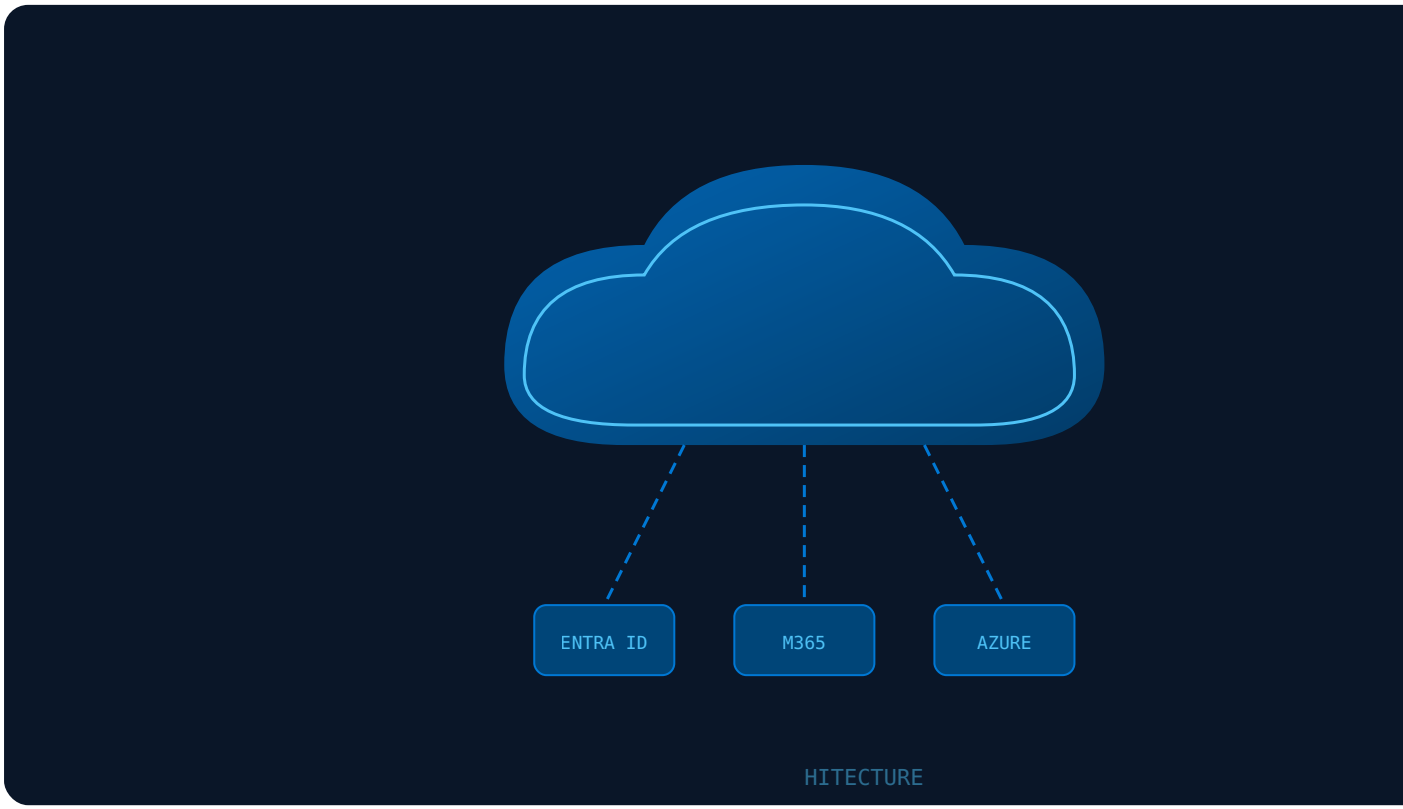
AYI NEDJIMI Consultants

Sécuriser Microsoft Teams : Gouvernance, DLP et Contrôle

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

Guide de sécurisation Microsoft Teams : gouvernance des équipes, DLP, applications tierces, partage externe, conformité RGPD et bonnes pratiques 2026.

Introduction



Microsoft Teams est devenu le hub de collaboration de plus de **320 millions d'utilisateurs actifs mensuels** en 2026. Cette adoption massive en fait simultanement un outil de productivite essentiel et un vecteur d'attaque privilege. Les messages de chat contiennent des credentials, les canaux hebergent des documents sensibles, les applications tierces accedent aux donnees via Graph API, et le partage externe ouvre des portes aux techniques d'exfiltration furtive. Selon Microsoft, 68 % des organisations n'ont pas de politique de gouvernance Teams formalisee, et 45 % autorisent l'installation non controlee d'applications tierces. Ce guide approfondi examine en detail les aspects fondamentaux et avances de Sécuriser Microsoft Teams, en proposant une analyse structuree et documentee des enjeux actuels. Les professionnels y trouveront des recommandations concretes, des methodologies eprouvees et des retours d'experience terrain directement applicables en environnement de production.

Points cles :

- Introduction
- Gouvernance des equipes
- Acces externe et invites
- DLP et protection des donnees
- Applications tierces : controle et audit

Ce guide couvre l'ensemble des mecanismes de securisation de Microsoft Teams : gouvernance des equipes (naming conventions, expiration, templates), gestion de l'acces externe et des invites B2B, protection des donnees avec DLP et les labels de sensibilite, controle des applications tierces via les permission policies et Resource-Specific Consent (RSC), securite des reunions (lobby, watermarks, chiffrement de bout en bout), et monitoring via les outils de compliance Microsoft Purview.

