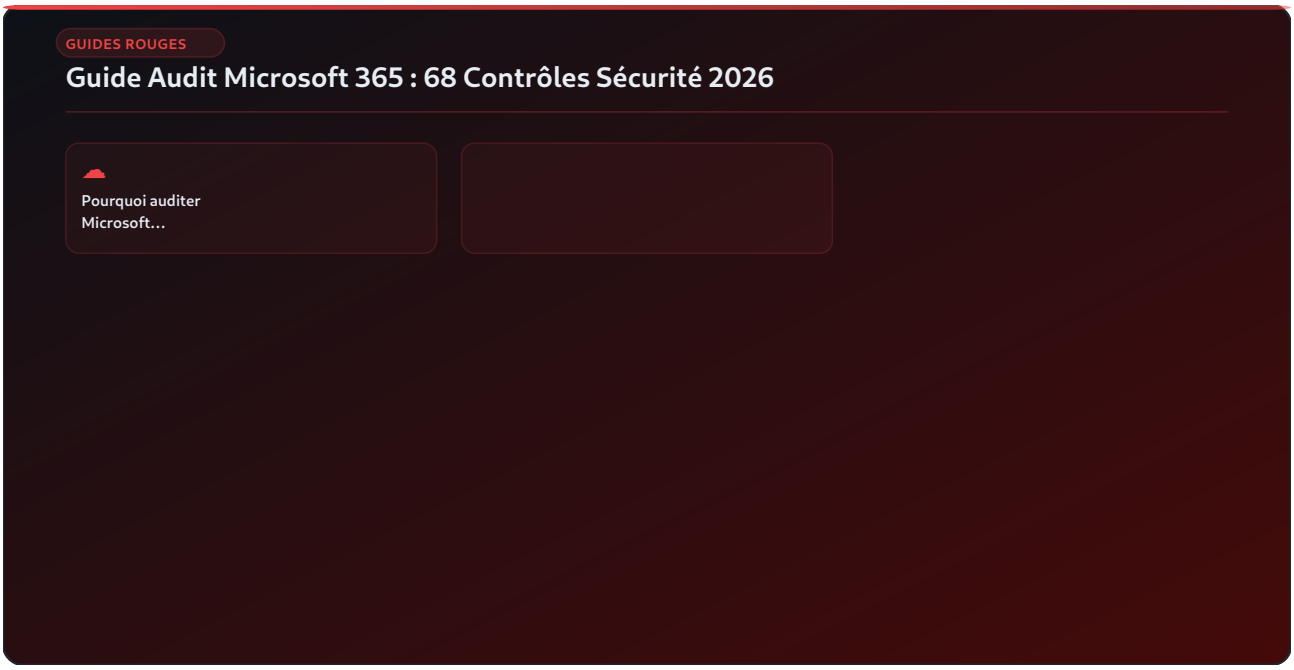
Guide Rouge : Audit Complet Microsoft 365 — 68 Contrôles

L'audit complet de Microsoft 365 est devenu incontournable pour toute organisation soucieuse de sa posture de sécurité. Avec plus de **400 millions d'utilisateurs actifs** dans le monde et une surface d'attaque en expansion permanente — **Entra ID**, Exchange Online, SharePoint, Teams, OneDrive, Defender, Purview — la plateforme concentre l'essentiel des identités, des données et des flux collaboratifs de l'entreprise. Une seule configuration permissive, un consentement applicatif oublié ou une règle de transfert malveillante suffisent à compromettre l'ensemble du tenant. Ce guide rouge structure la démarche autour de **68 contrôles** concrets, répartis par service et par niveau de criticité, du durcissement de l'authentification à la gouvernance des données. Chaque étape de cet **audit Microsoft 365 guide** vos équipes vers des vérifications reproductibles, mesurables et directement exploitables lors d'un audit interne, d'une certification ISO 27001 ou d'une réponse à incident.

En bref

- Un tenant M365 moyen (500 utilisateurs) expose 12 000+ permissions API via les applications enregistrées dans Entra ID
- Le temps moyen de détection d'une compromission M365 est de 197 jours sans audit proactif (IBM Cost of a Data Breach 2025)
- Les attaques de type AiTM phishing contournent le MFA dans 100 % des cas si aucune politique Conditional Access avec token binding ou Compliant Device n'est configurée
- Le coût moyen d'une compromission M365 (BEC, exfiltration de données) est de 4.88 millions de dollars en 2025
- Notre livre blanc Sécurité Microsoft 365 détaille les 50 contrôles prioritaires à implémenter immédiatement
- Obtenez une lettre de mission signée définissant le périmètre, la durée et les autorisations de l'audit



La question n'est plus de savoir si votre tenant Microsoft 365 sera ciblé, mais **quand**. Selon le rapport **Verizon DBIR 2025**, 74 % des compromissions impliquent un élément humain — vol d'identifiants, phishing, abus de privilèges — et Microsoft 365 concentre précisément ces trois vecteurs. Le rapport **CrowdStrike Global Threat Report 2026** documente une augmentation de 110 % des attaques ciblant les services d'identité cloud, Entra ID en tête. La compromission d'un seul compte Global Admin dans Entra ID donne un accès illimité à l'intégralité des données de l'organisation : emails, fichiers SharePoint, conversations Teams, pipelines DevOps, et même les applications SaaS fédérées via SAML ou OIDC.

La **surface d'attaque Microsoft 365** est considérable et en expansion permanente. Chaque nouveau service — Copilot, Loop, Viva, Fabric — ajoute des API, des permissions, des flux de données et des points d'intégration qu'un attaquant peut exploiter. En 2025, les techniques de compromission ont évolué bien au-delà du simple phishing par email :

Token theft et adversary-in-the-middle (AiTM) : des frameworks comme **Evilginx**, **Modlishka** et **EvilTokens** interceptent les jetons d'authentification post-MFA, rendant le MFA classique insuffisant

Consent phishing : l'attaquant enregistre une application malveillante dans Entra ID et convainc un utilisateur d'accorder des permissions OAuth étendues (`Mail.Read` , `Files.ReadWrite.All`)

Abuse d'applications enregistrées : les applications enregistrées dans Azure AD avec des secrets expirés ou des permissions excessives constituent des portes dérobées persistantes

Lateral movement via SharePoint et Teams : un attaquant ayant compromis un compte utilisateur standard peut accéder à des sites SharePoint sensibles si les permissions sont trop larges

Exfiltration via règles de transfert : la création silencieuse de règles Inbox Rules pour transférer les emails vers une adresse externe reste l'une des techniques les plus utilisées par les APT

Persistence via Service Principals : les Service Principals legacy permettent un accès programmatique persistant même après réinitialisation du mot de passe utilisateur

Entra ID : le nouveau périmètre de sécurité

Le paradigme traditionnel de sécurité périmétrique — pare-feu, DMZ, VPN — est obsolète dans un monde cloud-first. **Entra ID** (ex-Azure Active Directory) est devenu le **plan de contrôle central** : c'est lui qui authentifie les utilisateurs, autorise les accès, fédère les applications tierces, et conditionne l'application des politiques de sécurité. Un audit Microsoft 365 qui ne commence pas par Entra ID est fondamentalement incomplet.

Les statistiques sont éloquentes :

78 % des organisations ont au moins un compte Global Admin sans MFA activé (Microsoft Digital Defense Report 2025)

62 % des tenants M365 ont des politiques Conditional Access qui n'excluent pas les protocoles d'authentification legacy

45 % des applications enregistrées dans Entra ID ont des secrets qui n'ont pas été rotés depuis plus de 12 mois

89 % des incidents de sécurité M365 auraient pu être évités par une configuration correcte des Security Defaults ou du Conditional Access

À RETENIR

Surface d'attaque Microsoft 365 — Chiffres clés 2026

Un tenant M365 moyen (500 utilisateurs) expose **12 000+ permissions API** via les applications enregistrées dans Entra ID

Le temps moyen de détection d'une compromission M365 est de **197 jours** sans audit proactif (IBM Cost of a Data Breach 2025)

Les attaques de type **AiTM phishing** contournent le MFA dans 100 % des cas si aucune politique Conditional Access avec token binding ou Compliant Device n'est configurée

Le coût moyen d'une compromission M365 (BEC, exfiltration de données) est de **4.88 millions de dollars** en 2025

Notre livre blanc Sécurité Microsoft 365 détaille les 50 contrôles prioritaires à implémenter immédiatement

Prérequis et outillage de l'audit

Avant de lancer un audit Microsoft 365, il est essentiel de disposer des **permissions appropriées**, des **outils validés**, et d'une **méthodologie structurée**. Cette section détaille l'ensemble des prérequis techniques et organisationnels.

⚡ **Retour terrain**

L'une des leçons récurrentes de mes missions est que la sécurité n'est pas un état binaire mais un processus continu. Pour un groupe de distribution que j'accompagne depuis 3 ans, le niveau de maturité a progressé de façon mesurable — non pas parce que nous avons

tout sécurisé, mais parce que nous avons mis en place un cycle d'amélioration continue avec des métriques suivies au niveau direction.

Permissions requises dans Entra ID

L'audit nécessite un accès en lecture à l'ensemble de la configuration du tenant. Les rôles Entra ID recommandés sont :

Global Reader : lecture de toutes les configurations Entra ID, Exchange, SharePoint, Teams — c'est le rôle minimum pour un audit complet

Security Reader : accès aux alertes de sécurité, aux événements à risque, et aux rapports Defender

Compliance Reader : accès aux politiques DLP, aux labels de sensibilité, et aux rapports Purview

Exchange Administrator (en lecture) : accès aux configurations mail flow, anti-phishing, et DKIM/DMARC

SharePoint Administrator (en lecture) : accès aux paramètres de partage externe et aux permissions de site

Pour l'audit via **Microsoft Graph API** et PowerShell, vous aurez besoin d'une **App Registration** dédiée avec les permissions suivantes :

```
 # Permissions Microsoft Graph (Application)
Directory.Read.All
Policy.Read.All
AuditLog.Read.All
SecurityEvents.Read.All
# ... (extrait — voir documentation officielle)
```

Création de l'App Registration d'audit

La première étape technique consiste à créer une application dédiée dans Entra ID pour l'audit. Ce script PowerShell automatise le processus :

```
# ============================================================
# Création de l'App Registration dédiée à l'audit M365
# Auteur : Ayi NEDJIMI — Guide Rouge Audit M365
# ============================================================

# ... (extrait — voir documentation officielle)
```

Outils d'audit recommandés

L'écosystème d'outils d'audit M365 s'est considérablement enrichi. Voici les outils essentiels que tout auditeur doit maîtriser :

Maester — Framework d'audit automatisé

Maester est un framework open-source développé par la communauté Microsoft qui automatise les tests de conformité Entra ID et M365. Il s'appuie sur **Pester** (framework de tests PowerShell) et exécute plus de **180 contrôles** automatiquement :

```
# Installation de Maester
Install-Module Maester -Force -AllowClobber
Install-Module Pester -Force -SkipPublisherCheck

# Initialisation du répertoire de tests
# ... (extrait — voir documentation officielle)
```

ScubaGear — Outil CISA de conformité M365

ScubaGear (Secure Cloud Business Applications Gear) est l'outil officiel de la **CISA** (Cybersecurity and Infrastructure Security Agency) pour évaluer la conformité des tenants M365 par rapport aux **SCuBA baselines**. Il couvre 8 domaines :

```
# Installation de ScubaGear
Install-Module ScubaGear -Force

# Exécution de l'audit complet SCuBA
Invoke-SCuBA -ProductNames "*" -OutPath "C:\Audit-M365\ScubaGear"
# ... (extrait — voir documentation officielle)
```

