PowerShell -MinimumVersion 2.0 -Force -Scope CurrentUser
        shell: pwsh
      - name: Run Share Audit
        run: |
          .\Get-ShareAudit.ps1 `
            -TenantId "${{ secrets.TENANT_ID }}" `
            -ClientId "${{ secrets.CLIENT_ID }}" `
            -ClientSecret "${{ secrets.CLIENT_SECRET }}" `
            -AnonymousOnly `
            -OutputPath ".\audit-results"
        shell: pwsh
      - name: Upload results
        uses: actions/upload-artifact@v4
        with:
          name: audit-${{ github.run_number }}
          path: audit-results/
```

## Remédiation des partages anonymes

Une fois les **Anonymous Links** identifiés, la remédiation s'effectue en deux temps : révocation immédiate des liens à risque élevé, puis mise en place d'une politique de gouvernance préventive.

### Révocation par script PowerShell

```
 # Chargement des résultats d'audit
$anonymousLinks = Import-Csv "ShareAudit_20260521.csv" -Delimiter ";" |
    Where-Object { $_.IsAnonymous -eq "True" }

# Groupement par site pour minimiser les reconnexions
$bySite = $anonymousLinks | Group-Object SiteUrl

foreach ($siteGroup in $bySite) {
    Write-Host "Traitement du site : $($siteGroup.Name)"

    Connect-PnPOnline -Url $siteGroup.Name `
                      -ClientId $ClientId `
                      -ClientSecret $ClientSecret

    foreach ($link in $siteGroup.Group) {
        try {
            # Récupérer l'ID du lien de partage
            $sharingLinks = Get-PnPFileSharingLink -FileUrl $link.ItemPath
            $targetLink = $sharingLinks | Where-Object { $_.Link.WebUrl -eq $link.ShareUrl }

            if ($targetLink) {
                # Supprimer le lien anonyme
                Remove-PnPFileSharingLink -FileUrl $link.ItemPath -Id $targetLink.Id -Force
                Write-Host "  Révoqué : $($link.ItemName)" -ForegroundColor Green
            }
        } catch {
            Write-Host "  ERREUR pour $($link.ItemName) : $_" -ForegroundColor Red
        }
    }

    Disconnect-PnPOnline
}
```

### Politique de gouvernance — Désactiver les Anonymous Links au niveau tenant

```
Connect-PnPOnline -Url "https://contoso-admin.sharepoint.com" `
                  -ClientId $ClientId `
                  -ClientSecret $ClientSecret

# Désactiver les liens anonymes pour tout le tenant
Set-PnPTenant -SharingCapability Disabled
# Ou : autoriser le partage interne uniquement
Set-PnPTenant -SharingCapability ExternalUserSharingOnly

# Définir une durée d'expiration maximale pour les liens (en jours)
Set-PnPTenant -RequireAnonymousLinksExpireInDays 30

# Forcer l'expiration des liens existants
Set-PnPTenant -DefaultSharingLinkExpirationInDays 30
```

Ces paramètres s'appliquent au niveau tenant et affectent tous les sites. Pour une approche plus granulaire, appliquez des politiques de partage au niveau de chaque collection de sites (**Site Collection Administrator**) via `Set-PnPSite -SharingCapability`.

---

## Intégration dans un programme de gouvernance M365

L'audit ponctuel des partages n'est qu'une première étape. Une gouvernance durable des accès Microsoft 365 nécessite l'intégration de plusieurs outils et processus complémentaires.

### Microsoft Purview — Data Loss Prevention

**Microsoft Purview** (anciennement Microsoft Information Protection) permet de classer automatiquement les documents sensibles (données personnelles, informations confidentielles) et d'appliquer des politiques DLP qui bloquent le partage anonyme des fichiers classifiés. Configurez des règles DLP qui déclenchent une alerte — voire bloquent l'action — lorsqu'un utilisateur tente de créer un lien "Anyone" sur un document contenant des données RGPD.

### Microsoft Defender for Cloud Apps (MDCA)

**Microsoft Defender for Cloud Apps** offre une visibilité en temps réel sur les activités de partage SharePoint via ses politiques d'activité. Créez une alerte sur les activités `SharingSet` avec le scope `anonymous` pour être notifié en temps réel de chaque nouveau lien anonyme créé. Cette approche complémente l'audit périodique par une détection continue.

### Monitoring continu via Azure Monitor / Sentinel

Les logs d'audit Microsoft 365 (Unified Audit Log) enregistrent chaque création de lien de partage. Intégrez ces logs dans **Azure Monitor** ou Microsoft Sentinel pour un threat hunting M365 avancé et créez des règles analytiques KQL :

