AYI NEDJIMI Consultants

SharePoint et OneDrive : Maîtriser le Partage Externe et

Catégorie : Microsoft 365 Lecture : 5 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide de sécurisation SharePoint Online et OneDrive : contrôle du partage externe, classification des données, DLP, sensitivity labels et prévention.

La configuration globale se fait via le SharePoint Admin Center ou PowerShell. Le parametre tenant definit le plafond : un site ne peut jamais etre plus permissif que le tenant. Voici la configuration recommandee pour un environnement d'entreprise standard. Guide de sécurisation SharePoint Online et OneDrive : contrôle du partage externe, classification des données, DLP, sensitivity labels et prévention. Microsoft 365 est omniprésent en entreprise et sa surface d'attaque ne cesse de s'étendre. La sécurisation de sharepoint onedrive partage externe securite nécessite une approche structurée et des outils adaptés. Nous abordons notamment : 7. liens avec d'autres domaines de securite, questions frequentes et conclusion. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

```
# Connexion au module SharePoint Online
Connect-SPOService -Url https://contoso-admin.sharepoint.com

# Configurer le tenant en mode "New and Existing External Users"
Set-SPOTenant -SharingCapability ExternalUserSharingOnly

# Forcer l'expiration des liens de partage externe (30 jours)
Set-SPOTenant -ExternalUserExpireInDays 30
Set-SPOTenant -ExternalUserExpirationRequired $true

# Limiter les domaines autorises pour le partage
Set-SPOTenant -SharingDomainRestrictionMode AllowList
Set-SPOTenant -SharingAllowedDomainList "partenaire1.com partenaire2.fr cabinet-audit.com"

# Desactiver les liens Anyone par defaut
Set-SPOTenant -DefaultSharingLinkType Internal
Set-SPOTenant -FileAnonymousLinkType View
Set-SPOTenant -FolderAnonymousLinkType View

# Exiger la reauthentification des guests tous les 15 jours
Set-SPOTenant -BccExternalSharingInvitations $true
Set-SPOTenant -BccExternalSharingInvitationsList "securite@contoso.com"
```

1.3 Surcharge par site

Chaque site SharePoint peut avoir un niveau de partage plus restrictif que le tenant. Cette granularite est essentielle pour segmenter les donnees par sensibilite. Un site "Projets Clients" peut autoriser le partage avec des guests authentifies, tandis qu'un site "Donnees RH" bloque tout partage externe.

```
# Site RH : pas de partage externe
Set-SPOSite -Identity "https://contoso.sharepoint.com/sites/DonneesRH" `
    -SharingCapability Disabled

# Site Projets Clients : guests existants uniquement
Set-SPOSite -Identity "https://contoso.sharepoint.com/sites/ProjetsClients" `
    -SharingCapability ExistingExternalUserSharingOnly

# Site Marketing : partage externe avec nouveaux guests (domaines restreints)
Set-SPOSite -Identity "https://contoso.sharepoint.com/sites/Marketing" `
    -SharingCapability ExternalUserSharingOnly `
    -SharingDomainRestrictionMode AllowList `
    -SharingAllowedDomainList "agence-com.fr media-partner.com"
```

1.4 Expiration et revocation

Les liens de partage sans expiration sont un vecteur de fuite dormant. Un collaborateur partage un document avec un prestataire en janvier ; le prestataire quitte sa mission en mars, mais le lien reste actif indefiniment. Pour contrer cela, Microsoft propose plusieurs mecanismes : l'expiration automatique des liens anonymes, la revocation des acces guest via Access Reviews dans Entra ID, et le controle des sharing links via les policies de site.

