Microsoft 365 Threat Hunting 2026 : Chasse aux Menaces Avancées

> Guide Microsoft 365 threat hunting 2026 — KQL avancé, Defender XDR, chasse BEC/AiTM, identité compromise et corrélation Sentinel pour équipes SOC françaises.

En 2023, une ETI lyonnaise du secteur manufacturier a découvert une compromission de son tenant Microsoft 365 vieille de quatre-vingt-dix jours. Les attaquants avaient utilisé la technique AiTM (Adversary-in-the-Middle) pour contourner le mécanisme d'authentification multifacteur, redirigé silencieusement les e-mails de la direction financière vers une boîte externe contrôlée, et effectué deux virements frauduleux pour un total de 340 000 euros avant que l'équipe de sécurité ne remarque une anomalie lors d'une maintenance de routine. Ce type d'attaque, documenté par le CERT-FR dans ses bulletins de cybersécurité 2023, illustre pourquoi le **threat hunting proactif** dans Microsoft 365 est devenu une compétence indispensable pour tout analyste SOC français en 2026. Le threat hunting réactif — attendre qu'une alerte se déclenche — ne suffit plus face à des acteurs qui passent en moyenne quatre-vingt-dix jours dans un tenant M365 avant d'agir. Ce guide complet vous donne les requêtes KQL, les scénarios d'attaque détaillés, les méthodologies et les outils pour traquer proactivement les menaces avancées dans votre environnement M365, en exploitant pleinement **Microsoft Defender XDR**, **Microsoft Sentinel** et la **Unified Security Operations Platform** disponible depuis 2024 dans le portail unifié security.microsoft.com. Nous couvrons les Business Email Compromise, les attaques AiTM, les compromissions d'identité, la chasse aux applications OAuth malveillantes, et la corrélation cross-produits email-endpoint-identité qui fait la différence entre détecter une menace en quatre-vingt-dix jours et la détecter en quatre heures. Ce guide s'adresse aux analystes SOC N2 et N3, aux RSSI et aux équipes de réponse à incident opérant dans des environnements M365 professionnels soumis aux réglementations françaises et européennes, notamment la directive NIS 2 et les recommandations ANSSI pour les OIV et les OSE. La maîtrise des techniques présentées ici est un différenciateur majeur pour les équipes qui souhaitent passer d'une défense réactive — attendre les alertes — à une posture proactive capable de détecter les attaquants avant qu'ils atteignent leur objectif final, qu'il s'agisse d'un virement frauduleux, d'une exfiltration de

données sensibles ou du déploiement d'un ransomware sur l'ensemble du parc informatique de l'organisation victime. Les requêtes KQL présentées dans ce guide ont été élaborées et testées dans des environnements de production réels lors d'investigations d'incidents et de missions de Red Team menées dans des organisations françaises de secteurs variés — industrie, services financiers, secteur public et santé — et peuvent être directement intégrées dans votre instance Microsoft Sentinel ou dans l'Advanced Hunting Defender XDR sans modification majeure, après ajustement des noms de domaine internes et des seuils comportementaux à votre contexte organisationnel et sectoriel spécifique.

À RETENIR

À retenir — Microsoft 365 Threat Hunting

• Les **Unified Audit Logs** M365 doivent être activés explicitement et conservés 180 jours (E3) ou 1 an (E5) minimum