Perimetre de cet article
Cet article couvre la securisation de Microsoft Teams dans un contexte d'entreprise avec des licences **Microsoft 365 E3/E5**. Certaines fonctionnalites (DLP avancee, sensitivity labels automatiques, eDiscovery Premium) necessitent une licence E5 ou un add-on Microsoft 365 E5 Compliance.

Notre avis d'expert
L'identité cloud est le nouveau périmètre de sécurité dans un monde Microsoft 365. L'accès conditionnel, le MFA résistant au phishing et la gestion des sessions sont les trois piliers que nous auditons en priorité. Sans eux, le reste de la sécurité M365 est un château de cartes.

Gouvernance des equipes

Naming conventions et classification

Sans convention de nommage, les equipes proliferent de maniere anarchique : doublons, noms ambigus, equipes orphelines. Implementez des naming policies via Microsoft Entra ID pour imposer une structure coherente :

```
# Configurer la naming policy pour les groupes Microsoft 365 / Teams
Connect-MgGraph -Scopes "Directory.ReadWrite.All"

# Format : [Departement]-[NomProjet]-[Type]
# Exemple : IT-MigrationCloud-Projet, RH-Recrutement2026-Equipe
$namingPolicy = @{
    prefixSuffixNamingRequirement = "[Department]_[GroupName]_[CountryOrRegion]"
    customBlockedWordsList = @("CEO", "Confidentiel", "Secret", "Admin", "Root")
}

# Appliquer via GroupSettings
$settingsTemplate = Get-MgDirectorySettingTemplate | Where-Object { $_.DisplayName -eq
"Group.Unified" }
$settings = New-MgDirectorySetting -TemplateId $settingsTemplate.Id
Update-MgDirectorySetting -DirectorySettingId $settings.Id -Values @(
    @{ Name = "PrefixSuffixNamingRequirement"; Value = "[Department]_[GroupName]" }
    @{ Name = "CustomBlockedWordsList"; Value = "CEO,Confidentiel,Secret,Admin,Root" }
)
```

Expiration et cycle de vie

Les equipes inactives representent une surface d'attaque silencieuse : elles contiennent des donnees obsoletes, des membres ayant change de poste, et ne sont plus surveillees. Configurez une politique d'expiration :

- **Duree d'expiration** : 180 jours pour les equipes projet, 365 jours pour les equipes departementales.
- **Notification** : les proprietaires recoivent un e-mail 30 jours, 15 jours et 1 jour avant l'expiration.
- **Renouvellement** : le proprietaire peut renouveler l'equipe d'un clic. Si aucune action n'est prise, l'equipe est supprimee en soft-delete (recuperable pendant 30 jours).
- **Exception** : les equipes marquees comme "persistantes" (departement, direction) peuvent etre exemptees de l'expiration via un groupe de securite.

Templates d'equipe

Les templates Teams permettent de preconfigurer la structure des equipes (canaux, onglets, applications) et de standardiser la creation. Creez des templates pour chaque cas d'usage :

Template	Canaux preconfigures	Apps incluses	Label sensibilite
Projet Standard	General, Planning, Livrables	Planner, OneNote	Interne
Projet Client	General, Contrats, Livraisons	Planner, SharePoint	Confidentiel
Incident Response	Triage, Investigation, Remédiation	Lists, Wiki	Hautement confidentiel
Departement	Annonces, Ressources, Social	Viva Engage	Interne

Restriction de la creation d'equipes

Par defaut, tous les utilisateurs peuvent creer des equipes Teams, ce qui conduit a une proliferation incontrole. Restreignez la creation aux utilisateurs membres d'un groupe de securite specifique :

```
# Restreindre la creation de groupes/equipes a un groupe specifique
$groupCreatorsGroup = Get-MgGroup -Filter "displayName eq 'SG-Teams-Creators'"

$params = @{
    Values = @(
        @{ Name = "EnableGroupCreation"; Value = "false" }
        @{ Name = "GroupCreationAllowedGroupId"; Value = $groupCreatorsGroup.Id }
    )
}
Update-MgDirectorySetting -DirectorySettingId $settingId -BodyParameter $params
```

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

Acces externe et invites

Federation vs Guest Access

Teams propose deux mecanismes d'acces externe distincts qu'differencier :

- **Federation (External Access)** : permet la communication (chat, appels) avec des utilisateurs d'autres tenants Microsoft 365 ou Skype. Les utilisateurs externes restent dans leur propre tenant et n'ont pas acces aux fichiers ni aux canaux Teams. C'est un acces de communication uniquement.
- **Guest Access (B2B)** : les invites sont ajoutes comme membres d'une equipe. Ils accedent aux canaux, fichiers, applications et reunions de l'equipe. Ils apparaissent dans votre repertoire Entra ID comme des utilisateurs invites (userType = Guest). Ce modele offre plus de collaboration mais expose davantage de donnees.

Configuration recommandee pour l'acces externe

- **Federation** : limiter aux domaines de confiance (allowlist) plutot que d'autoriser tous les domaines. Bloquer les domaines connus comme malveillants.
- **Guest Access** : activer avec des restrictions strictes. Limiter les domaines autorises pour l'invitation B2B. Integrer avec Conditional Access pour forcer le MFA aux invites.
- **Anonymous join** : desactiver la participation anonyme aux reunions sauf exception documentee.