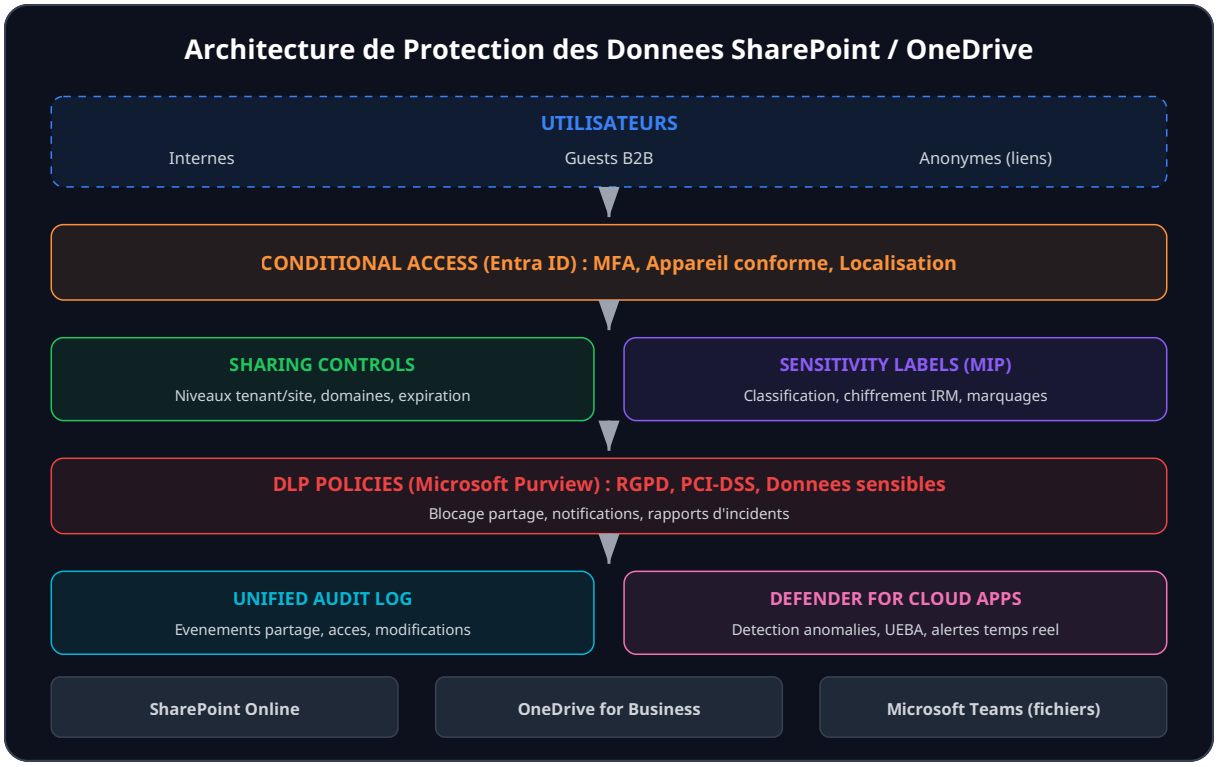
Point d'attention : liens "Anyone" sans expiration
Dans les organisations n'ayant jamais configure d'expiration, il est frequent de trouver des milliers de liens anonymes actifs datant de plusieurs mois voire annees. Un audit prealable via `Get-SPOSite | Get-SPOSiteGroup` et l'API Microsoft Graph est indispensable avant de deployer des politiques restrictives.

Microsoft Defender for Cloud Apps (anciennement MCAS) offre une couche de detection comportementale au-dessus des logs bruts. Il detecte des anomalies comme un utilisateur qui telecharge un volume inhabituel de fichiers, un acces depuis un pays inhabituel, ou un pattern d'exfiltration progressive. Les policies Defender for Cloud Apps specifiques a SharePoint incluent :

- **Mass download by a single user :** Alerte quand un utilisateur telecharge plus de X fichiers dans une fenetre de temps. Seuil recommande : 100 fichiers en 5 minutes.
- **Multiple sharing activities :** Detection d'un utilisateur qui partage massivement des fichiers avec des externes en peu de temps.
- **Access from risky IP :** Blocage ou alerte quand un acces SharePoint provient d'une IP sur liste noire (TOR, VPN anonymes, pays sous sanctions).
- **Impossible travel :** Detection d'acces depuis deux localisations geographiquement incompatibles dans un delai trop court.

- **Activity from inactive account :** Un compte guest dormant reprend soudainement de l'activite, signe potentiel de compromission.

L'integration avec Microsoft Sentinel permet d'alimenter un SIEM centralise avec les alertes Defender for Cloud Apps. Les equipes SOC peuvent alors correler les evenements SharePoint avec d'autres signaux (connexions suspectes Entra ID, alertes Defender for Endpoint) pour detecter des scenarios d'attaque complets comme l'exfiltration post-compromission d'un compte.