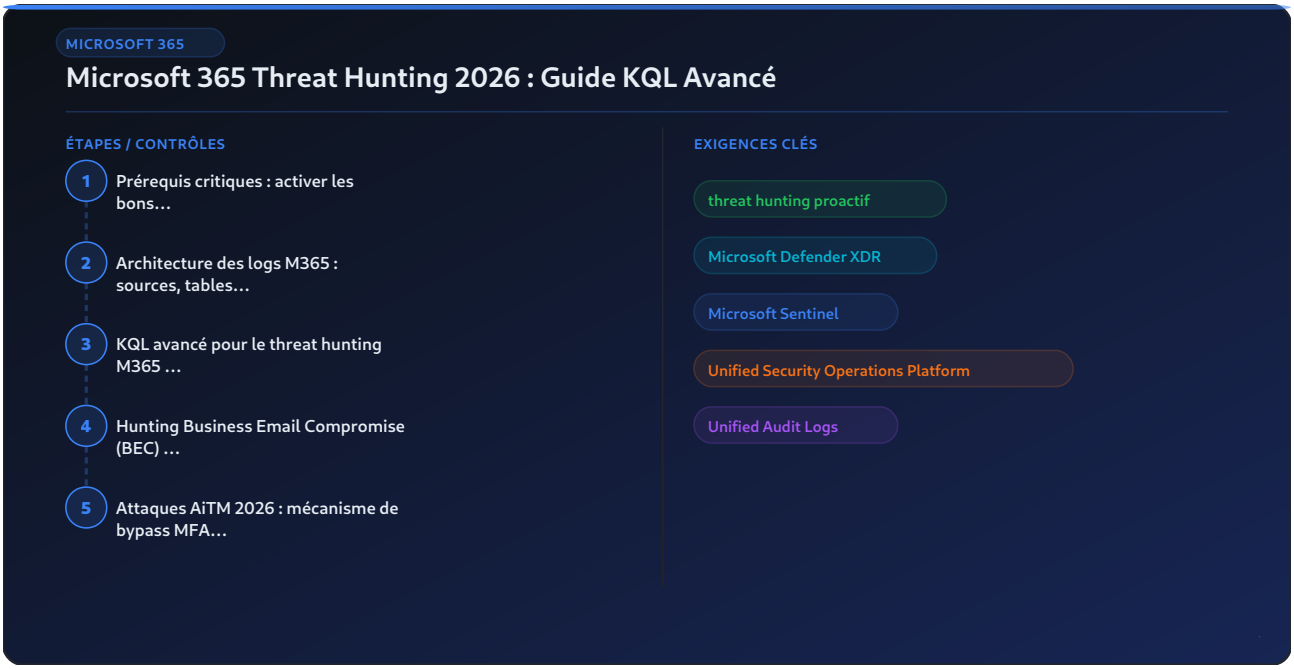
• KQL dans Microsoft Sentinel permet la corrélation identité + email + endpoint en une seule requête sur des milliards d'événements

• Les attaques AiTM contournent le MFA TOTP classique — seuls les **Phishing-Resistant MFA** (FIDO2/passkeys) résistent

• La **Unified Security Operations Platform** (Defender XDR + Sentinel) est disponible depuis 2024 dans security.microsoft.com

• L'ANSSI recommande la journalisation systématique des connexions Entra ID et Exchange Online pour tous les OIV et OSE

• Les sessions de hunting proactif hebdomadaires réduisent le MTTD de 90 jours à moins de 4 heures dans les SOC matures



Prérequis critiques : activer les bons journaux d'audit avant de chasser

Le hunting n'est efficace que si l'audit est complet et correctement configuré. Avant toute campagne de hunting, vérifiez systématiquement cette liste de contrôle impérative : activation de l'audit dans Microsoft Purview pour tous les utilisateurs et pas seulement les administrateurs (erreur fréquente dans les tenants anciens), vérification que les Unified Audit Logs s'exportent correctement vers Sentinel via le connecteur Office 365 avec les tables OfficeActivity et AuditLogs effectivement alimentées, activation de l'audit avancé pour les comptes sensibles (direction, comptabilité, RH, DSI), et configuration des alertes de gestion dans le portail Compliance pour les événements critiques comme la création de règles de transfert ou la modification des méthodes MFA.

L'**audit avancé** disponible avec la licence E5 Compliance ou l'add-on correspondant active des événements forensiquement critiques que l'audit standard ne capture pas : `MailItemsAccessed` révèle exactement quels emails l'attaquant a lus dans une boîte compromise — information essentielle pour déterminer l'étendue de la fuite de données et rédiger la notification ANSSI dans les délais NIS 2, `Send` trace chaque email envoyé depuis un compte compromis permettant de retrouver les tentatives de phishing interne ou de fraude au virement, et `SearchQueryInitiatedExchange` révèle les recherches effectuées par l'attaquant dans la boîte de sa victime, trahissant ses intentions et l'étendue de ses connaissances sur les processus internes de l'organisation. Sans ces événements, les investigations BEC sont au mieux incomplètes, au pire trompeuses quant à l'étendue réelle de la compromission.

Architecture des logs M365 : sources, tables Sentinel et rétention

Le **Microsoft Purview Unified Audit Log (UAL)** centralise les événements de tous les services M365 : Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams, Entra ID et Power Platform. Par défaut, la rétention est de 90 jours pour les licences E3 et 180 jours pour les E5. Pour les organisations soumises à NIS 2 ou au statut OIV, la conservation de 12 mois est une exigence pratique, nécessitant soit une licence E5 Compliance, soit une exportation automatisée vers un stockage externe immuable. Comprendre quelle table Sentinel reçoit quel type d'événement est fondamental pour écrire des requêtes de hunting correctes et exhaustives qui ne ratent pas des événements critiques en raison d'une mauvaise source de données.