AADInternals — Reconnaissance et audit offensif

AADInternals de Nestori Syynimaa est un outil de recherche en sécurité qui expose les fonctionnalités non documentées d'Entra ID. Pour l'auditeur, il permet de vérifier ce qu'un attaquant pourrait découvrir :

```
# Installation d'AADInternals
Install-Module AADInternals -Force

# Reconnaissance externe (sans authentification)
# Vérifie si un domaine utilise M365 et quel type de fédération
# ... (extrait — voir documentation officielle)
```

ROADtools — Cartographie d'Entra ID

ROADtools (Rogue Office 365 and Azure AD tools) de Dirk-jan Mollema permet de créer un snapshot complet du tenant Entra ID pour analyse hors ligne :

```
# Installation
pip install roadrecon roadlib

# Authentification
roadrecon auth -u auditor@entreprise.fr -p 'MotDePasse'
# ... (extrait — voir documentation officielle)
```

Hawk — Investigation de compromission

Hawk est un module PowerShell dédié à l'investigation de compromission M365. Il automatise la collecte des indicateurs de compromission :

```
# Installation de Hawk
Install-Module Hawk -Force

# Initialisation (définit la période d'investigation)
Initialize-HawkGlobalObject
# ... (extrait — voir documentation officielle)
```

Microsoft Graph PowerShell SDK

Le **Microsoft Graph PowerShell SDK** est l'outil de base pour interagir avec l'API Microsoft Graph. Notre article sur l'API Microsoft Graph pour l'audit et le monitoring détaille les techniques avancées.

```
 # Installation du SDK Microsoft Graph
Install-Module Microsoft.Graph -Force
Install-Module Microsoft.Graph.Beta -Force

# Connexion avec les scopes d'audit
# ... (extrait — voir documentation officielle)
```

À RETENIR

Checklist prérequis avant de lancer l'audit

Obtenez une **lettre de mission** signée définissant le périmètre, la durée et les autorisations de l'audit

Créez un compte **Global Reader** dédié à l'audit — ne réutilisez jamais un compte existant

Installez les modules PowerShell sur une **machine d'audit dédiée** (pas sur un poste utilisateur)

Vérifiez que l'**Unified Audit Log** est activé (`Get-AdminAuditLogConfig | Select UnifiedAuditLogIngestionEnabled`)

Documentez l'**état initial** du tenant avant toute modification : nombre d'utilisateurs, de licences, d'applications enregistrées

Prévoyez un espace de stockage sécurisé pour les **exports de données** (les exports UAL peuvent dépasser 50 Go pour un grand tenant)

Domaine 1 — Entra ID (Azure Active Directory)

Entra ID est le cœur de la sécurité Microsoft 365. C'est le service d'identité qui authentifie chaque utilisateur, chaque application, chaque appareil. Un audit Entra ID rigoureux couvre au minimum **15 domaines de contrôle** que nous détaillons ci-dessous. Pour approfondir les techniques d'attaque spécifiques à Entra ID, consultez notre guide de sécurisation Entra ID avec Conditional Access et MFA.

Contrôle 1.1 — Politiques Conditional Access

Les **Conditional Access Policies (CAP)** sont le mécanisme central de contrôle d'accès dans Entra ID. Elles permettent de conditionner l'accès aux ressources en fonction du contexte : identité, appareil, localisation, niveau de risque, application cible. Un tenant M365 sans Conditional Access correctement configuré est fondamentalement non sécurisé.

L'audit des politiques Conditional Access doit vérifier :

Couverture : toutes les applications cloud sont-elles couvertes par au moins une politique ?

MFA enforcement : le MFA est-il requis pour toutes les connexions, ou uniquement pour les administrateurs ?

Exclusions dangereuses : y a-t-il des comptes ou groupes exclus de toutes les politiques (break-glass accounts exclus) ?

Conditions de localisation : les Named Locations sont-elles correctement définies et utilisées ?

Device compliance : l'accès est-il conditionné à l'utilisation d'un appareil conforme (Intune) ?

Session controls : la durée des sessions et le re-auth sont-ils configurés pour les accès sensibles ?

```
 # ============================================================
# Audit complet des Conditional Access Policies
# ============================================================

# Récupération de toutes les politiques
# ... (extrait — voir documentation officielle)
```

Contrôle 1.2 — Configuration MFA et méthodes d'authentification

Le **Multi-Factor Authentication** est la première ligne de défense contre le vol d'identifiants. Mais toutes les méthodes MFA ne se valent pas : les SMS et appels vocaux sont vulnérables au SIM-swapping, tandis que les notifications push classiques sont vulnérables au **MFA fatigue** (l'attaquant bombarde la victime de notifications jusqu'à ce qu'elle approuve). Seules les méthodes **phishing-resistant** — FIDO2, Windows Hello for Business, Certificate-Based Authentication — protègent contre les attaques AiTM.

```
# ============================================================
# Audit de la configuration MFA et des méthodes d'authentification
# ============================================================

# Récupération de la politique d'authentification
# ... (extrait — voir documentation officielle)
```

Contrôle 1.3 — Blocage de l'authentification legacy

Les **protocoles d'authentification legacy** (IMAP, POP3, SMTP AUTH, EWS avec Basic Auth, ActiveSync avec Basic Auth) ne supportent pas le MFA. Un attaquant qui obtient un mot de passe via phishing ou password spraying peut contourner le MFA en utilisant ces protocoles. Microsoft a officiellement désactivé Basic Auth pour Exchange Online en octobre 2022, mais certains tenants conservent des exceptions ou utilisent des protocoles non couverts.

```
# ============================================================
# Audit du blocage de l'authentification legacy
# ============================================================

# Vérification dans les Conditional Access Policies
# ... (extrait — voir documentation officielle)
```

Contrôle 1.4 — Privileged Identity Management (PIM)

PIM (Privileged Identity Management) permet de gérer les rôles privilégiés avec des activations **Just-in-Time** : au lieu d'avoir un Global Admin permanent, l'utilisateur active le rôle pour une durée limitée, avec justification et approbation optionnelle. L'absence de PIM signifie que tous les administrateurs ont des privilèges **permanents** — un risque majeur en cas de compromission. Pour un guide détaillé, consultez notre article sur PIM Entra ID et la gestion des accès privilégiés Just-in-Time.

```
 # ============================================================
# Audit Privileged Identity Management (PIM)
# ============================================================

# Vérification de l'activation de PIM
# ... (extrait — voir documentation officielle)
```

Contrôle 1.5 — Applications enregistrées et Service Principals

Les **App Registrations** et **Service Principals** sont l'un des vecteurs de persistence les plus sous-estimés. Un attaquant qui compromet un Global Admin peut créer une application avec des permissions `Directory.ReadWrite.All` et un secret valide 2 ans — cette application continuera de fonctionner même après le changement du mot de passe admin. L'audit doit identifier toutes les applications, leurs permissions, leurs secrets, et les risques d'abus OAuth/OIDC associés.

```
 # ============================================================
# Audit des App Registrations et Service Principals
# ============================================================

$apps = Get-MgApplication -All
# ... (extrait — voir documentation officielle)
```

Contrôle 1.6 — Accès invités (Guest Access)

Les **utilisateurs invités (B2B)** dans Entra ID sont des comptes externes qui ont été invités à collaborer. Mal configurés, ils peuvent accéder à des ressources sensibles, énumérer l'annuaire, ou servir de pivot pour des attaques latérales. L'audit doit vérifier le nombre d'invités, leurs permissions, et les politiques de restriction.

```
 # ============================================================
# Audit des accès invités (Guest/B2B)
# ============================================================

$guests = Get-MgUser -Filter "userType eq 'Guest'" -All -Property "Id,DisplayName,Mail,UserPrincip
# ... (extrait — voir documentation officielle)
```

Contrôle 1.7 — Politiques de mots de passe et Password Protection

Même avec le MFA activé, les mots de passe restent critiques : ils constituent le premier facteur d'authentification et sont souvent réutilisés entre les comptes personnels et professionnels. Entra ID offre **Password Protection** qui bloque les mots de passe faibles et les variantes courantes.

```
# ============================================================
# Audit des politiques de mots de passe
# ============================================================

# Politique de mot de passe du tenant
# ... (extrait — voir documentation officielle)
```

Contrôle 1.8 — Sign-in Logs et détection des risques

Les **sign-in logs** d'Entra ID sont la source de données principale pour détecter les compromissions en cours. Entra ID Premium P2 ajoute la détection automatique des **risques d'identité** (Identity Protection) : connexions depuis des IP malveillantes, password spray détecté, token anomaly, impossible travel.

```
# ============================================================
# Audit des Sign-in Logs et Identity Protection
# ============================================================

$startDate = (Get-Date).AddDays(-30).ToString("yyyy-MM-ddTHH:mm:ssZ")
# ... (extrait — voir documentation officielle)
```

Contrôle 1.9 — Administrative Units et délégation

Les **Administrative Units** (AU) permettent de déléguer l'administration à des périmètres spécifiques — par département, filiale, pays ou entité juridique. Sans AU, un administrateur de mots de passe a la capacité de réinitialiser les mots de passe de **tous les utilisateurs du tenant**, y compris ceux d'autres filiales ou départements. Avec les AU, cette même permission est scoped à un sous-ensemble défini.

L'audit des Administrative Units vérifie plusieurs points critiques :

Existence et utilisation : des AU sont-elles définies ? Si l'organisation a plusieurs filiales ou départements, l'absence d'AU est un signal d'alarme

Couverture : tous les utilisateurs sensibles sont-ils membres d'une AU appropriée ?

Rôles au niveau tenant vs AU : des administrateurs qui devraient être limités à une AU ont-ils des rôles au niveau du tenant entier ?

Restricted Management AU : les AU à gestion restreinte empêchent même les Global Admins de modifier les objets qu'elles contiennent — une protection supplémentaire pour les comptes ultra-sensibles

```
 # ============================================================
# Audit des Administrative Units
# ============================================================

$adminUnits = Get-MgDirectoryAdministrativeUnit -All
# ... (extrait — voir documentation officielle)
```

Contrôle 1.10 — Named Locations et IP de confiance

Les **Named Locations** sont utilisées dans les politiques Conditional Access pour définir les réseaux de confiance (bureaux, VPN) et les zones à risque (pays à risque, Tor). L'audit vérifie que les plages IP sont à jour et que les pays bloqués correspondent à la politique de sécurité.

```
 # ============================================================
# Audit des Named Locations
# ============================================================

$locations = Get-MgIdentityConditionalAccessNamedLocation -All
# ... (extrait — voir documentation officielle)
```

Contrôle 1.11 — Rôles personnalisés et RBAC

Entra ID permet de créer des **rôles personnalisés** avec des permissions granulaires, au-delà des 80+ rôles built-in. L'audit vérifie que les rôles personnalisés n'accordent pas de permissions

excessives et que le principe du moindre privilège est respecté. Un rôle personnalisé mal conçu peut accidentellement accorder des permissions équivalentes à Global Admin.

Les points d'audit incluent :

Inventaire des rôles personnalisés : combien existent, par qui ont-ils été créés, à qui sont-ils assignés ?