7. Liens avec d'Autres Domaines de Securite

La securisation de SharePoint et OneDrive ne se fait pas en silo. Elle s'integre dans une strategie de securite globale couvrant l'identite, la protection des endpoints, la conformite reglementaire et la detection des menaces. Voici les connexions avec d'autres domaines couverts dans nos articles :

- Exfiltration furtive de donnees : les techniques d'exfiltration via SharePoint (sync OneDrive, API Graph, liens anonymes) et comment les detecter avec les mecanismes presentes dans cet article.
- Securite OAuth et tokens : les applications tierces enregistrees dans Entra ID peuvent acceder a SharePoint via des permissions defi ees (Sites.Read.All, Files.ReadWrite.All). Un consentement abusif est un vecteur d'exfiltration massif.
- RGPD 2026 et conformite CNIL : les obligations de protection des donnees personnelles qui justifient les policies DLP et les Sensitivity Labels presentes dans cet article.
- Secrets Sprawl : les fichiers SharePoint et OneDrive contiennent souvent des secrets (cles API, mots de passe, certificats) stockes dans des documents non proteges. L'auto-labeling peut detecter ces patterns.

- Web Cache Deception : les portails SharePoint exposes sur Internet (extranet) peuvent etre cibles par des attaques de cache deception si un CDN est mal configure devant le reverse proxy.
- ISO 27001 Guide Complet : la gestion des actifs informationnels (A.8) et le controle d'acces (A.9) de l'ISO 27001 s'appuient directement sur les mecanismes de gouvernance SharePoint decrits ici.

Pour approfondir ce sujet, consultez notre outil open-source azure-ad-audit-tool qui facilite l'analyse de la configuration Azure AD.

Questions frequentes

Comment mettre en place SharePoint et OneDrive dans un environnement de production ?

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

Pourquoi SharePoint et OneDrive est-il essentiel pour la securite des systemes d'information ?

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

Quelles sont les bonnes pratiques pour SharePoint et OneDrive en 2026 ?

Les bonnes pratiques pour SharePoint et OneDrive en 2026 incluent l'adoption d'une approche Zero Trust, l'automatisation des controles de securite, la mise en place d'une veille continue sur les vulnerabilites et l'integration des recommandations des organismes de reference comme l'ANSSI et le NIST.

Sources et références : Microsoft Security Docs · CERT-FR

> Points clés à retenir
>
> - 7. Liens avec d'Autres Domaines de Securite
> - Questions frequentes
> - Conclusion