Conditional Access pour les invites B2B

Les invites representent un risque particulier car leur posture de securite n'est pas sous votre controle. Creez des politiques Conditional Access specifiques pour les invites, une approche coherente avec les techniques de prevention contre les attaques de phishing sans piece jointe :

- **MFA obligatoire** : forcez le MFA pour tous les invites, sans exception. Utilisez la cross-tenant access policy pour accepter le MFA du tenant d'origine si le tenant est de confiance.

- **Restriction d'applications** : limitez l'acces des invites a Teams et SharePoint Online uniquement, pas a l'ensemble du tenant M365.
- **Session controls** : activez le sign-in frequency de 4 heures et desactivez la persistance du navigateur pour les invites.
- **Localisation** : bloquez les connexions invites depuis des pays non autorises.

Access Reviews pour les invites

Les comptes invites ont tendance a persister bien apres la fin de la collaboration. Configurez des Access Reviews trimestrielles pour que les proprietaires d'equipes confirment que chaque invite est toujours necessaire. Activez l'auto-revocation apres 14 jours sans reponse. Ces revues sont complementaires a celles de PIM documentees dans l'article sur la gestion des acces privilegies Just-in-Time.

Cas concret
En janvier 2024, Microsoft a révélé que le groupe Midnight Blizzard (ex-Nobelium) avait compromis les boîtes mail de dirigeants Microsoft via une attaque par password spraying sur un compte de test sans MFA. Cet incident a démontré qu'aucune organisation n'est à l'abri et que les comptes de service non protégés sont des portes d'entrée critiques.

DLP et protection des donnees

Sensitivity Labels pour Teams

Les sensitivity labels (labels de sensibilite) de Microsoft Purview s'appliquent directement aux equipes Teams pour controler les parametres de securite au niveau du conteneur. Lorsqu'un label est applique a une equipe, il gouverne automatiquement :

- **Privacy** : l'equipe est publique ou privee.
- **Guest Access** : les invites externes sont autorises ou non dans cette equipe.
- **External Sharing** : le partage de fichiers SharePoint associe est restreint.
- **Unmanaged Device Access** : l'acces depuis des appareils non geres (BYOD) est autorise, limite (web only) ou bloque.
- **Meeting settings** : controle du watermark, du chiffrement E2E et de l'enregistrement.

Label	Privacy	Invites	BYOD	DLP
Public	Public	Autorise	Autorise	Standard
Interne	Prive	Autorise	Web only	Standard
Confidentiel	Prive	Restreint	Bloque	Stricte
Tres confidentiel	Prive	Bloque	Bloque	Chiffrement + DLP