Permissions dangereuses : certaines permissions individuelles sont critiques — `microsoft.directory/applications/credentials/update` permet d'ajouter un secret à n'importe quelle application

Rôles non utilisés : des rôles personnalisés créés mais jamais assignés encombrent la configuration

Comparaison avec les rôles built-in : un rôle personnalisé qui duplique un rôle built-in devrait être remplacé par ce dernier pour bénéficier des mises à jour Microsoft

```
 # ============================================================
# Audit des rôles personnalisés Entra ID
# ============================================================

$customRoles = Get-MgRoleManagementDirectoryRoleDefinition -Filter "isBuiltIn eq false" -All
# ... (extrait — voir documentation officielle)
```

Contrôle 1.12 — Tenant-wide settings et External Identities

Les paramètres au niveau du tenant contrôlent des comportements critiques : qui peut créer des groupes, qui peut enregistrer des applications, quel est le consentement utilisateur par défaut pour les applications OAuth. Ces paramètres sont souvent laissés à leurs valeurs par défaut — qui sont trop permissives.

```
 # ============================================================
# Audit des paramètres tenant-wide
# ============================================================

# Politique de consentement utilisateur
# ... (extrait — voir documentation officielle)
```

Contrôle 1.13 — Groupes dynamiques et assignation automatique

Les **groupes dynamiques** dans Entra ID ajoutent ou retirent automatiquement des membres basés sur des attributs utilisateur. Un groupe dynamique mal configuré peut accorder des accès non souhaités — par exemple, un groupe "Tous les employés IT" basé sur l'attribut `department eq 'IT'` qui inclut accidentellement des sous-traitants ayant le même département.

Contrôle 1.14 — Token lifetime et session policies

La durée de vie des tokens d'accès et des sessions détermine combien de temps un token volé reste exploitable. Par défaut, un **refresh token** est valide 90 jours — un attaquant qui vole un refresh token a donc 3 mois d'accès silencieux.

```
 # ============================================================
# Audit des Token Lifetime Policies
# ============================================================

$tokenPolicies = Get-MgPolicyTokenLifetimePolicy -All
# ... (extrait — voir documentation officielle)
```

Contrôle 1.15 — Provisioning et synchronisation hybride

Pour les organisations en mode hybride (Active Directory on-premises + Entra ID), la synchronisation via **Entra Connect** (ex-Azure AD Connect) est un point critique. Une compromission du serveur Entra Connect donne un accès direct au tenant cloud. Les risques incluent le SyncJacking et l'extraction des credentials de synchronisation.

```
 # ============================================================
# Audit de la synchronisation hybride
# ============================================================

# Vérification du statut Entra Connect
# ... (extrait — voir documentation officielle)
```

À RETENIR

Les 5 contrôles Entra ID les plus critiques

Conditional Access + MFA phishing-resistant pour tous les administrateurs — c'est la mesure #1 qui bloque 99.9 % des attaques d'identité

Blocage complet de l'authentification legacy — les protocoles Basic Auth contournent le MFA et doivent être bloqués sans exception

PIM activé pour tous les rôles Global Admin — aucun compte ne devrait avoir le rôle Global Administrator de manière permanente

Audit des App Registrations — identifiez et nettoyez les applications avec des secrets expirés, des permissions excessives, ou sans propriétaire

Restriction du consentement utilisateur — désactivez la possibilité pour les utilisateurs d'accorder des permissions OAuth sans approbation admin

Domaine 2 — Exchange Online

Exchange Online est le service de messagerie de Microsoft 365 et l'une des cibles prioritaires des attaquants. La compromission d'une boîte mail permet l'exfiltration de données sensibles, l'usurpation d'identité (BEC — Business Email Compromise), et la création de règles de persistence. L'audit Exchange Online couvre la configuration anti-phishing, les protocoles d'authentification email (SPF, DKIM, DMARC), les règles de flux de messagerie, et les paramètres de sécurité avancés. Pour un guide complet de durcissement, consultez notre article sur le durcissement Exchange Online et le blocage de l'authentification basique.

Contrôle 2.1 — Règles de flux de messagerie (Transport Rules)

Les **Transport Rules** d'Exchange Online permettent de modifier, rediriger ou bloquer des emails en transit. Un attaquant ayant compromis un compte admin Exchange peut créer des règles de

transport malveillantes pour intercepter tous les emails contenant certains mots-clés (facture, virement, mot de passe) ou pour supprimer les notifications de sécurité.

```
 # ============================================================
# Connexion à Exchange Online
# ============================================================
Import-Module ExchangeOnlineManagement
Connect-ExchangeOnline -UserPrincipalName auditor@entreprise.fr
# ... (extrait — voir documentation officielle)
```

Contrôle 2.2 — Règles de boîte mail (Inbox Rules)

Les **Inbox Rules** au niveau utilisateur sont le mécanisme de persistence #1 des attaquants BEC. Après compromission d'un compte, l'attaquant crée une règle qui transfère automatiquement tous les emails vers une adresse externe, ou qui supprime les emails de notification (réponses à des emails frauduleux envoyés depuis le compte compromis). Notre article sur la forensique Microsoft 365 et l'analyse du Unified Audit Log détaille les techniques d'investigation de ces incidents.

```
 # ============================================================
# Audit des Inbox Rules suspectes sur toutes les boîtes mail
# ============================================================

$mailboxes = Get-Mailbox -ResultSize Unlimited -RecipientTypeDetails UserMailbox
# ... (extrait — voir documentation officielle)
```

Contrôle 2.3 — Configuration anti-phishing et anti-spoofing

Les politiques **Anti-Phishing** d'Exchange Online Protection (EOP) et de **Defender for Office 365** protègent contre l'usurpation d'identité (impersonation), le spoofing de domaine, et le phishing ciblé. L'audit vérifie que ces protections sont activées et correctement configurées.

```
 # ============================================================
# Audit Anti-Phishing Policies
# ============================================================

$antiPhishPolicies = Get-AntiPhishPolicy
# ... (extrait — voir documentation officielle)
```

Contrôle 2.4 — SPF, DKIM et DMARC

Les trois protocoles d'authentification email — **SPF** (Sender Policy Framework), **DKIM** (DomainKeys Identified Mail) et **DMARC** (Domain-based Message Authentication, Reporting and Conformance) — constituent la base de la protection contre le spoofing de domaine. Sans DMARC en mode `reject`, n'importe qui peut envoyer des emails en usurpant votre domaine.

```
 # ============================================================
# Audit SPF, DKIM et DMARC
# ============================================================

# Récupération des domaines acceptés
# ... (extrait — voir documentation officielle)
```

Contrôle 2.5 — Mailbox Forwarding et délégation

Le transfert de boîte mail (mailbox forwarding) peut être configuré à plusieurs niveaux : SMTP forwarding au niveau de la boîte, Inbox Rules, et transport rules. Chaque niveau doit être audité séparément car ils ne sont pas visibles dans les mêmes interfaces.

```
 # ============================================================
# Audit complet du Mailbox Forwarding
# ============================================================

$mailboxes = Get-Mailbox -ResultSize Unlimited
# ... (extrait — voir documentation officielle)
```

Contrôle 2.6 — Safe Attachments et Safe Links

Safe Attachments et **Safe Links** sont des fonctionnalités de **Microsoft Defender for Office 365** (Plan 1 et 2) qui analysent les pièces jointes dans un sandbox et réécrivent les URLs pour vérification au moment du clic.

```
 # ============================================================
# Audit Safe Attachments et Safe Links
# ============================================================

# Safe Attachments
# ... (extrait — voir documentation officielle)
```

Contrôle 2.7 — Unified Audit Log (UAL)

Le **Unified Audit Log** est la source de données centrale pour la détection et l'investigation d'incidents dans Microsoft 365. Si l'UAL n'est pas activé, aucune investigation post-incident n'est possible. La rétention par défaut est de 180 jours (E5) ou 90 jours (E3).

```
 # ============================================================
# Vérification de l'Unified Audit Log
# ============================================================

$auditConfig = Get-AdminAuditLogConfig
# ... (extrait — voir documentation officielle)
```

Contrôle 2.8 — Configuration anti-spam

Les politiques **anti-spam** définissent les seuils de détection et les actions pour les emails indésirables. L'audit vérifie que les niveaux de filtrage sont appropriés et qu'aucune exception dangereuse n'a été créée. Les erreurs courantes incluent : la mise en liste blanche de domaines entiers (ce qui contourne le filtrage pour tous les emails de ce domaine), des seuils SCL trop élevés (qui laissent passer des spams), et l'absence de quarantaine pour les emails à haute confiance de phishing.

```
 # ============================================================
# Audit des politiques anti-spam
# ============================================================

$spamPolicies = Get-HostedContentFilterPolicy
# ... (extrait — voir documentation officielle)
```

Contrôle 2.9 — Permissions de boîtes mail partagées et délégation

Les **boîtes mail partagées** et les **délégations** (Send As, Send on Behalf, Full Access) sont souvent accordées de manière trop large et rarement auditées. Un utilisateur avec la permission `Full Access` sur une boîte exécutive peut lire tous les emails confidentiels sans que cela ne soit détecté dans les logs standards.

```
 # ============================================================
# Audit des permissions de boîtes mail
# ============================================================

$mailboxes = Get-Mailbox -ResultSize Unlimited -RecipientTypeDetails UserMailbox, SharedMailbox
# ... (extrait — voir documentation officielle)
```

Contrôle 2.10 — Quarantaine et notifications

La **quarantaine** Exchange Online retient les messages détectés comme malveillants ou suspects. L'audit vérifie que les politiques de quarantaine sont configurées pour notifier les administrateurs et que les utilisateurs n'ont pas la possibilité de libérer des messages de phishing hautement confirmés.

Contrôle 2.11 — Connecteurs et partenaires de messagerie

Les **connecteurs** Exchange Online définissent les routes de messagerie avec des systèmes externes (passerelles de sécurité, serveurs on-premises, partenaires). Un connecteur mal configuré peut permettre de contourner le filtrage anti-spam ou de relayer des emails sans authentification.

```
 # ============================================================
# Audit des connecteurs Exchange Online
# ============================================================

$inboundConnectors = Get-InboundConnector
# ... (extrait — voir documentation officielle)
```

Domaine 3 — SharePoint Online et OneDrive for Business

SharePoint Online et **OneDrive for Business** stockent les données les plus sensibles de l'organisation : documents stratégiques, rapports financiers, fichiers RH, propriété intellectuelle. La mauvaise configuration du partage externe est l'un des vecteurs d'exfiltration les plus courants — un simple lien anonyme créé par un utilisateur peut exposer des milliers de documents à Internet. Pour un guide détaillé, consultez notre article sur SharePoint et OneDrive : maîtriser le partage externe et la sécurité.

Contrôle 3.1 — Paramètres de partage externe

Le **partage externe** SharePoint/OneDrive est configuré à deux niveaux : au niveau du tenant (paramètres globaux) et au niveau de chaque site (qui peut être plus restrictif, mais jamais plus permissif que le tenant). Les quatre niveaux de partage sont :

Anyone (liens anonymes) : n'importe qui avec le lien peut accéder — le plus dangereux

New and existing guests : partage avec des invités, même non encore enregistrés dans Entra ID

Existing guests : partage uniquement avec des invités déjà présents dans l'annuaire

Only people in your organization : aucun partage externe — le plus sécurisé

```
 # ============================================================
# Connexion à SharePoint Online
# ============================================================
Import-Module Microsoft.Online.SharePoint.PowerShell
Connect-SPOService -Url "https://entreprise-admin.sharepoint.com"
# ... (extrait — voir documentation officielle)
```

Contrôle 3.2 — Liens anonymes et documents exposés

```
 # ============================================================
# Audit des liens anonymes actifs
# ============================================================

$sites = Get-SPOSite -Limit All -IncludePersonalSite $false
# ... (extrait — voir documentation officielle)
```

Contrôle 3.3 — Data Loss Prevention (DLP) SharePoint

Les politiques **DLP** (Data Loss Prevention) empêchent le partage accidentel ou malveillant de données sensibles (numéros de carte bancaire, données personnelles RGPD, informations médicales). L'audit vérifie que des politiques DLP sont en place, actives, et couvrent les types de données sensibles pertinents pour l'organisation. Une organisation sans DLP sur SharePoint est aveugle aux fuites de données — un employé peut partager un fichier Excel contenant 10 000 numéros de sécurité sociale avec un lien externe sans qu'aucune alerte ne soit générée.