Conclusion

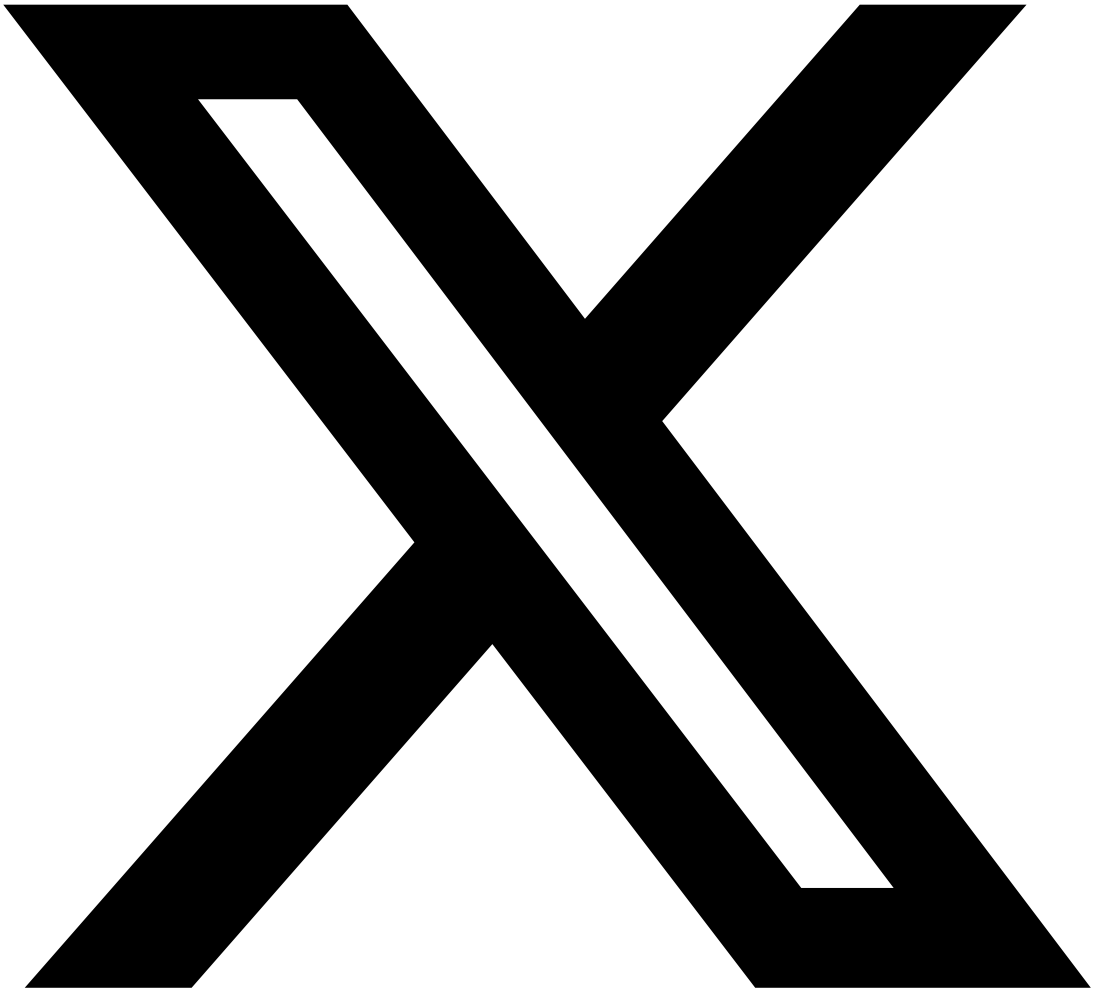
La securisation du partage externe dans SharePoint Online et OneDrive for Business est un equilibre permanent entre securite et productivite. L'approche recommandee repose sur cinq piliers : des **niveaux de partage differencies** par site en fonction de la sensibilite des donnees, une **classification automatique** via les Sensitivity Labels et l'auto-labeling, des **policies DLP** qui bloquent les fuites de donnees reglementees, une **gouvernance des permissions** avec des Access Reviews regulieres, et un **monitoring continu** croisant l'Unified Audit Log et Defender for Cloud Apps.

L'erreur la plus frequente est d'aborder la securite SharePoint de maniere reactive, apres un incident de fuite. L'approche proactive consiste a deployer ces controles de maniere progressive : commencer par l'audit de l'existant (liens actifs, guests, permissions), puis deployer les labels et DLP en mode observation avant de passer en mode bloquant. La communication avec les utilisateurs est essentielle : expliquez pourquoi un lien de partage est refuse, proposez des alternatives securisees, et formez les equipes aux bonnes pratiques de partage.

Enfin, n'oubliez pas que la securite SharePoint n'est qu'un maillon de la chaine. Un document correctement protege dans SharePoint peut etre exfiltre via un endpoint compromis, un consentement OAuth abusif, ou une synchronisation OneDrive non controlee. Seule une approche Zero Trust integrant l'identite, l'appareil, le reseau et les donnees offre une protection reellement efficace contre les fuites dans les environnements Microsoft 365 modernes.

Partagez cet Article

Cet article vous a ete utile ? Partagez-le avec votre reseau professionnel !