Politiques DLP pour Teams

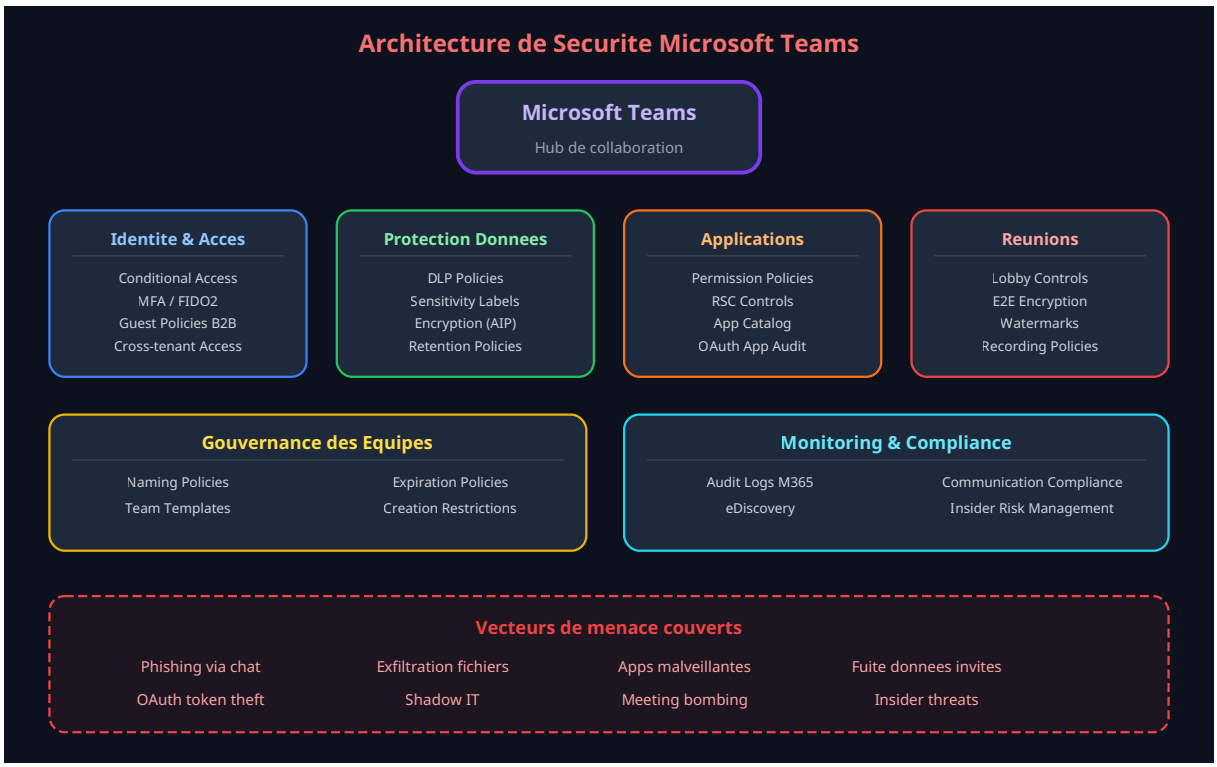
Les politiques DLP (Data Loss Prevention) de Microsoft Purview s'appliquent aux messages de chat Teams et aux fichiers partages dans les canaux. Elles detectent et bloquent le partage d'informations sensibles selon des types d'informations sensibles (SIT) preconfigures ou personnalises :

```
# Creer une politique DLP pour Teams
New-DlpCompliancePolicy -Name "DLP-Teams-Donnees-Sensibles" `
    -TeamsLocation All `
    -Mode Enable `
    -Comment "Protege contre la fuite de donnees sensibles dans Teams"

# Ajouter une regle pour detecter les numeros de carte bancaire
New-DlpComplianceRule -Name "Block-Credit-Cards-Teams" `
    -Policy "DLP-Teams-Donnees-Sensibles" `
    -ContentContainsSensitiveInformation @{
        Name = "Credit Card Number"
        MinCount = 1
        MinConfidence = 85
    } `
    -BlockAccess $true `
    -NotifyUser "SiteAdmin","LastModifier" `
    -NotifyPolicyTipCustomText "Ce message contient un numero de carte bancaire. Le
partage est bloque conformement a la politique de securite." `
    -GenerateIncidentReport "SiteAdmin" `
    -IncidentReportContent "All"

# Regle pour les donnees personnelles (RGPD)
New-DlpComplianceRule -Name "Warn-Personal-Data-Teams" `
    -Policy "DLP-Teams-Donnees-Sensibles" `
    -ContentContainsSensitiveInformation @(
        @{ Name = "France National ID Card (CNI)"; MinCount = 1; MinConfidence = 75 },
        @{ Name = "France Social Security Number (INSEE)"; MinCount = 1; MinConfidence =
75 },
        @{ Name = "EU Debit Card Number"; MinCount = 1; MinConfidence = 75 }
    ) `
    -NotifyUser "LastModifier" `
    -NotifyPolicyTipCustomText "Ce message semble contenir des donnees personnelles
protegees par le RGPD. Verifiez avant de partager."
```

Chiffrement et retention

Combinez les labels de sensibilite avec le chiffrement Azure Information Protection et les politiques de retention pour une protection complete, conforme aux exigences du RGPD 2026 :

- **Chiffrement des messages** : les messages dans les canaux marques "Tres confidentiel" sont chiffres au repos et en transit avec des cles gerees par le client (Customer Key).
- **Retention policies** : configurez une retention de 7 ans pour les canaux projet (obligation legale) et de 90 jours pour les conversations de chat informelles.
- **Information barriers** : isolez les equipes entre departements ayant des conflits d'interets (ex : Trading vs Compliance dans le secteur financier).



Applications tierces : controle et audit

Permission Policies

Les applications Teams constituent un vecteur d'attaque sous-estime. Une application tierce malveillante installee dans Teams peut acceder aux conversations, fichiers et contacts de l'utilisateur via Microsoft Graph API, un risque similaire aux vulnerabilites OAuth documentees dans nos articles. Implementez des permission policies a trois niveaux :

- **Org-wide settings** : desactivez l'installation d'applications tierces par defaut. Activez uniquement le catalogue d'applications approuvees par l'IT.
- **Permission policies par groupe** : creez des policies differentes pour les equipes IT (acces elargi aux applications de developpement), les equipes business (applications approuvees uniquement) et les equipes sensibles (aucune application tierce).
- **Setup policies** : pin les applications approuvees dans la barre laterale Teams et retirez les applications non approuvees.

Resource-Specific Consent (RSC)

RSC est un modele de permissions granulaire introduit par Microsoft pour Teams. Au lieu d'accorder des permissions tenant-wide via le consentement administrateur classique, RSC permet aux proprietaires d'equipes d'accorder des permissions limitees a l'equipe concernee uniquement. Les permissions RSC incluent :

- `TeamSettings.Read.Group` : lire les parametres de l'equipe.
- `ChannelMessage.Read.Group` : lire les messages des canaux.
- `TeamMember.Read.Group` : lire la liste des membres.

Audit des applications existantes
Avant de restreindre les applications, auditez les applications deja installees. Utilisez le **Teams Admin Center > Manage apps** pour identifier les applications avec des permissions Graph API elevees. Les applications demandant `Mail.ReadWrite`, `Files.ReadWrite.All` ou `User.ReadWrite.All` doivent etre examinees en priorite, en lien avec les risques decrits dans l'article sur les attaques API GraphQL et REST.

Votre configuration Microsoft 365 résisterait-elle à un audit de sécurité approfondi ?