Les contrôles DLP SharePoint à vérifier incluent :

Couverture des workloads : les politiques DLP couvrent-elles SharePoint, OneDrive, ET les conversations Teams ?

Types d'informations sensibles : les types RGPD (CNI, INSEE, IBAN, passeport) sont-ils configurés ?

Mode d'application : les politiques sont-elles en mode Enforce (bloque le partage) ou Test (notification seule) ?

Actions de remédiation : que se passe-t-il quand une violation est détectée ? Notification à l'utilisateur, blocage, notification au DPO ?

Exceptions : des groupes ou sites sont-ils exclus des politiques DLP ? Ces exceptions sont-elles justifiées ?

Contrôle 3.4 — Permissions des sites et héritage

Le modèle de permissions SharePoint repose sur l'**héritage** : par défaut, un sous-site ou une bibliothèque hérite des permissions du site parent. Lorsque l'héritage est cassé (broken inheritance), les permissions deviennent indépendantes et difficiles à auditer. L'accumulation de permissions cassées crée une **dette de sécurité significative** : après quelques années, personne ne sait exactement qui a accès à quoi.

L'audit des permissions SharePoint doit examiner :

Groupes SharePoint par défaut : les groupes Owners, Members et Visitors sont-ils utilisés correctement, ou des utilisateurs individuels sont-ils ajoutés directement ?

Permissions "Everyone" ou "Everyone except external users" : ces permissions accordent l'accès à tous les employés et sont souvent accordées par négligence

Sites avec héritage cassé : identifiez les bibliothèques et dossiers avec des permissions uniques et vérifiez que ces exceptions sont justifiées

Comptes de service et applications : des applications ou comptes de service avec Full Control sur des sites sensibles

Anciennes permissions : des employés qui ont quitté l'organisation mais dont les permissions n'ont pas été révoquées sur les sites SharePoint (l'offboarding ne nettoie pas toujours les permissions SharePoint directes)

```
 # ============================================================
# Audit des permissions SharePoint — sites sensibles
# ============================================================

# Liste des sites à auditer en priorité (RH, Finance, Direction)
# ... (extrait — voir documentation officielle)
```

Contrôle 3.5 — Versioning et Corbeille

Le **versioning** SharePoint est critique pour la récupération après une attaque ransomware. Si un attaquant chiffre tous les fichiers d'un site SharePoint via un compte compromis, les versions précédentes permettent de restaurer les données. Cependant, les attaquants sophistiqués connaissent cette protection et peuvent modifier les paramètres de versioning (réduire le nombre de versions à 1) avant de chiffrer les fichiers, rendant la restauration impossible. L'audit vérifie que :

Le versioning est activé avec un nombre suffisant de versions (**minimum 100**, idéalement 500 pour les bibliothèques critiques)

La corbeille de second niveau (site collection recycle bin) conserve les éléments pendant **93 jours**

Les permissions de modification des paramètres de versioning sont restreintes aux administrateurs de site

Un plan de sauvegarde externe existe (SharePoint n'est pas un service de backup — les sauvegardes Microsoft ne sont pas conçues pour la restauration granulaire à la demande)

Contrôle 3.6 — Applications tierces et compléments SharePoint

Les **compléments SharePoint** (add-ins) et les **applications tierces** installées dans le App Catalog peuvent accéder aux données des sites. L'audit inventorie toutes les applications installées, vérifie leurs permissions, et identifie les applications non approuvées ou obsolètes. Les risques incluent :

Applications avec permissions FullControl sur des sites contenant des données sensibles

Applications abandonnées dont l'éditeur n'existe plus ou ne fournit plus de mises à jour de sécurité

SPFx extensions non approuvées qui s'exécutent dans le contexte de l'utilisateur et peuvent accéder à toutes les données visibles

Webhooks et Flow/Power Automate connectés à des services externes non approuvés

Contrôle 3.7 — OneDrive for Business : synchronisation et restrictions d'appareils

```
 # ============================================================
# Audit OneDrive for Business
# ============================================================

Write-Host "=== AUDIT ONEDRIVE ===" -ForegroundColor Cyan
# ... (extrait — voir documentation officielle)
```

Contrôle 3.8 — Classification et étiquetage des sites

Les **labels de sensibilité** appliqués aux sites SharePoint permettent de contrôler automatiquement les paramètres de partage et d'accès en fonction de la classification du contenu. Un site étiqueté "Confidentiel" devrait automatiquement bloquer le partage externe.

Contrôle 3.9 — Alertes et monitoring SharePoint

Les alertes SharePoint permettent de détecter les activités suspectes : téléchargement massif de fichiers, modification de permissions, suppression de bibliothèques. L'audit vérifie que des alertes sont configurées pour les activités critiques.

Contrôle 3.10 — Information Barriers

Les **Information Barriers** empêchent certains groupes d'utilisateurs de communiquer ou de partager des documents entre eux (par exemple, entre le département Trading et le département Recherche dans une banque d'investissement). L'audit vérifie que les barriers sont correctement configurées pour les organisations soumises à des obligations réglementaires.

À RETENIR

Recommandations prioritaires SharePoint/OneDrive

Désactivez les **liens anonymes (Anyone)** au niveau du tenant — utilisez au minimum "New and existing guests" avec vérification d'identité

> Configurez une **expiration automatique** des liens de partage externe (maximum 30 jours pour les liens invités, 7 jours pour les liens anonymes si utilisés)
>
> Activez les **politiques DLP** pour détecter le partage de données sensibles (IBAN, numéros de carte, données RGPD)
>
> Restreignez la **synchronisation OneDrive** aux appareils gérés (domain-joined ou Intune compliant) via `AllowedDomainListForSyncClient`
>
> Activez **Safe Attachments pour SharePoint/OneDrive/Teams** — les fichiers malveillants uploadés dans SharePoint ne sont pas scannés par défaut sans Defender for Office 365

Domaine 4 — Microsoft Teams

Microsoft Teams est devenu le hub central de communication et de collaboration pour la majorité des organisations utilisant Microsoft 365. Avec plus de **320 millions d'utilisateurs actifs mensuels**, Teams gère les conversations, les fichiers, les réunions, et les intégrations applicatives. Les risques de sécurité sont multiples : accès invité non contrôlé, applications tierces avec des permissions excessives, fuites de données dans les conversations, et politiques de réunion trop permissives. Notre article sur la sécurisation de Microsoft Teams : gouvernance, DLP et contrôle fournit un guide complémentaire détaillé.

Contrôle 4.1 — Accès invité dans Teams

```
 # ============================================================
# Connexion à Microsoft Teams
# ============================================================
Import-Module MicrosoftTeams
Connect-MicrosoftTeams
# ... (extrait — voir documentation officielle)
```

Contrôle 4.2 — Accès externe (fédération)

L'**accès externe** (External Access / Federation) dans Teams permet aux utilisateurs de communiquer avec des utilisateurs d'autres organisations Teams ou Skype. Contrairement à l'accès invité (qui donne accès aux ressources du tenant), l'accès externe permet uniquement la messagerie et les appels. Cependant, il peut être utilisé pour du phishing ciblé via Teams.

```
 # ============================================================
# Audit de l'accès externe Teams
# ============================================================

$externalAccess = Get-CsTenantFederationConfiguration
# ... (extrait — voir documentation officielle)
```

Contrôle 4.3 — Politiques de réunion

Les **politiques de réunion** Teams contrôlent qui peut créer des réunions, qui peut rejoindre sans être admis (lobby bypass), et quelles fonctionnalités sont disponibles pendant la réunion. Des politiques trop permissives permettent à des utilisateurs anonymes de rejoindre des réunions confidentielles.

```
 # ============================================================
# Audit des politiques de réunion Teams
# ============================================================

$meetingPolicies = Get-CsTeamsMeetingPolicy
# ... (extrait — voir documentation officielle)
```

Contrôle 4.4 — Applications Teams autorisées

Les **applications Teams** (bots, onglets, connecteurs, extensions de messagerie) peuvent accéder aux conversations, fichiers et données utilisateur. L'audit vérifie quelles applications sont autorisées, si les applications tierces non vérifiées sont bloquées, et si des applications à risque sont installées.

```
 # ============================================================
# Audit des applications Teams
# ============================================================

$appPermissionPolicy = Get-CsTeamsAppPermissionPolicy
# ... (extrait — voir documentation officielle)
```

Contrôle 4.5 — Politiques de messagerie Teams

Les politiques de messagerie contrôlent les fonctionnalités disponibles dans les conversations Teams : édition et suppression de messages, URL previews, Giphy, mèmes, et — plus important pour la sécurité — la possibilité d'envoyer des messages urgents et des fichiers. Du point de vue de l'audit, les éléments critiques sont :

Suppression de messages : si les utilisateurs peuvent supprimer leurs messages, les preuves d'une communication suspecte peuvent être effacées. Dans les secteurs réglementés, la suppression devrait être désactivée ou limitée

URL preview : les previews d'URL révèlent l'IP du serveur Teams aux sites web visités et peuvent déclencher des actions côté serveur (pre-fetch). Certaines organisations les désactivent pour les conversations sensibles

Lecture de messages modifiés : la possibilité de voir l'historique des modifications d'un message est importante pour la traçabilité

```
 # ============================================================
# Audit des politiques de messagerie Teams
# ============================================================

$messagingPolicies = Get-CsTeamsMessagingPolicy
# ... (extrait — voir documentation officielle)
```

Contrôle 4.6 — DLP dans Teams

Les politiques **DLP** s'appliquent aux conversations et fichiers Teams pour empêcher le partage de données sensibles. Depuis 2024, les politiques DLP peuvent inspecter les messages Teams en temps réel et bloquer ou masquer les messages contenant des informations sensibles (numéros de

carte bancaire, IBAN, numéros de sécurité sociale). L'audit vérifie que les politiques DLP couvrent les canaux Teams publics, les canaux privés, et les conversations 1:1. Un point souvent oublié : les fichiers partagés dans Teams sont stockés dans SharePoint — les politiques DLP SharePoint s'appliquent donc également, mais les messages texte dans les conversations nécessitent une politique DLP Teams spécifique.

Contrôle 4.7 — Rétention et eDiscovery dans Teams

Les messages Teams, y compris les conversations privées (1:1 et group chats) et les messages de canal, sont soumis aux politiques de rétention Microsoft 365. Les messages Teams sont stockés dans des boîtes mail cachées dans Exchange Online (pour les 1:1 chats) et dans des boîtes de groupe (pour les canaux). L'audit vérifie que :

Une **politique de rétention Teams** spécifique existe (les politiques Exchange ne couvrent pas automatiquement les messages Teams)

La durée de rétention est conforme aux obligations légales et sectorielles

Les messages Teams sont **inclus dans l'eDiscovery** : un eDiscovery Manager peut-il rechercher et exporter les conversations Teams dans le cadre d'une investigation ?

Les **réactions, fichiers partagés, et messages modifiés/supprimés** sont inclus dans la rétention

Contrôle 4.8 — Canaux partagés et canaux privés

Les **canaux partagés** (Shared Channels) représentent un risque de sécurité unique : ils permettent de collaborer avec des utilisateurs d'autres organisations **sans les ajouter comme invités** dans Entra ID. Cela signifie que les utilisateurs externes n'apparaissent pas dans l'inventaire des guests et ne sont pas soumis aux politiques Conditional Access du tenant hôte. L'audit vérifie que :

La création de canaux partagés est **restreinte** aux équipes et utilisateurs approuvés

Les **Cross-tenant Access Policies** définissent explicitement quels tenants sont autorisés pour les canaux partagés

Les **canaux privés** sont inventoriés — chaque canal privé crée un site SharePoint séparé avec ses propres permissions, invisible depuis le site principal de la team

Les données partagées via les canaux partagés sont soumises aux **politiques DLP et de rétention**

Domaine 5 — Microsoft Defender

Microsoft Defender est la suite de protection intégrée à Microsoft 365 qui couvre la protection du courrier électronique (Defender for Office 365), des endpoints (Defender for Endpoint), des identités (Defender for Identity), et des applications cloud (Defender for Cloud Apps). L'audit vérifie que chaque composant est correctement configuré et que les alertes sont traitées.