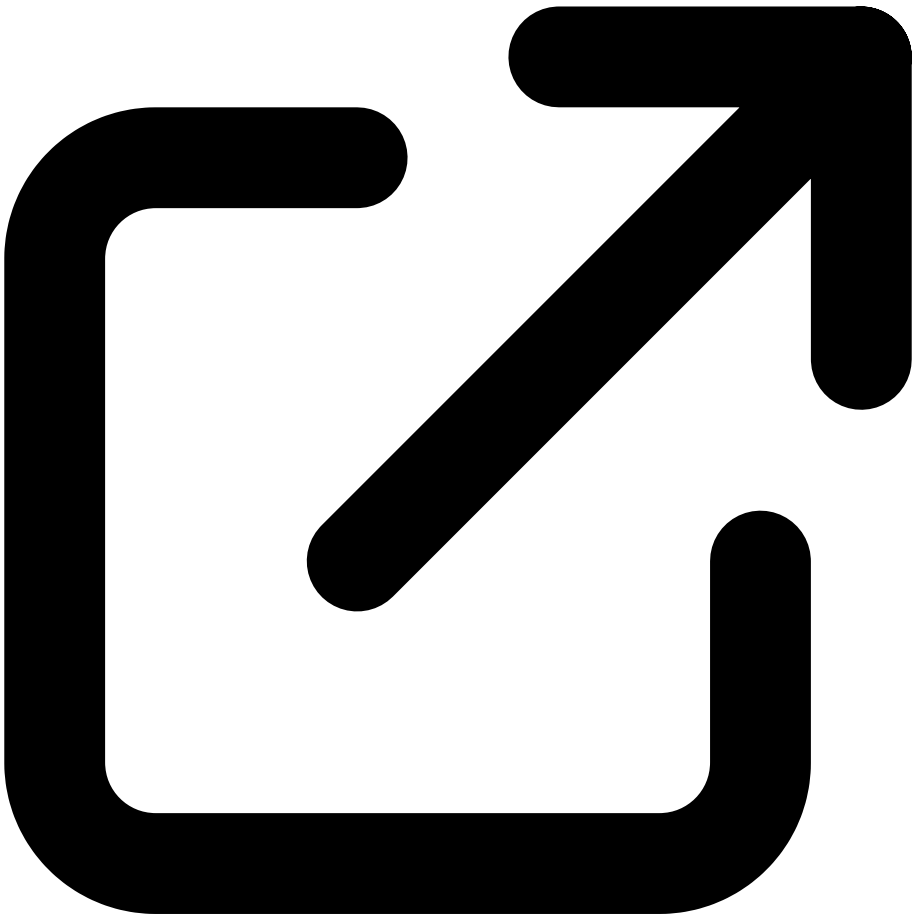


Partager sur X

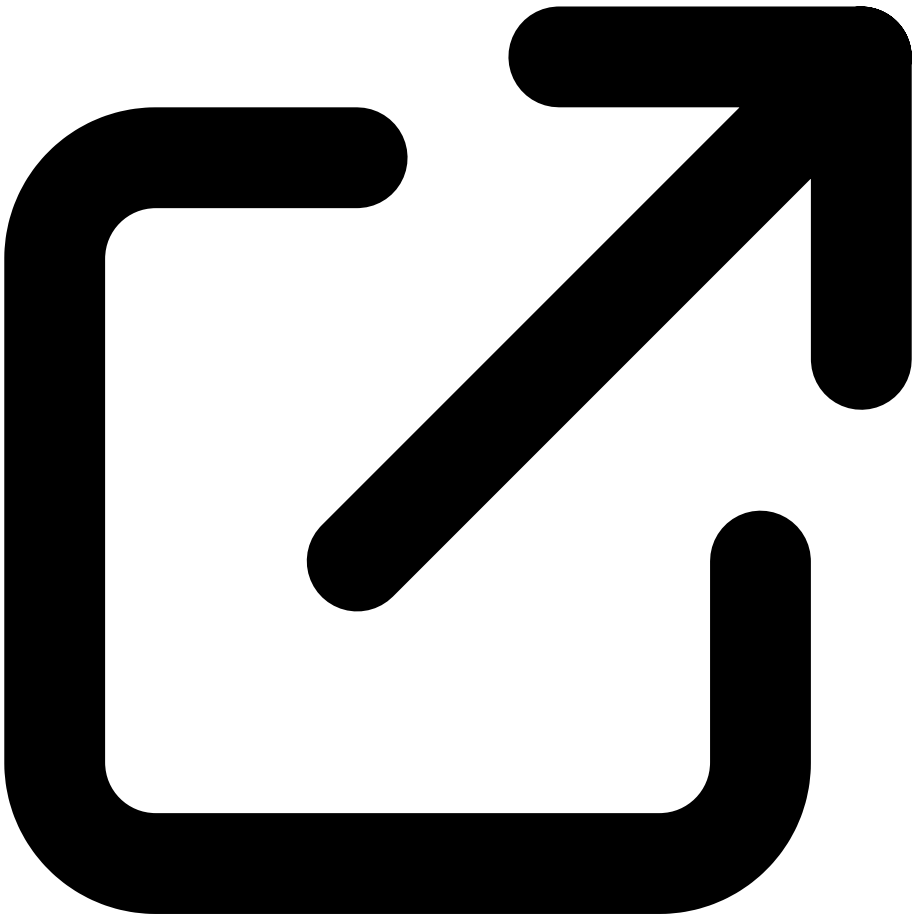
Partager sur LinkedIn

Ressources & References Officielles

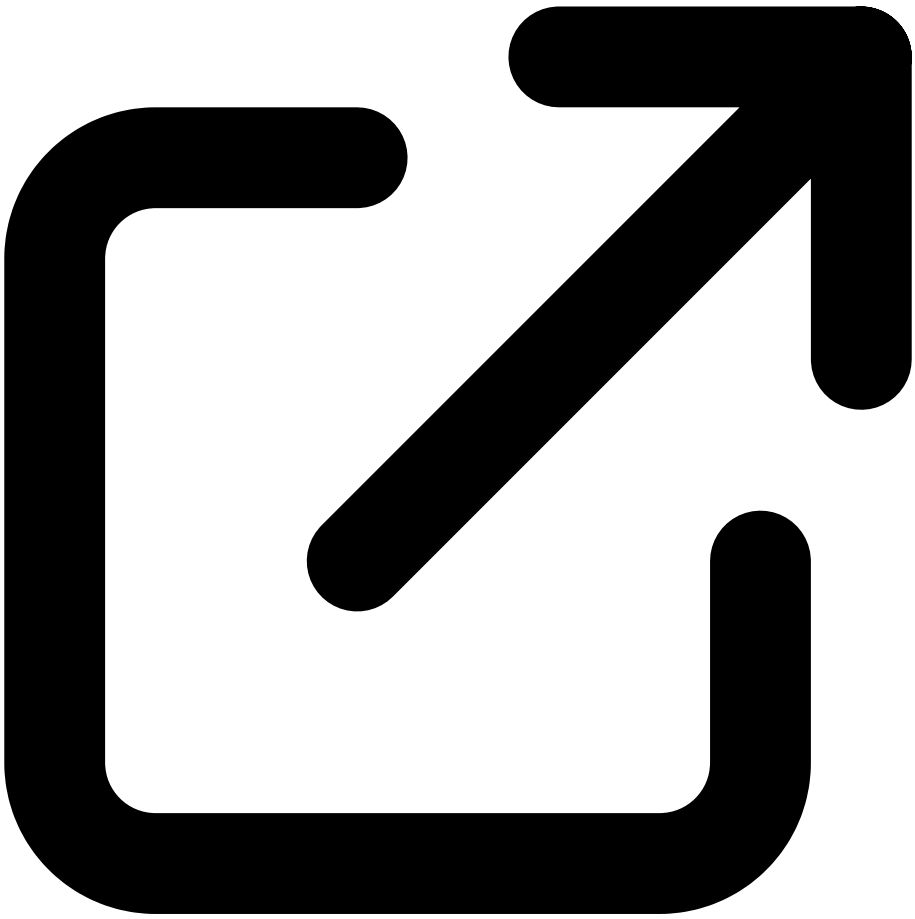
Documentations officielles et ressources de la communaute



Microsoft - SharePoint External Sharing
learn.microsoft.com



Microsoft Purview - Sensitivity Labels
learn.microsoft.com



Microsoft Purview - Data Loss Prevention
learn.microsoft.com

Ayi NEDJIMI

Expert en Cybersécurité & Intelligence Artificielle

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

LinkedIn Profil complet Tous ses articles

References et ressources externes

- Microsoft - External Sharing Overview -- Documentation officielle du partage externe SharePoint
- Microsoft Purview - Sensitivity Labels for SharePoint/OneDrive -- Guide de deploiement des labels sur les fichiers
- Defender for Cloud Apps - Protect Office 365 -- Policies de protection Cloud App Security
- CNIL - RGPD -- Obligations RGPD appliquees au stockage cloud

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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