Securite des reunions

Controles de lobby et admission

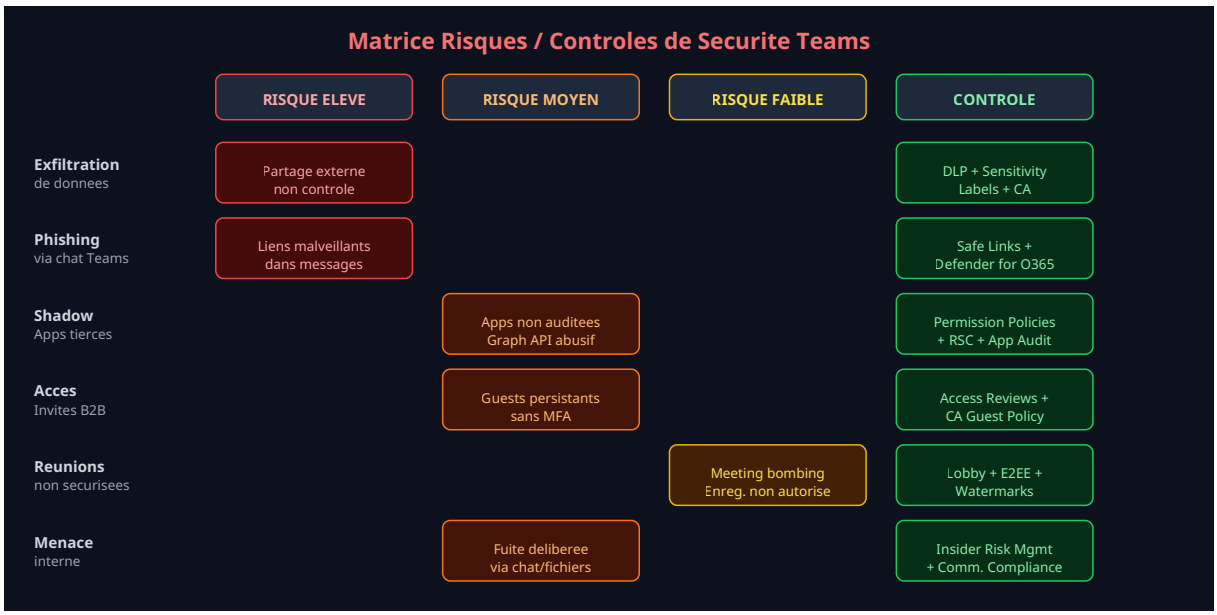
Les reunions Teams sont vulnerables au "meeting bombing" (intrusion d'utilisateurs non autorises) et a l'espionnage. Configurez les parametres de reunion selon la sensibilite :

Parametre	Standard	Confidentiel	Tres confidentiel
Qui contourne le lobby	Org uniquement	Organisateur seul	Organisateur seul
Enregistrement	Autorise	Organisateur	Desactive
Chat	Active	Active	Desactive
Watermark video	Non	Oui	Oui
E2E Encryption	Non	Non	Oui
Copilot	Active	Restreint	Desactive

Chiffrement de bout en bout (E2EE)

Le chiffrement de bout en bout pour les reunions Teams 1:1 et les reunions jusqu'a 200 participants est disponible depuis 2024. Lorsque E2EE est active, les flux audio, video et partage d'ecran sont chiffres de bout en bout, et Microsoft n'a pas acces aux cles de dechiffrement. Les limitations actuelles incluent :

- L'enregistrement cloud, les transcriptions et les sous-titres en direct sont desactives.
- Le Copilot ne peut pas acceder au contenu de la reunion.
- Les participants PSTN (dial-in) ne peuvent pas rejoindre.
- Les salles de sous-commission (breakout rooms) ne sont pas supportees.



Monitoring et conformite

Audit Logs et eDiscovery

Microsoft 365 Unified Audit Log capture l'ensemble des activites Teams : creation d'equipes, ajout/suppression de membres, messages envoyes (metadonnees), fichiers partages, applications installees, et parametres modifies. Ces logs sont essentiels pour la detection d'incidents et les investigations forensiques.

```
// KQL - Detecter les ajouts massifs de membres externes a Teams
OfficeActivity
| where Operation == "MemberAdded"
| where TargetUserOrGroupType == "Guest"
| extend TeamName = tostring(parse_json(tostring(Item)).ObjectId)
| summarize GuestAddedCount=count() by UserId, TeamName, bin(TimeGenerated, 1h)
| where GuestAddedCount > 5
| order by GuestAddedCount desc

// KQL - Applications Teams installees par les utilisateurs
OfficeActivity
| where Operation == "AppInstalled"
| extend AppName = tostring(parse_json(tostring(Item)).AppId)
| summarize InstallCount=count() by AppName, UserId
| order by InstallCount desc

// KQL - Fichiers partages avec des externes depuis Teams
OfficeActivity
| where Operation == "SharingSet" or Operation == "AnonymousLinkCreated"
| where OfficeWorkload == "SharePoint"
| extend SharedWith = tostring(TargetUserOrGroupName)
| where SharedWith has "#EXT#" or Operation == "AnonymousLinkCreated"
| project TimeGenerated, UserId, SourceFileName, SharedWith, Operation
```

Communication Compliance

Communication Compliance de Microsoft Purview permet de detecter les contenus inappropries, les violations de politique et les risques reglementaires dans les messages Teams. Les cas d'usage incluent :

- **Detection de langage offensant** : les classificateurs entraines par Microsoft detectent le harcelement, les menaces et le langage discriminatoire.
- **Conflits d'interet** : detection des communications entre departements soumis a des information barriers.
- **Partage de credentials** : detection de patterns correspondant a des mots de passe, cles API ou tokens partages dans les conversations Teams.
- **Conformite reglementaire** : surveillance des communications pour les secteurs reglementes (finance, sante) conformement aux exigences du RGPD.