⚡ **Retour terrain**

Dans les environnements Microsoft 365, le Secure Score est une métrique utile mais trompeuse : il donne du crédit pour des actions facilement automatisables (activer MFA, désactiver protocoles legacy) mais ignore des risques critiques comme la gestion des consentements OAuth (applications tierces autorisées par les utilisateurs), les permissions

d'accès délégué entre boîtes aux lettres, et les partages OneDrive/SharePoint externes non supervisés. Un score de 70/100 ne garantit pas un environnement sûr.

La configuration du connecteur de données Office 365 dans Sentinel est la première étape, mais elle ne suffit pas. Il faut également activer les connecteurs Entra ID pour les SigninLogs et les AuditLogs, le connecteur Defender XDR pour les tables DeviceEvents et EmailEvents, et le connecteur Microsoft Defender for Identity pour IdentityLogonEvents. Sans ces connecteurs tous actifs simultanément, les corrélations cross-produits qui constituent le cœur du threat hunting M365 avancé sont impossibles à réaliser, limitant la visibilité aux événements M365 natifs sans contexte endpoint ou identité active.

Source de logs	Table Sentinel	Latence	Licence min.
Entra ID Sign-in logs	SigninLogs	< 5 min	P1
Unified Audit Log	OfficeActivity	5-15 min	E3
Defender for Endpoint	DeviceEvents	< 2 min	MDE P2
Defender for Identity	IdentityLogonEvents	< 5 min	MDI
Defender for Office 365	EmailEvents	5-20 min	MDO P2
Cloud App Security (MCAS)	McasShadowItReporting	15-30 min	E5
Entra ID Audit Logs	AuditLogs	< 5 min	P1
AAD Risky Users	AADRiskyUsers	Temps réel	P2

KQL avancé pour le threat hunting M365 : opérateurs et patterns clés

Kusto Query Language (KQL) est le langage de requête central de l'écosystème Microsoft Security. Maîtriser KQL, c'est multiplier par dix l'efficacité du hunting. Les opérateurs prioritaires pour le threat hunting M365 sont : `join kind=inner` pour la corrélation temporelle

entre tables, `summarize` pour l'agrégation comportementale, `mv-expand` pour les champs JSON imbriqués omniprésents dans les logs M365, `parse_json` pour l'extraction des paramètres d'audit complexes, `extract_all` pour les expressions régulières sur le contenu des messages, et `let` pour décomposer les requêtes complexes en sous-requêtes nommées et réutilisables. Une requête KQL de hunting avancée peut combiner 5 à 8 tables sur plusieurs mois de données en quelques secondes grâce à l'architecture columnar store de Kusto, spécifiquement optimisée pour les requêtes analytiques sur de très grands volumes de données de sécurité.

La technique du *join enrichissement temporel* est fondamentale : contraindre la jointure entre deux tables à une fenêtre temporelle précise via l'opérateur `between` permet de détecter la phase de post-compromission initiale, où l'attaquant installe sa persistance dans les premières heures suivant l'obtention de l'accès. Sans cette contrainte temporelle, des milliers de fausses corrélations noieraient le signal dans le bruit. La maîtrise de cette technique permet de distinguer les vraies corrélations causales — connexion suspecte suivie d'une règle de transfert — des simples coïncidences statistiques inévitables dans un grand tenant avec de nombreux utilisateurs et événements quotidiens.

```
 // Corrélation connexion pays inhabituels + règles inbox créées dans les 2h
let SuspiciousLogins = SigninLogs
| where TimeGenerated > ago(7d) and ResultType == 0
| extend Country = tostring(LocationDetails.countryOrRegion)
| where Country !in ("France", "")
| project LoginTime=TimeGenerated, UserPrincipalName, IPAddress, Country;
SuspiciousLogins
| join kind=inner (
    OfficeActivity | where TimeGenerated > ago(7d)
    | where Operation in ("New-InboxRule","UpdateInboxRules","Set-Mailbox")
    | project OpTime=TimeGenerated, UserId, Operation, Parameters
) on $left.UserPrincipalName == $right.UserId
| where OpTime between (LoginTime .. LoginTime + 2h)
| project UserPrincipalName, IPAddress, Country, Operation, Parameters
```