Contrôle 5.1 — Defender for Office 365 : Plan et configuration

```
 # ============================================================
# Audit Defender for Office 365
# ============================================================

Write-Host "=== DEFENDER FOR OFFICE 365 ===" -ForegroundColor Cyan
# ... (extrait — voir documentation officielle)
```

Contrôle 5.2 — Defender for Endpoint : couverture et configuration

Defender for Endpoint (MDE) protège les postes de travail et les serveurs. L'audit vérifie le taux d'onboarding (combien d'appareils sont inscrits vs le parc total), la configuration des politiques de détection, et l'état des alertes non traitées.

```
 # ============================================================
# Audit Defender for Endpoint
# ============================================================

# Récupération des appareils onboarded
# ... (extrait — voir documentation officielle)
```

Contrôle 5.3 — Defender for Identity

Defender for Identity (ex-Azure ATP) surveille les contrôleurs de domaine Active Directory pour détecter les attaques d'identité en temps réel : Kerberoasting, Pass-the-Hash, Pass-the-Ticket, Golden Ticket, Diamond Ticket, reconnaissance LDAP, DCSync, Shadow Credentials. Pour les organisations en mode hybride (AD on-prem + Entra ID), Defender for Identity est un composant critique qui comble le gap de visibilité entre le monde on-premises et le cloud.

L'audit Defender for Identity vérifie :

Couverture des capteurs : un capteur Defender for Identity est-il installé sur **chaque** contrôleur de domaine, y compris les RODC et les DC de sites distants ?

Santé des capteurs : les capteurs sont-ils tous en ligne, avec des versions à jour ? Un capteur hors ligne crée un angle mort de détection

Configuration du compte de service : le compte gMSA ou Directory Service Account utilisé par le capteur a-t-il les permissions appropriées (lecture des objets AD, accès au SAM) ?

Alertes non traitées : combien d'alertes Defender for Identity sont en attente de traitement ? Les alertes supprimées l'ont-elles été pour de bonnes raisons ?

Exclusions : des comptes ou IP sont-ils exclus de la détection ? Ces exclusions réduisent la couverture et doivent être justifiées et documentées

Honeytokens : des comptes honeypot sont-ils configurés pour détecter les tentatives de reconnaissance LDAP ?

Contrôle 5.4 — Defender for Cloud Apps (CASB)

Defender for Cloud Apps (ex-MCAS) est le CASB (Cloud Access Security Broker) de Microsoft. Il remplit quatre fonctions essentielles pour la sécurité M365 :

Shadow IT Discovery : analyse des logs proxy/firewall pour identifier toutes les applications cloud utilisées par les employés — la plupart des organisations découvrent que leurs employés utilisent 200 à 500 applications cloud non approuvées

App Governance : surveillance des applications OAuth connectées à M365, détection des applications surprivilégiées ou malveillantes, révocation automatique des consentements suspects

Session Control : proxy inverse qui conditionne l'accès en temps réel — permet par exemple de bloquer le téléchargement de fichiers depuis un appareil non géré tout en autorisant la visualisation dans le navigateur

UEBA (User and Entity Behavior Analytics) : détection des comportements anormaux — un utilisateur qui télécharge 500 fichiers en une heure, qui se connecte depuis un pays inhabituel, ou qui accède à des données qu'il ne consulte jamais habituellement

L'audit vérifie que le Discovery est alimenté par les logs proxy, que les politiques de session sont configurées pour les applications sensibles, et que les alertes UEBA sont monitorées par le SOC.

Contrôle 5.5 — Politiques d'alerte et notification

Les alertes de sécurité Microsoft 365 ne sont utiles que si elles sont **lues et traitées**. L'audit vérifie que les alertes sont envoyées aux bonnes personnes et qu'un processus de traitement est en place. Les vérifications incluent :

Destinataires des alertes : les alertes critiques sont-elles envoyées à une liste de distribution de sécurité, ou à un individu qui pourrait être en vacances ?

Alertes personnalisées : au-delà des alertes par défaut, des alertes personnalisées sont-elles configurées pour les événements critiques spécifiques à l'organisation (modification de Conditional Access, ajout d'un Global Admin, création d'un connecteur Exchange) ?

Intégration SIEM : les alertes Microsoft 365 sont-elles intégrées dans le SIEM de l'organisation (Sentinel, Splunk, QRadar) pour corrélation avec d'autres sources ?

Temps de traitement : quel est le temps moyen entre la génération d'une alerte et sa prise en charge ? Les benchmarks recommandent moins de 15 minutes pour les alertes critiques

```
 # ============================================================
# Audit des politiques d'alerte M365
# ============================================================

$alertPolicies = Get-ProtectionAlert
# ... (extrait — voir documentation officielle)
```

Contrôle 5.6 — Automated Investigation and Response (AIR)

L'**investigation automatisée (AIR)** dans Defender for Office 365 Plan 2 et Defender for Endpoint permet de trier automatiquement les alertes et de proposer ou exécuter des actions de remédiation. AIR peut automatiquement supprimer les emails de phishing livrés dans les boîtes mail, bloquer les URL malveillantes, isoler les endpoints compromis, et révoquer les sessions utilisateur suspectes.

L'audit vérifie que AIR est activé et que le **niveau d'automatisation** est approprié. Trois niveaux existent : Full (les actions sont exécutées automatiquement), Semi (les actions nécessitent une approbation humaine), et No automated response (désactivé). Pour la plupart des organisations, le mode **Semi** est recommandé — il combine la rapidité de l'automatisation avec le contrôle humain pour éviter les faux positifs.

Contrôle 5.7 — Threat Intelligence et IOC personnalisés

Les **Indicators of Compromise** (IOC) personnalisés permettent de bloquer proactivement des domaines, IP, URLs ou hash de fichiers connus comme malveillants, issus de la veille threat intelligence de l'organisation ou de feeds tiers. L'audit vérifie que des IOC sont configurés et mis à jour régulièrement. Les sources d'IOC recommandées incluent : les bulletins CERT-FR/ANSSI, les feeds STIX/TAXII de l'industrie, les rapports d'incidents internes, et les plateformes de partage comme MISP. Un tenant M365 sans IOC personnalisés repose uniquement sur la threat intelligence de Microsoft, qui est excellente mais ne couvre pas les menaces spécifiques à votre secteur ou organisation.

Contrôle 5.8 — Attack Surface Reduction (ASR) Rules

Les règles **ASR** (Attack Surface Reduction) bloquent les comportements couramment exploités par les malwares : exécution de macros Office, scripts obfusqués, création de processus enfants depuis Office, utilisation de WMI pour la persistence. L'audit vérifie que les règles ASR critiques sont en mode Block (pas seulement Audit).

```
 # ============================================================
# Audit des règles ASR via Intune/Graph
# ============================================================

$asrPolicies = Invoke-MgGraphRequest -Method GET -Uri "https://graph.microsoft.com/beta/deviceMana
# ... (extrait — voir documentation officielle)
```

Domaine 6 — Compliance et Microsoft Purview

Microsoft Purview (ex-Microsoft 365 Compliance) regroupe les outils de gouvernance des données, de protection de l'information, et de conformité réglementaire. Pour les organisations soumises au RGPD, à NIS2, à DORA, ou à des réglementations sectorielles, l'audit Purview est incontournable.

Contrôle 6.1 — Labels de sensibilité (Sensitivity Labels)

Les **labels de sensibilité** permettent de classifier et protéger les données en fonction de leur niveau de confidentialité. Un label peut appliquer automatiquement le chiffrement, le filigrane, les restrictions de copie/impression, et le contrôle d'accès. L'audit vérifie que les labels sont définis, publiés, et effectivement utilisés.

```
 # ============================================================
# Audit des Sensitivity Labels
# ============================================================

# Connexion au Security & Compliance Center
# ... (extrait — voir documentation officielle)
```

Contrôle 6.2 — Politiques DLP (Data Loss Prevention)

```
 # ============================================================
# Audit des politiques DLP
# ============================================================

$dlpPolicies = Get-DlpCompliancePolicy
# ... (extrait — voir documentation officielle)
```

Contrôle 6.3 — Politiques de rétention

Les **politiques de rétention** définissent combien de temps les données sont conservées et quand elles sont supprimées. En France, les obligations légales varient selon le type de données : 10 ans pour les documents comptables, 5 ans pour les contrats commerciaux, 5 ans après le départ pour les données RH, et des obligations spécifiques RGPD pour les données personnelles (conservation limitée à la durée nécessaire). L'audit vérifie la couverture des politiques (Exchange, SharePoint, OneDrive, Teams) et leur conformité avec ces obligations.

```
 # ============================================================
# Audit des politiques de rétention
# ============================================================

$retentionPolicies = Get-RetentionCompliancePolicy -DistributionDetail
# ... (extrait — voir documentation officielle)
```

Contrôle 6.4 — eDiscovery et Legal Hold

L'**eDiscovery** permet de rechercher, collecter et exporter des données Microsoft 365 dans le cadre d'enquêtes juridiques, d'incidents de sécurité, ou de conformité réglementaire. Le **Legal Hold** (conservation juridique) empêche la suppression de données sous investigation — même si l'utilisateur ou un administrateur tente de les supprimer. L'audit vérifie plusieurs aspects critiques :

Accès eDiscovery : qui a le rôle eDiscovery Manager ou eDiscovery Administrator ? Ces rôles donnent accès à toutes les données du tenant — un abus est un risque d'insider threat majeur

Cas eDiscovery actifs : y a-t-il des cas ouverts ? Sont-ils suivis et fermés quand l'investigation est terminée ?

Legal Holds actifs : quels utilisateurs ou boîtes mail sont sous Legal Hold ? Un Hold oublié conserve des données indéfiniment et peut poser des problèmes RGPD (conservation excessive)

Recherches de conformité : les recherches effectuées par les eDiscovery Managers sont-elles auditées et justifiées ?

Contrôle 6.5 — Insider Risk Management

L'**Insider Risk Management** (IRM) détecte les comportements à risque des employés en corrélant plusieurs signaux : téléchargement massif de fichiers, copie de données sur USB, impression de documents sensibles, accès inhabituels à des données hors de leur périmètre, activité après les heures de bureau, et — critiquement — les signaux RH comme un préavis de départ ou une mise en plan de performance. La combinaison de ces signaux permet de détecter l'exfiltration de données avant un départ, le vol de propriété intellectuelle, ou le sabotage intentionnel.

L'audit vérifie que les politiques IRM sont configurées, que les indicateurs pertinents sont activés (signaux Office, signaux endpoint via Defender for Endpoint, signaux RH si connecteur HR disponible), et que les alertes sont traitées par un comité approprié (RH + Sécurité + Juridique). La confidentialité est un point critique : les noms des utilisateurs à risque doivent être pseudonymisés par défaut et ne sont révélés qu'aux personnes autorisées dans le cadre d'une investigation formelle.

Contrôle 6.6 — Communication Compliance

Communication Compliance surveille les communications (emails, Teams, Yammer) pour détecter les violations de politique : divulgation d'informations confidentielles, harcèlement, langage inapproprié, conflit d'intérêt, et communication non conforme dans les secteurs réglementés (finance, santé). L'audit vérifie la configuration et la couverture des politiques. Pour les organisations soumises à **MiFID II**, **SOX**, ou des réglementations sectorielles, la surveillance des communications est une obligation légale — l'absence de Communication Compliance expose l'organisation à des sanctions réglementaires.