Insider Risk Management

Insider Risk Management correle les activites Teams avec d'autres signaux (DLP violations, telechargements massifs, connexions inhabituelles) pour identifier les comportements a risque. Les indicateurs specifiques a Teams incluent :

- Telechargement massif de fichiers depuis des canaux Teams.
- Partage de fichiers avec des comptes personnels (gmail, outlook personnel).
- Copie de messages de canaux sensibles vers des conversations personnelles.
- Installation d'applications non approuvees juste avant un depart de l'entreprise.

Ces mecanismes de detection sont complementaires aux techniques de securisation de la supply chain applicative, car les applications Teams constituent un point d'entree potentiel pour les attaquants ciblant la chaine d'approvisionnement logicielle.

Questions frequentes

Comment mettre en place Sécuriser Microsoft Teams dans un environnement de production ?

La mise en place de Sécuriser Microsoft Teams 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 Sécuriser Microsoft Teams est-il essentiel pour la securite des systemes d'information ?

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

Comment auditer la configuration de sécurité de Sécuriser Microsoft Teams : Gouvernance, DLP et Contrôle ?

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

Pour approfondir ce sujet, consultez notre outil open-source m365-security-audit qui facilite l'audit de sécurité de l'environnement Microsoft 365.

Conclusion

La securisation de Microsoft Teams ne peut pas etre une reflexion apres-coup. Avec 320 millions d'utilisateurs actifs et une adoption croissante dans les processus critiques, Teams est devenu un systeme d'information a part entiere qui necessite une strategie de securite dediee, couvrant la gouvernance, la protection des donnees, le controle des applications et la surveillance continue.

Les cles d'un deploiement securise reposent sur cinq piliers : premierement, une **gouvernance rigoureuse** avec des naming conventions, des templates et des politiques d'expiration ; deuxiemement, un **controle strict de l'acces externe** avec des Conditional Access Policies dediees aux invites et des Access Reviews regulieres ; troisiemement, une **protection des donnees** via DLP, sensitivity labels et chiffrement ; quatriemement, un **controle des applications** avec des permission policies restrictives et un audit regulier des permissions Graph API ; et cinquiemement, un **monitoring continu** via les outils Microsoft Purview.

L'approche recommandee est progressive : commencez par restreindre la creation d'equipes et les applications tierces (gains rapides), puis deployez les sensitivity labels et les politiques DLP, et enfin implementez Communication Compliance et Insider Risk Management pour une couverture complete. Chaque etape renforce la posture de securite globale de votre environnement de collaboration.

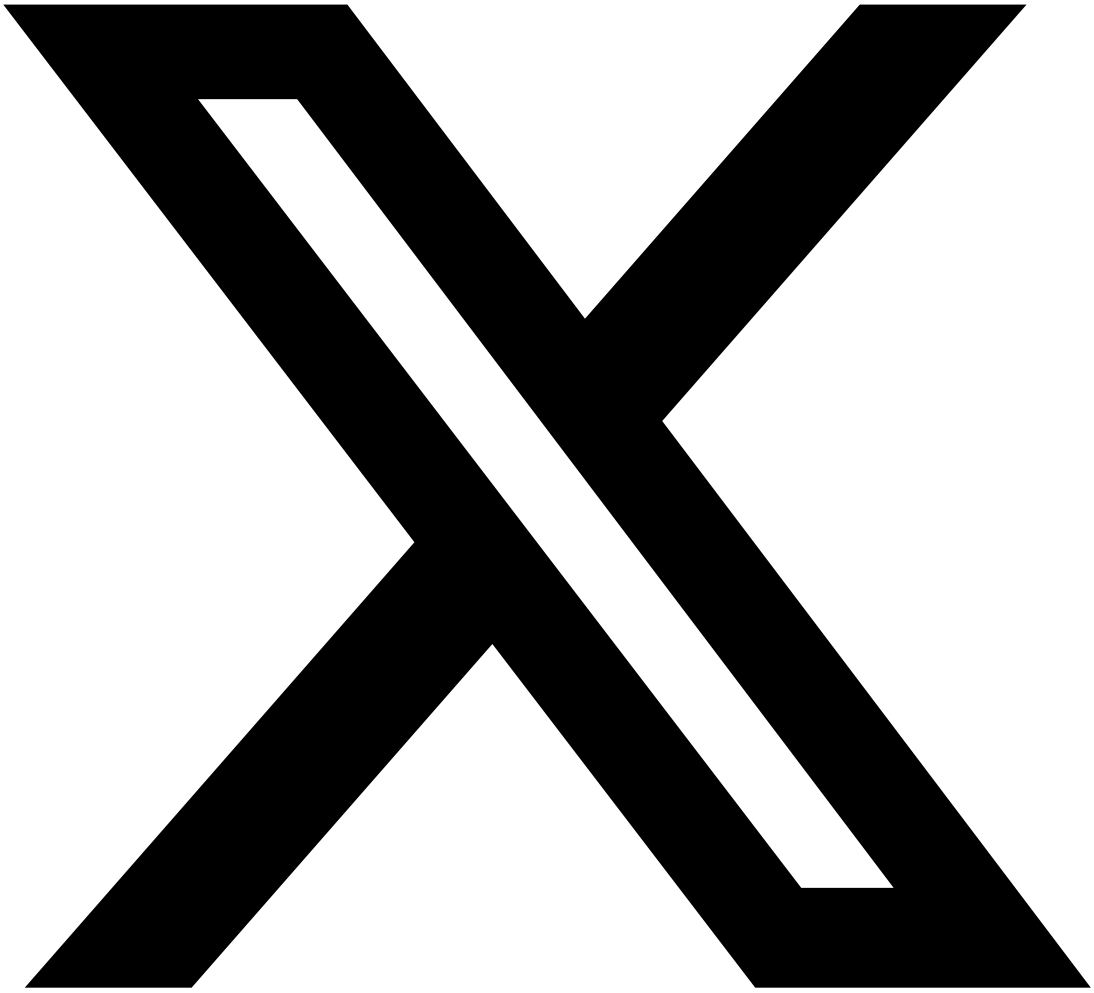
Sources et références : Microsoft Security Docs · CERT-FR