```
OfficeActivity
| where Operation == "SharingSet"
| where SharingType == "Anyone"
| project TimeGenerated, UserId, SourceRelativeUrl, OfficeObjectId
| order by TimeGenerated desc
```

Cette requête KQL peut être programmée comme alerte quotidienne dans Sentinel pour détecter les nouveaux Anonymous Links dès leur création.

### Révision périodique et Access Reviews

Les **Azure AD Access Reviews** peuvent être configurées pour inclure les partages SharePoint — bien que les liens Anonymous soient hors scope natif. Complétez avec une exécution hebdomadaire de `Get-ShareAudit.ps1 -AnonymousOnly` via une tâche planifiée ou Azure Automation. Intégrez ce script dans votre programme de gouvernance cybersécurité porté au niveau RSSI/COMEX.

Pour les organisations soumises à **ISO 27001**, le contrôle A.9.4.1 (restriction d'accès à l'information) exige une revue périodique des droits d'accès. L'audit régulier des partages M365 constitue une preuve tangible de ce contrôle lors des audits de certification. Consultez également notre guide sur l'Identity Governance et la gestion du cycle de vie des comptes pour une approche intégrée.

Pour un programme d'audit plus large couvrant l'ensemble de Microsoft 365, nous vous recommandons notre guide complet d'audit de sécurité Microsoft 365 qui aborde Active Directory, Exchange Online, Teams et les configurations de sécurité avancées.

## FAQ — Questions fréquentes

### Quelles permissions minimales sont nécessaires pour exécuter le script en lecture seule ?

En mode Microsoft.Graph (sans PnP.PowerShell), les permissions `Sites.Read.All` et `Files.Read.All` en mode Application suffisent pour auditer tous les partages SharePoint. Pour inclure OneDrive, ajoutez `User.Read.All`. Ces trois permissions ne permettent aucune modification et respectent strictement le principe du moindre privilège. Le consentement administrateur reste obligatoire car ce sont des permissions d'application (pas déléguées).

### Le script peut-il auditer les OneDrive d'utilisateurs qui ont quitté l'organisation ?

Oui, si les **OneDrive for Business** des comptes désactivés n'ont pas été supprimés. Par défaut, Microsoft conserve les données OneDrive 30 jours après la désactivation d'un compte (configurable jusqu'à 3 650 jours). Le script liste l'ensemble des drives retournés par `/users/{id}/drive`, y compris ceux des comptes désactivés dont le drive est encore actif. C'est souvent là que se trouvent les partages les plus anciens et les plus risqués — les anciens collaborateurs créaient parfois des liens de travail non documentés.

### Comment prouver la conformité RGPD avec les résultats de cet audit ?

Les exports CSV et HTML générés par `Get-ShareAudit.ps1` constituent des preuves d'audit opposables. Pour une conformité RGPD solide : (1) conservez les rapports d'audit datés, (2) documentez les actions correctives prises (révocation des liens), (3) intégrez cet audit dans votre registre de traitements comme mesure de contrôle périodique (Art. 30 RGPD). La CNIL recommande une fréquence minimale annuelle pour les revues d'accès aux données personnelles,

mais trimestrielle pour les organisations traitant des données sensibles (santé, finances). Consultez également les recommandations CISA sur la sécurisation des environnements cloud et la documentation officielle Microsoft sur la gestion du partage externe SharePoint.

## Automatisation de la surveillance continue des partages anonymes SharePoint Online

La surveillance ponctuelle via PowerShell est utile pour un audit initial mais insuffisante pour maintenir une posture de sécurité continue et opérationnelle. Les partages anonymes SharePoint Online sont créés quotidiennement par les utilisateurs — souvent de bonne foi pour partager un document avec un partenaire externe qui ne dispose pas de compte dans le tenant — mais ils s'accumulent progressivement sans processus de révocation systématique dans la plupart des organisations. La mise en place d'une surveillance automatisée permet de détecter les nouveaux partages anonymes en temps réel et d'alerter les équipes sécurité avant que des données sensibles ne soient exposées publiquement pendant une durée prolongée sans contrôle de l'équipe de sécurité informatique.

Les logs d'activité SharePoint Online sont automatiquement ingérés dans Microsoft Sentinel via le connecteur Microsoft 365. L'événement SharePoint correspondant à la création d'un lien de partage anonyme est de type "SharingLinkCreated" avec le champ "LinkType" égal à "AnonymousLink". Une règle d'analyse Sentinel basée sur cet événement peut déclencher une alerte en temps réel incluant le contexte complet : nom de l'utilisateur ayant créé le lien, nom du fichier ou dossier partagé, site SharePoint concerné, et si Microsoft Purview Information Protection est déployé dans l'organisation, la classification de sensibilité du document partagé (Public, Interne, Confidentiel ou Hautement confidentiel selon le schéma de classification de l'entreprise).

Pour les organisations disposant d'un volume important de partages — plusieurs dizaines de milliers de fichiers partagés dans un grand tenant Microsoft 365 avec des milliers d'utilisateurs actifs — les politiques Data Loss Prevention (DLP) dans Microsoft Purview permettent d'aller plus loin que la simple détection réactive : bloquer automatiquement la création de liens

anonymes sur les fichiers classifiés "Confidentiel" ou "Hautement confidentiel", ou exiger une justification métier documentée et une approbation explicite d'un responsable hiérarchique avant tout partage externe non authentifié. Cette approche préventive complète la surveillance réactive post-incident et réduit considérablement le risque de fuite de données sensibles via des partages anonymes non maîtrisés par les équipes sécurité de l'organisation.

**À RETENIR**

Points essentiels à retenir

Les **Anonymous Links** SharePoint ("Anyone with the link") exposent vos fichiers sans aucune authentification — ils constituent le risque de conformité le plus élevé dans un tenant M365 mal gouverné.

`Get-ShareAudit.ps1` audite exhaustivement **SharePoint Online** et **OneDrive for Business** en utilisant PnP.PowerShell (préféré) ou **Microsoft Graph API** (fallback automatique), avec retry sur throttling HTTP 429.

Les permissions minimales requises sont `Sites.Read.All` + `Files.Read.All` + `User.Read.All` (Application permissions, consentement admin obligatoire).

La remédiation passe par `Remove-PnPFileSharingLink` pour les liens identifiés et `Set-PnPTenant -RequireAnonymousLinksExpireInDays 30` pour prévenir les créations futures.

Intégrez cet audit dans votre programme de gouvernance M365 : **Microsoft Purview** DLP, **Defender for Cloud Apps** et les Access Reviews Azure AD forment un dispositif de contrôle continu complémentaire aux audits périodiques.

Le script est disponible en open source sur GitHub : [github.com/ayinedjimi/sharepoint-onedrive-share-audit](github.com/ayinedjimi/sharepoint-onedrive-share-audit). Contributions et retours d'expérience bienvenus.