Contrôle 6.7 — Information Barriers

Les **Information Barriers** empêchent la communication et le partage de documents entre des segments d'utilisateurs définis. Elles sont obligatoires dans certains secteurs réglementés — par exemple, dans une banque d'investissement, le département Research ne doit pas pouvoir communiquer avec le département Trading pour prévenir le délit d'initié. L'audit vérifie que les segments sont correctement définis, que les barrières sont appliquées à Teams, SharePoint et OneDrive, et qu'aucun utilisateur n'est accidentellement bloqué ou autorisé à tort.

Contrôle 6.8 — Audit logs et alertes Purview

Purview génère ses propres logs d'audit pour tracer les activités de conformité : recherches eDiscovery effectuées par les managers, modifications de politiques DLP, changements de labels de sensibilité, violations DLP détectées et leurs résolutions. L'audit vérifie que ces logs sont activés, conservés pendant une durée suffisante (minimum 1 an), et monitorés. Les activités eDiscovery sont particulièrement sensibles : un eDiscovery Manager malveillant pourrait rechercher et exporter des données confidentielles sans que personne ne le sache si les logs Purview ne sont pas surveillés.

Domaine 7 — Microsoft Secure Score

Le **Microsoft Secure Score** est un indicateur centralisé qui évalue la posture de sécurité du tenant Microsoft 365 sur une échelle de 0 à 100 %. Il agrège les résultats de centaines de contrôles couvrant l'identité, les données, les appareils et les applications. L'audit du Secure Score est à la fois un point de départ rapide pour identifier les lacunes et un outil de suivi de l'amélioration continue.

```
 # ============================================================
# Audit du Microsoft Secure Score
# ============================================================

$secureScore = Invoke-MgGraphRequest -Method GET -Uri "https://graph.microsoft.com/v1.0/security/s
# ... (extrait — voir documentation officielle)
```

Interprétation du Secure Score

Le Secure Score est un indicateur utile mais imparfait. Voici comment l'interpréter correctement :

Score < 30 % : posture de sécurité critique — les mesures de base (MFA, Conditional Access, blocage legacy auth) ne sont probablement pas en place

Score 30-50 % : posture insuffisante — les bases sont partiellement en place mais des lacunes majeures subsistent

Score 50-70 % : posture correcte — les fondamentaux sont en place, les améliorations portent sur la détection et la réponse avancées

Score 70-85 % : bonne posture — le tenant est bien sécurisé, les gains restants sont marginaux ou coûteux

Score > 85 % : excellente posture — attention, certains points du Secure Score ne sont pas pertinents pour toutes les organisations

Le Secure Score ne couvre pas tout : il ne mesure pas la qualité des processus de réponse aux incidents, la formation des utilisateurs, ou la sécurité des applications métier intégrées à M365. Il doit être complété par un audit manuel approfondi — ce que ce Guide Rouge propose précisément.

Automatisation de l'audit : script PowerShell complet

Cette section fournit un **script d'audit automatisé complet** qui exécute tous les contrôles des 7 domaines et génère un rapport HTML. Ce script peut être utilisé comme base pour un audit

récurrent (mensuel ou trimestriel). Pour aller plus loin dans l'automatisation, consultez notre article sur l'automatisation de l'audit de sécurité Microsoft 365 avec PowerShell et Graph.

```
 # ============================================================
# SCRIPT D'AUDIT AUTOMATISÉ MICROSOFT 365
# Version 2.0 — Guide Rouge Ayi NEDJIMI
# ============================================================
#
# ... (extrait — voir documentation officielle)
```

Checklist complète de l'audit Microsoft 365

Cette checklist recense les **80+ contrôles** de sécurité couverts par ce Guide Rouge. Chaque contrôle est classé par domaine, criticité, et statut d'implémentation. Utilisez ce tableau comme support de suivi lors de vos audits.

#	Domaine	Contrôle	Criticité	Référence
1	Entra ID	Conditional Access Policies actives et couvrant toutes les apps	Critique	CIS 1.1
2	Entra ID	MFA activé pour 100% des utilisateurs	Critique	CIS 1.2
3	Entra ID	Méthodes MFA phishing-resistant (FIDO2/WHfB) pour les admins	Critique	CISA SCuBA
4	Entra ID	Authentification legacy bloquée	Critique	CIS 1.3
5	Entra ID	PIM activé pour Global Admin et rôles critiques	Critique	CIS 1.4
6	Entra ID	Nombre de Global Admins entre 2 et 5	Haute	CIS 1.5
7	Entra ID	Comptes break-glass configurés et testés	Haute	Microsoft Best Practice
8	Entra ID	Consentement utilisateur pour les apps désactivé ou limité	Haute	CIS 2.1
9	Entra ID	Apps enregistrées auditées (secrets, permissions, propriétaires)	Haute	CISA SCuBA
10	Entra ID	Guest access restreint (Restricted Guest User role)	Moyenne	CIS 1.7
11	Entra ID	Invités inactifs (+90j) identifiés et nettoyés	Moyenne	Hygiène
12	Entra ID	Password Protection activée (custom banned passwords)	Moyenne	CIS 1.8
13	Entra ID	Identity Protection configurée (risk policies)	Haute	CIS 1.9
14	Entra ID	Named Locations à jour (IP de confiance, pays bloqués)	Moyenne	CIS 1.10
15	Entra ID	Token lifetime policies configurées	Moyenne	CISA SCuBA
16	Entra ID	Cross-tenant access policies restrictives	Moyenne	Microsoft Best Practice
17	Entra ID	Entra Connect : serveur sécurisé, sync récente	Haute	Hybride
18	Entra ID	Self-Service Password Reset configuré avec méthodes fortes	Moyenne	CIS 1.11
19	Exchange	Unified Audit Log activé	Critique	CIS 3.1
20	Exchange	Transport Rules auditées (pas de redirection externe)	Haute	CIS 3.2
21	Exchange	Inbox Rules suspectes identifiées	Haute	Forensique
22	Exchange	Anti-phishing Policy avec impersonation protection	Haute	CIS 3.3
23	Exchange	SPF en hard fail (-all) pour tous les domaines	Haute	CIS 3.4
24	Exchange	DKIM activé et signé pour tous les domaines	Haute	CIS 3.5
25	Exchange	DMARC en p=reject pour tous les domaines	Haute	CIS 3.6
26	Exchange	Forwarding externe bloqué (AutoForwardingMode=Off)	Critique	CIS 3.7
27	Exchange	Safe Attachments activé (Dynamic Delivery ou Block)	Haute	CIS 3.8

#	Domaine	Contrôle	Criticité	Référence
28	Exchange	Safe Links activé avec scan des URLs	Haute	CIS 3.9
29	Exchange	Safe Attachments pour SharePoint/OneDrive/Teams	Haute	CIS 3.10
30	Exchange	Connecteurs entrants avec TLS requis et restriction IP	Moyenne	Réseau
31	Exchange	Permissions de boîtes mail auditées (Full Access, Send As)	Moyenne	Hygiène
32	Exchange	Quarantaine configurée (admins notifiés)	Basse	Opérationnel
33	SharePoint	Partage externe limité (pas de liens anonymes)	Critique	CIS 4.1
34	SharePoint	Expiration des liens de partage configurée	Haute	CIS 4.2
35	SharePoint	Domaines autorisés/bloqués pour le partage externe	Moyenne	CIS 4.3
36	SharePoint	DLP activé pour SharePoint et OneDrive	Haute	CIS 4.4
37	SharePoint	Sites sensibles avec partage externe désactivé	Haute	Gouvernance
38	SharePoint	Versioning activé (50+ versions)	Moyenne	Anti-ransomware
39	SharePoint	Sync OneDrive restreint aux appareils gérés	Haute	CIS 4.5
40	SharePoint	Applications tierces SharePoint auditées	Moyenne	Hygiène
41	SharePoint	Sensitivity Labels appliqués aux sites	Moyenne	Classification
42	SharePoint	Conditional Access pour accès non géré (browser-only)	Haute	Zero Trust
43	Teams	Guest access configuré et restreint	Haute	CIS 5.1
44	Teams	External access limité aux domaines approuvés	Moyenne	CIS 5.2
45	Teams	Lobby activé pour les utilisateurs anonymes et externes	Haute	CIS 5.3
46	Teams	Applications tierces non vérifiées bloquées	Haute	CIS 5.4
47	Teams	DLP appliqué aux conversations Teams	Haute	CIS 5.5
48	Teams	Recording policies conformes (consentement, stockage)	Moyenne	RGPD
49	Teams	Canaux partagés avec restrictions cross-tenant	Moyenne	Gouvernance
50	Teams	Rétention des messages Teams configurée	Moyenne	Compliance
51	Defender	Defender for Office 365 Plan 2 activé	Haute	Protection
52	Defender	Safe Documents activé	Moyenne	CIS 6.1
53	Defender	Attack Simulation Training utilisé régulièrement	Moyenne	Formation
54	Defender	Defender for Endpoint : taux d'onboarding > 95%	Haute	Protection
55	Defender	Defender for Identity : capteurs sur tous les DC	Haute	Hybride
56	Defender	Defender for Cloud Apps : Shadow IT discovery	Moyenne	Visibilité

#	Domaine	Contrôle	Criticité	Référence
57	Defender	ASR Rules en mode Block pour les règles critiques	Haute	CIS 6.2
58	Defender	Automated Investigation and Response (AIR) activé	Moyenne	Détection
59	Purview	Sensitivity Labels définis et publiés	Haute	CIS 7.1
60	Purview	Auto-labeling configuré pour les types sensibles	Moyenne	Classification
61	Purview	DLP couvrant Exchange, SharePoint, OneDrive, Teams	Haute	CIS 7.2
62	Purview	Types d'informations sensibles RGPD configurés	Haute	RGPD
63	Purview	Rétention conforme aux obligations légales	Haute	Compliance
64	Purview	eDiscovery : accès restreint aux rôles autorisés	Moyenne	Gouvernance
65	Purview	Insider Risk Management configuré	Moyenne	Détection
66	Purview	Communication Compliance activé (si applicable)	Basse	Réglementaire
67	Secure Score	Score global > 60%	Haute	Baseline
68	Secure Score	Quick wins identifiés et implémentés	Moyenne	Amélioration

Structure type du rapport d'audit

Le livrable final d'un audit Microsoft 365 doit être un rapport structuré, actionnable, et adapté à plusieurs audiences (direction, équipe sécurité, équipe IT). Voici la structure recommandée :

Page de garde

Titre : "Rapport d'Audit de Sécurité Microsoft 365"

Client, date, version, classification (Confidentiel)

Auditeur(s), périmètre, méthodologie

Executive Summary (1-2 pages)

Score global : note sur 100 avec code couleur (rouge/orange/vert)

Findings critiques : les 3-5 vulnérabilités les plus graves, en langage non technique

Recommandations prioritaires : les 5 actions à entreprendre immédiatement

Comparaison sectorielle : positionnement par rapport au Secure Score moyen du secteur

Méthodologie et périmètre

Périmètre audité (services M365, nombre d'utilisateurs, nombre de licences)

Période d'audit et durée

Outils utilisés (Maester, ScubaGear, scripts personnalisés)

Référentiels de conformité (CIS Benchmarks, CISA SCuBA, ANSSI)

Limitations et exclusions

Résultats par domaine

Pour chaque domaine (Entra ID, Exchange, SharePoint, Teams, Defender, Purview, Secure Score) :

Score du domaine : nombre de contrôles conformes / total

Tableau des findings : contrôle, sévérité, description, preuve (screenshot/commande), remédiation

Quick wins : améliorations à faible effort avec fort impact

Plan de remédiation

Court terme (0-30 jours) : findings critiques et quick wins

Moyen terme (30-90 jours) : findings élevés, mise en place de PIM, DLP, labels

Long terme (90-180 jours) : findings moyens, optimisation, formation utilisateurs

Annexes techniques

Export complet des Conditional Access Policies

Liste des applications enregistrées avec permissions

Liste des utilisateurs sans MFA

Export des règles de transport et inbox rules suspectes

Rapport ScubaGear/Maester complet

Configuration DNS (SPF/DKIM/DMARC) de chaque domaine

À RETENIR

Conseils pour un rapport d'audit efficace

L'Executive Summary est la seule partie que la direction lira — soignez-la particulièrement avec des métriques concrètes et des risques business (pas techniques)

Chaque finding doit inclure une **preuve** (screenshot, output de commande) — sans preuve, le finding sera contesté

Priorisez les remédiations par **rapport risque/effort** — un contrôle critique mais facile à corriger doit être traité en premier

Incluez une **estimation du coût** de chaque remédiation (licences nécessaires, jours/homme) pour faciliter la prise de décision

Proposez un **audit de suivi** à 6 mois pour vérifier l'implémentation des remédiations

Comment réaliser un audit M365 avec Maester en moins de 2 heures ?