Articles complementaires

Techniques Hacking
Exfiltration Furtive
Techniques d'exfiltration de donnees et detection
Social Engineering
Phishing Sans Piece Jointe
Attaques de phishing modernes via liens et QR codes
Identity Security
OAuth Security
Vulnerabilites OAuth et securisation des flux
Conformite
RGPD 2026 Securite CNIL

Exigences RGPD pour la protection des donnees
Web & API
Attaques API GraphQL & REST
Securisation des API Microsoft Graph
Supply Chain
Supply Chain Applicative
Risques des dependances tierces et applications

Partagez cet article

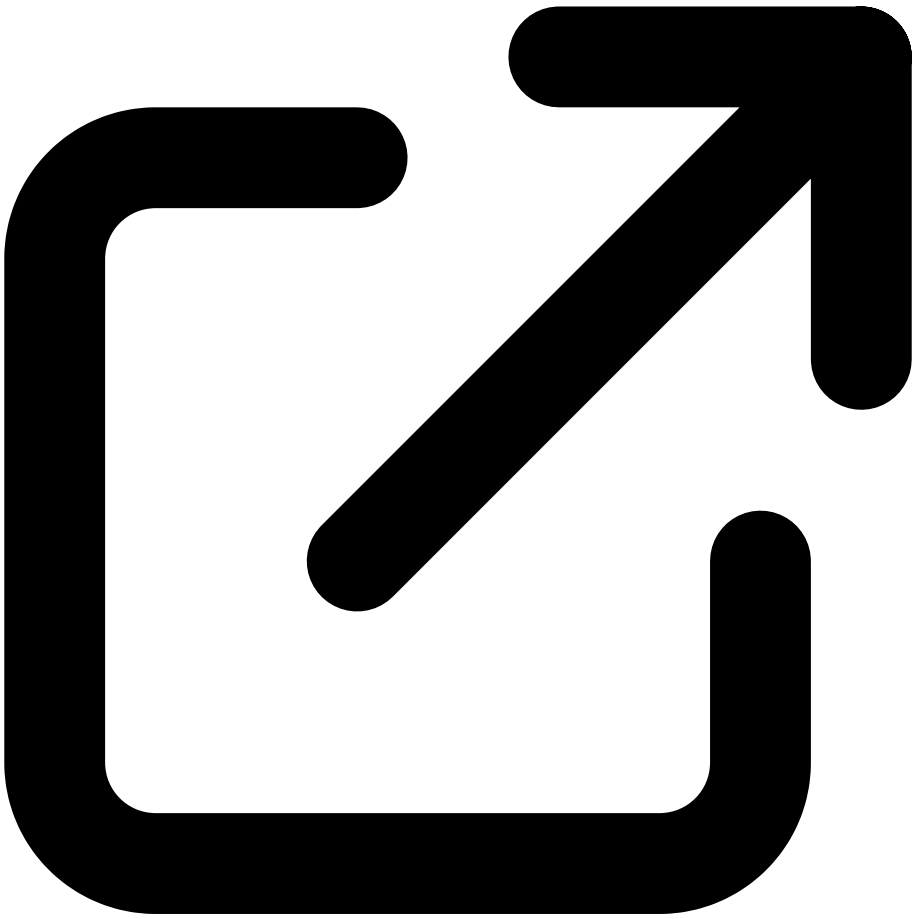


Partager sur X

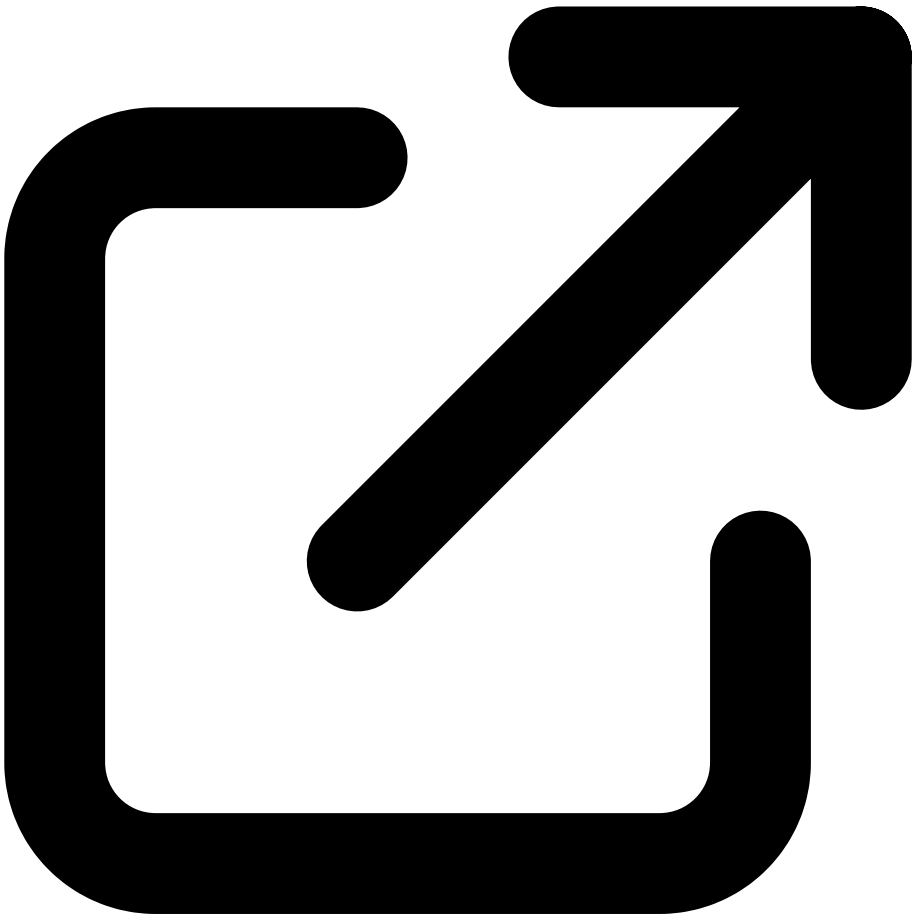
Partager sur LinkedIn

Ressources & References Officielles