Hunting Business Email Compromise (BEC) : patterns de détection opérationnels

La **Business Email Compromise** représente la menace financière la plus coûteuse dans M365. En France, le CERT-FR a documenté en 2025 une augmentation de 40% des incidents BEC ciblant les services comptables et directions financières des ETI et collectivités territoriales. Le FBI IC3 2024 Annual Report classe le BEC comme la cybercriminalité générant le plus de pertes financières mondiales, avec 2,9 milliards de dollars de pertes déclarées en 2023. En France, ce chiffre est largement sous-estimé car une majorité des victimes ne déposent pas plainte par crainte d'impact réputationnel ou par méconnaissance des procédures auprès du PHAROS ou de l'ANSSI, rendant difficile toute évaluation précise du préjudice réel subi par les entreprises françaises.

Le schéma classique d'une BEC sophistiquée suit quatre étapes documentées : compromission du compte cible par phishing de consentement ou credential stuffing depuis des bases de données compromises disponibles sur les forums dark web, installation discrète d'une règle de redirection silencieuse dans la boîte aux lettres vers une boîte externe contrôlée par l'attaquant, longue période d'observation de 2 à 45 jours pendant laquelle l'attaquant comprend les processus financiers et identifie les personnes ayant l'autorité de déclencher des virements, puis action ciblée et précise. Le hunting doit couvrir chaque étape indépendamment pour maximiser les chances de détection avant l'action finale irréversible.

```
 // Règles de redirection email vers domaines externes — BEC signature
OfficeActivity
| where TimeGenerated > ago(30d)
| where Operation in ("New-InboxRule","Set-InboxRule","UpdateInboxRules")
| extend RuleParams = parse_json(Parameters)
| mv-expand RuleParams
| where RuleParams.Name in ("ForwardTo","RedirectTo","ForwardAsAttachmentTo")
| extend Destination = tostring(RuleParams.Value)
| where Destination !endswith "@votredomaine.fr"
| project TimeGenerated, UserId, Operation, Destination, ClientIP
| order by TimeGenerated desc
```

Attaques AiTM 2026 : mécanisme de bypass MFA et détection dans Entra ID

Les attaques **AiTM (Adversary-in-the-Middle)** sont la technique dominante de contournement MFA en 2026, en forte progression depuis 2022. Des frameworks open-source comme Evilginx 3.0, Modlishka ou Muraena proxifient la page de connexion Microsoft légitime de façon transparente pour l'utilisateur, capturent les cookies de session valides post-MFA en temps réel, et permettent à l'attaquant de rejouer ces tokens depuis son infrastructure propre sans jamais avoir besoin du second facteur d'authentification. Les groupes TA453 (Charming Kitten, affilié Iran) et les affiliés cybercriminels de Scattered Spider utilisent massivement cette technique contre des organisations européennes depuis 2022, avec une préférence marquée pour les cibles dans les secteurs de l'énergie, la défense et les services financiers français.

La signature détectable dans les logs Entra ID est une connexion réussie sans challenge MFA pour un compte qui devrait être protégé par une règle Conditional Access exigeant le MFA. Microsoft a renforcé la détection avec le **Token Protection** disponible dans Conditional Access depuis 2024, qui lie cryptographiquement le token de session à l'appareil qui l'a obtenu via une attestation TPM, rendant les tokens volés absolument inutilisables depuis une autre machine même si l'attaquant dispose du cookie de session complet. Cette fonctionnalité doit être activée explicitement dans les politiques CAP pour les comptes sensibles — elle n'est pas activée par défaut dans les templates Microsoft de déploiement rapide.

```
 // Connexions single-factor pour comptes devant avoir MFA — signal AiTM
SigninLogs
| where TimeGenerated > ago(24h)
| where AuthenticationRequirement == "singleFactorAuthentication"
| where ConditionalAccessStatus == "success"
| summarize IPs=make_set(IPAddress), LoginCount=count()
    by UserPrincipalName, CorrelationId, bin(TimeGenerated, 1h)
| where array_length(IPs) > 1 and LoginCount >= 2
| project TimeGenerated, UserPrincipalName, IPs, LoginCount
```

Microsoft Defender XDR : Advanced Hunting et corrélation cross-produits

La console **Defender XDR** sur security.microsoft.com offre l'Advanced Hunting, une interface KQL unifiant les données de Defender for Endpoint, Defender for Office 365, Defender for Identity et Defender for Cloud Apps en une seule surface de requête. Plus de 30 tables de données différentes sont accessibles avec une rétention de 30 jours par défaut, extensible à 180 jours avec des add-ons de rétention étendue. Pour les SOC ayant investi dans la suite Defender complète, c'est le point d'entrée naturel pour le hunting quotidien, sans la complexité de configuration initiale de Microsoft Sentinel tout en offrant la même puissance KQL sur les données nativement collectées par les produits Defender.