Maester est l'outil le plus rapide pour obtenir un premier état des lieux de la sécurité d'un tenant M365. Il exécute automatiquement plus de 180 tests Pester couvrant les bonnes pratiques Microsoft et les benchmarks CIS. Voici la procédure complète pour réaliser un audit express :

Installez les modules requis : `Install-Module Maester, Pester -Force`

Créez un répertoire de travail et initialisez les tests : `Install-MaesterTests`

Connectez-vous avec un compte Global Reader : `Connect-Maester`

Lancez l'audit complet : `Invoke-Maester -OutputFolder "./Results"`

Analysez le rapport HTML généré dans le dossier de sortie

Le rapport Maester classe chaque test en Pass/Fail avec une description claire et un lien vers la documentation Microsoft. Il est particulièrement utile comme **complément à un audit manuel** : Maester vérifie les configurations, tandis que l'audit manuel (ce Guide Rouge) analyse les risques opérationnels et les comportements utilisateurs.

Quels sont les prérequis de licence pour un audit M365 complet ?

Toutes les fonctionnalités de sécurité M365 ne sont pas disponibles avec toutes les licences. Voici les prérequis par domaine d'audit :

Entra ID P1 : Conditional Access, Self-Service Password Reset, Dynamic Groups

Entra ID P2 : PIM, Identity Protection (risk policies), Access Reviews

Microsoft 365 E3 : Exchange Online Protection (EOP), DLP de base, Sensitivity Labels manuels

Microsoft 365 E5 : Defender for Office 365 P2, Defender for Endpoint P2, Defender for Identity, Defender for Cloud Apps, Purview Insider Risk, eDiscovery Premium, auto-labeling

Add-on Compliance : Purview Compliance Manager, Communication Compliance, Information Barriers

L'audit identifie les gaps de couverture liés aux licences et recommande les upgrades nécessaires avec une analyse coût/bénéfice.

Comment auditer les applications OAuth consenties par les utilisateurs ?

Les applications **OAuth consenties** sont l'un des vecteurs d'attaque les plus insidieux dans M365. Un utilisateur qui consent à une application malveillante lui donne un accès direct et persistant à ses données — et ce, sans que l'attaquant n'ait besoin du mot de passe. Notre article sur les abus OAuth/OIDC et la sécurité des consentements détaille les techniques d'attaque.

```
 # ============================================================
# Audit des consentements OAuth utilisateur
# ============================================================

$oauthGrants = Get-MgOAuth2PermissionGrant -All
# ... (extrait — voir documentation officielle)
```

Comment intégrer l'audit M365 dans un programme Zero Trust ?

L'audit Microsoft 365 s'inscrit naturellement dans une démarche **Zero Trust**. Le modèle Zero Trust repose sur trois principes — vérifier explicitement, utiliser le moindre privilège, présumer la compromission — qui s'appliquent directement aux contrôles de ce Guide Rouge. Pour une implémentation complète, consultez notre article sur l'implémentation Zero Trust dans Microsoft 365.

Les contrôles d'audit s'alignent avec les piliers Zero Trust de la manière suivante :

Identité (Entra ID) : MFA phishing-resistant, Conditional Access, PIM, Identity Protection

Endpoints (Defender for Endpoint, Intune) : Device compliance, ASR rules, onboarding coverage

Données (Purview, SharePoint) : Sensitivity Labels, DLP, classification automatique

Applications (Defender for Cloud Apps) : Shadow IT discovery, app governance, OAuth audit

Réseau (Conditional Access, Named Locations) : Segmentation logique, restrictions géographiques

Visibilité (Unified Audit Log, Defender) : Logging centralisé, détection automatisée, investigation

Comment détecter une compromission M365 en cours ?

L'audit de sécurité est préventif, mais il peut également révéler des compromissions actives. Voici les indicateurs de compromission (IOC) à rechercher dans un tenant M365 :

Inbox Rules suspectes : transfert vers des adresses externes, suppression automatique de messages de sécurité

Applications OAuth inconnues : nouvelles applications consenties avec des scopes sensibles (Mail.Send, Files.ReadWrite.All)

Connexions impossibles : même utilisateur connecté depuis deux pays distants en moins d'une heure (impossible travel)

Connexions depuis des IP anonymes : Tor, VPN anonymes, proxies résidentiels

Création de Transport Rules : nouvelles règles qui redirigent ou copient en BCC vers l'extérieur

Modification des paramètres MFA : désactivation du MFA, ajout d'un nouveau numéro de téléphone ou d'une nouvelle app Authenticator

Création de nouveaux comptes admin : élévation de privilèges non autorisée

Exfiltration massive SharePoint/OneDrive : téléchargement de centaines de fichiers en quelques heures

Quel est le coût d'un audit M365 et comment le budgéter ?

Le coût d'un audit M365 dépend de la taille du tenant, du périmètre, et du niveau de profondeur. Voici les ordres de grandeur :

Audit express (1-2 jours) : exécution de Maester + ScubaGear, revue rapide des findings critiques. Budget : 2 000-5 000 EUR

Audit standard (3-5 jours) : les 7 domaines de ce Guide Rouge, rapport complet avec plan de remédiation. Budget : 8 000-15 000 EUR

Audit approfondi (5-10 jours) : audit standard + investigation des logs (UAL, sign-in), test de phishing, revue des processus. Budget : 15 000-30 000 EUR

Programme d'audit continu (annuel) : audit trimestriel automatisé + audit annuel approfondi + suivi des remédiations. Budget : 30 000-60 000 EUR/an

Le retour sur investissement est clair : le coût moyen d'une compromission BEC est de **125 000 EUR** (FBI IC3 2025), tandis qu'une compromission complète du tenant avec exfiltration de données coûte en moyenne **4.88 millions de dollars** (IBM 2025). Un audit à 15 000 EUR qui prévient une seule compromission offre un ROI de 800 %.

Comment former les équipes IT à l'audit M365 ?

La formation des équipes internes est essentielle pour pérenniser les résultats de l'audit. Les compétences requises incluent :

PowerShell avancé : Microsoft Graph SDK, Exchange Online Management, Teams PowerShell

Entra ID : Conditional Access, PIM, Identity Protection, App Registrations

Sécurité email : SPF/DKIM/DMARC, anti-phishing, Safe Attachments/Links

Gouvernance des données : DLP, Sensitivity Labels, rétention, eDiscovery

Détection et réponse : Unified Audit Log, Defender alerts, investigation d'incidents

Les certifications recommandées sont : **SC-200** (Security Operations Analyst), **SC-300** (Identity and Access Administrator), **SC-400** (Information Protection and Compliance), et **MS-102** (Microsoft 365 Administrator).

Quelles différences entre l'audit M365 et l'audit Google Workspace ?

Bien que les deux plateformes couvrent des fonctionnalités similaires (email, stockage, collaboration), les approches d'audit diffèrent significativement. Notre Guide Complet d'Audit Google Workspace couvre les spécificités de l'écosystème Google. Les principales différences sont :

Identité : Entra ID vs Google Cloud Identity — Entra ID est plus complexe avec PIM, Conditional Access granulaire, et l'hybridation AD

Email : Exchange Online vs Gmail — Exchange a plus de surface d'attaque (Transport Rules, Inbox Rules, protocoles legacy)

Outils d'audit : PowerShell/Graph API vs Apps Script/Admin SDK — l'écosystème Microsoft est plus mature pour l'audit automatisé

Conformité : Purview vs Google Vault — Purview est plus complet pour les organisations européennes (RGPD, NIS2)

Comment auditer Copilot for Microsoft 365 ?

Copilot for Microsoft 365 introduit de nouveaux risques de sécurité : l'IA peut accéder à toutes les données auxquelles l'utilisateur a accès, ce qui signifie que des permissions excessives deviennent encore plus dangereuses. Si un utilisateur a accès à un site SharePoint contenant des données RH sensibles (qu'il ne consulte jamais manuellement), Copilot peut les surfacer dans une réponse à une question anodine. La faille Copilot découverte en 2025 a démontré que l'exfiltration de données via Copilot est un risque réel.

L'audit Copilot doit vérifier :

Les permissions SharePoint/OneDrive — nettoyez les accès excessifs AVANT de déployer Copilot

Les Sensitivity Labels — les documents hautement confidentiels doivent être labelisés et exclus de Copilot si nécessaire

Les politiques DLP — vérifiez que Copilot ne peut pas contourner les restrictions DLP

Les logs d'utilisation — auditez les requêtes Copilot pour détecter les tentatives d'accès à des données sensibles

Quelles sont les erreurs les plus fréquentes lors d'un audit M365 ?

Après avoir réalisé des dizaines d'audits M365 pour des organisations de toutes tailles, voici les erreurs les plus couramment observées :

Compter sur le Secure Score seul : le Secure Score ne détecte pas les compromissions actives, les permissions excessives granulaires, ou les mauvaises pratiques utilisateur

Oublier les applications OAuth : les applications consenties par les utilisateurs sont souvent le plus grand angle mort de la sécurité M365

Ne pas vérifier les Inbox Rules : les règles de transfert au niveau utilisateur ne sont pas visibles dans l'interface admin Exchange sans requête spécifique

Ignorer le DMARC : beaucoup d'organisations ont un SPF correct mais pas de DMARC, ce qui ne protège pas contre le spoofing

PIM non activé : les comptes Global Admin permanents sont la vulnérabilité #1 — PIM est inclus dans Entra ID P2 mais souvent non configuré

Conditional Access en Report-Only : des politiques en mode "test" depuis des mois sans être passées en mode enforcement

Forwarding externe non bloqué : `AutoForwardingMode` n'est pas à "Off" par défaut dans certaines configurations

Safe Attachments désactivé pour SharePoint/OneDrive : la protection des fichiers dans SharePoint et OneDrive n'est pas activée par défaut

Unified Audit Log non activé : sans l'UAL, aucune investigation post-incident n'est possible

Pas de revue des accès invités : des dizaines d'invités inactifs ou avec des invitations en attente depuis des mois

Comment maintenir la conformité M365 après l'audit ?