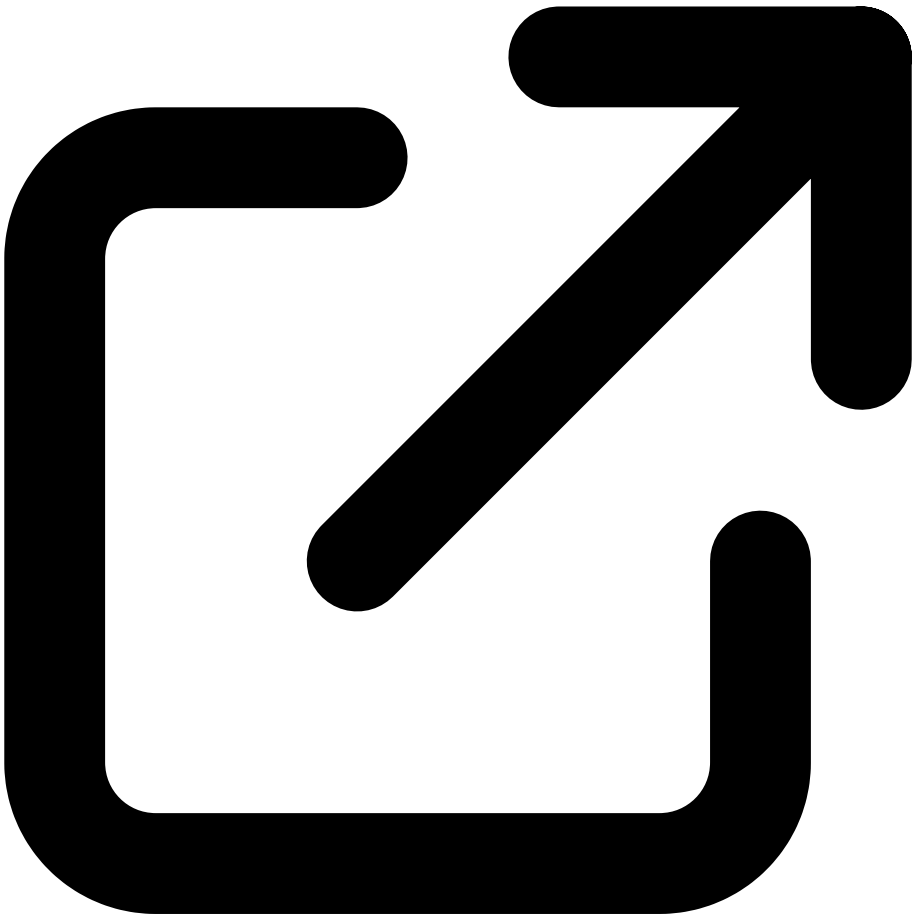
Documentations officielles Microsoft et guides de securite



Microsoft Teams Security & Compliance
learn.microsoft.com



DLP for Microsoft Teams
learn.microsoft.com



Manage Teams Apps
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 Teams Security Overview -- Documentation officielle securite et conformite Teams
- Sensitivity Labels for Teams -- Labels de sensibilite pour les equipes et sites
- MITRE ATT&CK T1199 -- Trusted Relationship : exploitation des acces partenaires
- CISA Best Practices -- Recommandations de securite pour les environnements collaboratifs

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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