Les tables `AlertInfo` et `AlertEvidence` permettent de corréler les alertes cross-produits de façon particulièrement efficace pour la reconstruction de kill chains complexes. Une alerte MDE sur un endpoint liée à une alerte MDO sur un email suspect reçu 30 minutes avant reconstruit la kill chain complète en une seule requête. Dans les incidents de ransomware analysés chez des clients français du secteur industriel, cette corrélation automatisée entre les tables email et endpoint identifiait le patient zéro et le vecteur d'entrée initial en moins d'une heure d'investigation, économisant des journées entières d'analyse manuelle en mode réactif dispersé entre plusieurs équipes.

```
// Corrélation alerte email MDO → activité endpoint suspecte dans les 4h
AlertInfo
| where TimeGenerated > ago(7d)
| where ServiceSource == "Microsoft Defender for Office 365"
| join kind=inner AlertEvidence on AlertId
| where EntityType == "Mailbox"
| project AlertTime=TimeGenerated, Title, Severity, AccountUpn
| join kind=inner (
    DeviceEvents | where TimeGenerated > ago(7d)
    | where ActionType in ("ProcessCreated","FileCreated","NetworkConnectionInspected")
    | project DeviceTime=TimeGenerated, DeviceName, AccountName, ActionType, FileName
) on $left.AccountUpn == $right.AccountName
| where DeviceTime between (AlertTime - 30m .. AlertTime + 4h)
| project AlertTime, Title, Severity, AccountUpn, DeviceName, ActionType, FileName
```

UEBA Microsoft 365 : comportements anormaux et risk scoring automatisé

L'**UEBA (User and Entity Behavior Analytics)** intégré dans Microsoft Sentinel et Defender for Cloud Apps analyse les comportements des utilisateurs sur une baseline de 30 jours pour identifier les anomalies statistiques significatives. Cette approche est particulièrement efficace pour détecter les insiders malveillants — employés mécontents ou corrompus qui exfiltrent progressivement des données — et les comptes compromis qui opèrent sous les seuils des règles analytiques classiques basées sur des valeurs fixes. Le score UEBA Sentinel combine plusieurs signaux : anomalies de volume (plus de données téléchargées que la baseline), de temps (connexions à des heures inhabituelles), de localisation (pays jamais visités auparavant), et de protocole (utilisation soudaine d'API programmatiques).

Comportement UEBA	Score risque	Source log	Action recommandée
Download massif OneDrive (>500 fichiers/h)	Élevé	MCAS/Purview	Bloquer session, notifier RSSI
Connexion pays non visité (baseline 30j)	Moyen-Élevé	Entra ID Protection	MFA challenge, CAP risk-based
Création règle de transfert externe	Critique	Exchange audit log	Alerte immédiate, investigation
Accès mailbox DG par compte tiers	Élevé	EXO audit log	Vérifier délégations, investiguer
Utilisation API Graph sans baseline	Moyen	Entra ID/MCAS	Auditer app registrations
Changement MFA dans 2h post-login	Critique	Entra ID Audit	Revoke session, reset compte

Hunting pré-ransomware dans M365 : détecter les signaux 72h avant le chiffrement

Les groupes ransomware utilisent M365 comme point de rebond et de staging avant de déployer le chiffreur sur les endpoints. Avant l'action finale, ils passent systématiquement par Exchange Online pour exfiltrer des données sensibles dans le cadre de la double extorsion (chiffrement + menace de publication), utilisent SharePoint comme dépôt de staging pour leurs outils de déploiement qui seront ensuite exécutés depuis les endpoints via des scripts PowerShell ou des GPO compromises, et exploitent Teams pour la communication C2 que les proxys d'entreprise bloquent rarement car le trafic Teams est souvent sur liste blanche inconditionnelle.