L'audit n'est qu'un instantané de la posture de sécurité. Pour maintenir la conformité dans le temps, mettez en place :

Audit automatisé hebdomadaire : exécutez Maester en CI/CD et alertez en cas de régression

Revue mensuelle des accès : Access Reviews dans Entra ID pour les groupes sensibles et les accès invités

Revue trimestrielle des applications : nettoyez les applications OAuth, rotez les secrets, supprimez les apps inutilisées

Formation continue : Attack Simulation Training mensuel pour maintenir la vigilance des utilisateurs

Suivi du Secure Score : configurez des alertes en cas de baisse du score

Veille sécurité M365 : suivez les annonces Microsoft (Message Center) et les CVE affectant les services M365

À RETENIR

Programme d'audit continu recommandé

Quotidien : monitoring automatisé des alertes Defender, vérification des sign-in à risque via Identity Protection

Hebdomadaire : exécution de Maester, revue des nouvelles applications OAuth, vérification des Inbox Rules suspectes

> **Mensuel** : revue des accès invités, audit des modifications Conditional Access, vérification des secrets d'application proches de l'expiration
>
> **Trimestriel** : audit complet des 7 domaines (ce Guide Rouge), mise à jour du plan de remédiation, rapport à la direction
>
> **Annuel** : audit approfondi avec test de phishing, revue de l'architecture, benchmark sectoriel, mise à jour des politiques de sécurité

Qu'est-ce que audit microsoft 365 guide et pourquoi est-ce important ?

La réponse dépend du contexte organisationnel, mais les principes fondamentaux restent constants : évaluation du périmètre, identification des actifs critiques et priorisation par risque réel plutôt que par vulnérabilité isolée.

Comment mettre en oeuvre les bonnes pratiques liées à audit microsoft 365 guide ?

Une approche structurée et documentée est clé. Les outils et méthodologies évoluent rapidement — rester informé des ressources ANSSI, NIST et MITRE ATT&CK est indispensable pour adapter les recommandations génériques à chaque contexte.

Quelles ressources pour approfondir audit microsoft 365 guide ?

Les ressources officielles (ANSSI, CISA, CERT-FR) constituent le point de départ. Complétées par des retours d'expérience terrain, elles permettent d'adapter les recommandations aux réalités opérationnelles de chaque organisation.

Sources et références

[Microsoft Learn — Microsoft 365 Security]

CIS Benchmark — Microsoft 365

ANSSI — Guide de sécurisation Microsoft 365

Vous souhaitez en savoir plus ou évaluer votre exposition ?

Contacter nos experts ou contactez-nous directement.

FAQ — Questions fréquentes sur l'audit Microsoft 365

Quelle est la fréquence recommandée pour un audit M365 ?

La fréquence dépend de la taille de l'organisation et de son exposition aux risques. En règle générale, un **audit complet trimestriel** est recommandé, complété par un monitoring automatisé hebdomadaire (via Maester ou des scripts personnalisés). Les organisations soumises à des réglementations spécifiques (NIS2, DORA, PCI DSS) doivent respecter les fréquences imposées par leur cadre réglementaire — souvent annuel au minimum. L'événement déclencheur le plus important est le **changement** : toute modification majeure de la configuration M365 (nouvelle politique Conditional Access, activation de Copilot, migration vers E5) devrait déclencher un audit ciblé du domaine concerné.

Peut-on réaliser un audit M365 sans accès Global Admin ?

Oui, et c'est même recommandé. Le rôle **Global Reader** suffit pour la grande majorité des contrôles d'audit. Ce rôle donne un accès en lecture à toutes les configurations Entra ID, Exchange, SharePoint et Teams sans possibilité de modification. Pour les audits Purview et eDiscovery, les rôles **Security Reader** et **Compliance Reader** sont nécessaires en complément. L'utilisation d'un compte Global Admin pour l'audit introduit un risque inutile : si les credentials d'audit sont compromises, l'attaquant n'obtient qu'un accès en lecture. La seule exception est l'audit des paramètres PIM, qui nécessite le rôle **Privileged Role Administrator** en lecture.

Combien de temps faut-il pour remédier aux findings d'un audit M365 ?

Le temps de remédiation varie considérablement selon la maturité de l'organisation. Les **quick wins** (activation du MFA, blocage de l'authentification legacy, désactivation du forwarding externe) peuvent être implémentés en **quelques heures**. Les mesures intermédiaires (déploiement de Conditional Access, configuration de PIM, mise en place de DLP) nécessitent typiquement **2 à 4 semaines** de planification et d'implémentation. Les mesures structurelles (déploiement de Sensitivity Labels avec formation utilisateurs, mise en place d'un SOC, intégration SIEM) peuvent prendre **3 à 6 mois**. Un plan de remédiation réaliste prévoit trois vagues : immédiat (0-30 jours), moyen terme (30-90 jours), et long terme (90-180 jours).

L'audit M365 est-il pertinent pour les petites organisations (moins de 50 utilisateurs) ?

Absolument. Les petites organisations sont souvent **plus vulnérables** car elles n'ont pas d'équipe sécurité dédiée et leurs tenants M365 sont configurés avec les paramètres par défaut — qui sont rarement optimaux pour la sécurité. Un audit express utilisant **Maester** et **ScubaGear** peut être réalisé en moins de 2 heures et identifie les lacunes les plus critiques. Pour les petites organisations, les priorités sont claires : activer les **Security Defaults** (gratuit), configurer le **MFA pour tous les utilisateurs**, bloquer le **forwarding externe**, et activer le **Unified Audit Log**. Ces quatre mesures couvrent 80 % des risques pour un effort minimal.

Comment l'audit M365 s'articule-t-il avec les certifications ISO 27001 et SOC 2 ?

L'audit M365 couvre un sous-ensemble des contrôles ISO 27001 et SOC 2 — principalement les domaines de gestion des accès (A.9), de sécurité des communications (A.13), de sécurité des opérations (A.12), et de conformité (A.18). Les findings d'un audit M365 peuvent être directement mappés aux contrôles ISO 27001 dans le rapport de certification. Pour SOC 2, les critères de sécurité (CC6 — Logical and Physical Access), de disponibilité, et de confidentialité sont les plus pertinents. L'avantage d'un audit M365 structuré est qu'il fournit des **preuves documentées** (exports PowerShell, rapports Maester, screenshots) directement réutilisables pour les audits de certification.

Quels sont les risques juridiques d'un audit M365 mal conduit ?

Un audit M365 manipule des données sensibles : logs de connexion (données personnelles RGPD), contenu de boîtes mail (correspondance privée), informations de sécurité (mots de passe, tokens). Les risques juridiques incluent : violation du RGPD si les données d'audit ne sont pas protégées, violation du secret des correspondances si le contenu des emails est lu sans base légale, et responsabilité en cas de compromission des credentials d'audit. Pour se protéger : obtenez une **lettre de mission signée** définissant le périmètre, utilisez des **comptes dédiés en lecture seule**, chiffrez tous les exports, et **supprimez les données d'audit** à la fin de la mission (conservez uniquement le rapport final).

Comment mesurer le retour sur investissement (ROI) d'un audit M365 ?

Le ROI d'un audit M365 se mesure en **risques évités** plutôt qu'en gains directs. Les métriques pertinentes incluent : le nombre de findings critiques corrigés (chacun représentant un vecteur d'attaque éliminé), l'amélioration du Secure Score (mesurable et comparable dans le temps), la réduction du temps de détection des incidents (Mean Time to Detect — MTTD), et la conformité réglementaire obtenue (évitement de sanctions). En termes financiers, le coût moyen d'une compromission BEC est de 125 000 EUR et d'une exfiltration de données M365 de 4.88 millions de dollars. Un audit à 15 000 EUR qui identifie et corrige une vulnérabilité critique (MFA manquant sur les Global Admins, forwarding externe non bloqué) a un ROI immédiat et considérable.

Peut-on automatiser entièrement l'audit M365 ?

On peut automatiser environ **70 % des contrôles techniques** (vérification des configurations, compliance checks, inventaires) avec des outils comme Maester, ScubaGear, et les scripts PowerShell de ce Guide Rouge. Les **30 % restants** nécessitent un jugement humain : évaluation de la pertinence des exceptions Conditional Access, analyse de la légitimité des applications OAuth, revue des processus de réponse aux incidents, et évaluation de la formation des utilisateurs. L'approche recommandée est un modèle hybride : automatisation des contrôles techniques (exécution hebdomadaire avec alerting), complétée par un audit expert humain trimestriel ou annuel pour les aspects nécessitant du jugement.

Comment gérer les findings que l'organisation refuse de corriger ?

Dans tout audit, certains findings seront contestés ou reportés pour des raisons opérationnelles (impact utilisateurs trop important, coût de la licence nécessaire, dépendance technique). La procédure recommandée est la suivante : documentez le finding avec sa preuve technique, présentez le risque en termes business (pas techniques), proposez des **mesures compensatoires** si la correction directe n'est pas possible, et faites signer une **acceptation de risque formelle** par un responsable de niveau approprié (RSSI ou Direction). Un finding critique refusé sans acceptation de risque signée est une bombe à retardement : en cas d'incident, l'absence de remédiation et l'absence d'acceptation de risque engagent la responsabilité de l'organisation.

Quelles sont les nouveautés M365 à surveiller pour les audits en 2026-2027 ?

Plusieurs évolutions Microsoft 365 vont impacter significativement les audits de sécurité dans les 12 prochains mois. **Copilot for Microsoft 365** nécessite un audit des permissions avant déploiement (Copilot accède à toutes les données accessibles à l'utilisateur). **Microsoft Entra Verified ID** introduit des attestations d'identité décentralisées qui compliquent le modèle d'authentification. Le **Microsoft Security Exposure Management** remplace progressivement le Secure Score avec une vue plus granulaire de la surface d'attaque. **Continuous Access Evaluation (CAE) v2** avec token binding renforce la protection contre le vol de tokens. Enfin, l'intégration croissante de l'**IA dans Defender** (Security Copilot) modifie les processus de détection et de réponse — l'audit devra vérifier que les recommandations de l'IA sont revues par un humain avant exécution.

Questions fréquentes

Conclusion

L'audit de sécurité Microsoft 365 n'est pas un exercice ponctuel — c'est un **processus continu** qui doit être intégré dans la gouvernance de sécurité de l'organisation. Ce Guide Rouge vous a fourni la méthodologie, les outils, et les scripts pour mener un audit complet et actionnable couvrant les 7 domaines critiques de M365 : Entra ID, Exchange Online, SharePoint/OneDrive, Teams, Microsoft Defender, Purview, et le Secure Score.

Les menaces ciblant Microsoft 365 évoluent rapidement : les attaques AiTM contournent le MFA, le consent phishing exploite la confiance des utilisateurs, et les techniques de persistence via les Service Principals et les App Registrations deviennent de plus en plus sophistiquées. Seul un audit régulier et systématique, combinant des outils automatisés (Maester, ScubaGear) et une analyse experte manuelle, permet de maintenir une posture de sécurité robuste.

Les **80+ contrôles** documentés dans ce guide, accompagnés de leurs **scripts PowerShell complets** et de leur **checklist de suivi**, constituent un kit d'audit opérationnel prêt à l'emploi. Que vous réalisiez votre premier audit M365 ou que vous cherchiez à industrialiser votre processus d'audit, ce Guide Rouge est votre référence.

Pour aller plus loin dans la sécurisation de votre environnement Microsoft, consultez nos guides complémentaires : le Livre Blanc Sécurité Microsoft 365 pour une vue d'ensemble stratégique, le guide de sécurisation Entra ID avec Conditional Access pour une implémentation détaillée des politiques d'accès conditionnel, et notre article sur l'automatisation de l'audit avec PowerShell et Graph API pour industrialiser le processus. La sécurité de votre tenant Microsoft 365 est un investissement — chaque contrôle implémenté réduit votre surface d'attaque et augmente le coût pour l'attaquant.

© Ayi NEDJIMI Consultants — Tous droits réservés