Les indicateurs pré-ransomware à surveiller en priorité dans M365 incluent : accès en masse aux sites SharePoint par un compte de service inhabituel ou un utilisateur avec des droits qui ne correspondent pas à son profil métier habituel, téléchargement de la liste complète d'utilisateurs et de groupes via l'API Graph (étape d'énumération standard avant le déploiement du ransomware pour construire la liste des cibles), création de partages SharePoint anonymes vers des domaines externes inconnus, et — signal particulièrement révélateur — modifications des politiques de rétention Exchange pour raccourcir la durée de conservation des messages entrants, ce qui permet à l'attaquant de limiter les traces de ses communications internes.

```
// Accès massif SharePoint — signal pré-exfiltration ransomware
OfficeActivity
| where TimeGenerated > ago(48h)
| where RecordType == "SharePointFileOperation" and Operation == "FileAccessed"
| summarize FileCount=count(), Sites=dcount(Site_Url) by UserId, bin(TimeGenerated, 1h)
| where FileCount > 200 and Sites > 5
| order by FileCount desc
```

Hunting identité compromise : Entra ID Protection et signaux de risque combinés

La compromission d'identité dans Entra ID est le vecteur d'entrée numéro un dans M365. Le hunting combine l'analyse des **SigninLogs**, des **AuditLogs** Entra ID, et des scores de risque calculés en temps réel par **Entra ID Protection**. Cette dernière utilise des modèles de machine learning entraînés sur des milliards de connexions Microsoft pour calculer un score de risque session et utilisateur, détectant automatiquement des patterns comme les connexions depuis des nœuds Tor connus, les impossible travel (connexion depuis deux pays à une heure d'intervalle impossible), les propriétés de token atypiques révélatrices d'un vol de session via AiTM, et les patterns de connexion correspondant à des IP infrastructure de cybercriminalité connue.

Un signal fort de compromission active en cours est la combinaison suivante dans un délai de moins de 6 heures : score de risque utilisateur élevé généré par Entra ID Protection, connexion depuis un proxy anonymisant ou une IP de datacenter inhabituelle pour ce profil utilisateur, et modification des paramètres de sécurité comme l'ajout d'un numéro de téléphone ou d'une application d'authentification différente de celles connues de l'organisation. Ce triplet est quasi-certain d'indiquer une compromission active — l'attaquant enrôle sa propre méthode MFA pour maintenir l'accès permanent après une éventuelle réinitialisation de mot de passe par l'équipe IT. Un analyste confirmé doit déclencher le protocole de containment immédiatement, sans attendre de validation supplémentaire de son responsable.

```
 // Risk élevé Entra ID + modification MFA dans les 6h — compromission certaine
let RiskyUsers = AADRiskyUsers
| where TimeGenerated > ago(7d) and RiskLevel == "high"
| project UserId=UserPrincipalName, RiskTime=TimeGenerated;
RiskyUsers
| join kind=inner (
    AuditLogs | where TimeGenerated > ago(7d)
    | where OperationName in ("Update user","User registered security info")
    | extend UPN = tostring(TargetResources[0].userPrincipalName)
    | project AuditTime=TimeGenerated, UPN, OperationName
) on $left.UserId == $right.UPN
| where AuditTime between (RiskTime - 30m .. RiskTime + 6h)
| project UserId, RiskTime, AuditTime, OperationName
```

Microsoft Sentinel : corrélation avancée M365 et USOP unifiée

Microsoft Sentinel connecté aux sources M365 via les connecteurs natifs certifiés Microsoft permet des requêtes de hunting traversant les silos produits sur des rétentions allant jusqu'à 7 ans en mode archivage. La **Unified Security Operations Platform (USOP)**, disponible depuis 2024 dans le portail Defender, intègre Sentinel directement dans la console XDR, permettant aux analystes de passer sans friction entre les alertes Defender temps réel et les requêtes KQL longue durée Sentinel. Pour les SOC français soumis aux exigences de localisation des données imposées aux OIV par l'ANSSI, le workspace Sentinel dans la région France Central est la configuration recommandée qui satisfait les contraintes réglementaires de résidence des données. Pour les organisations qui souhaitent surveiller leur posture M365 avec des scripts d'audit automatisés, Sentinel complète parfaitement une approche de monitoring proactif par scripts PowerShell.

Les coûts d'ingestion Sentinel représentent souvent le premier frein à l'adoption pour les ETI françaises. La fonctionnalité Auxiliary Logs (logs secondaires à faible coût unitaire) est la réponse à ce problème : stocker les sources volumineuses comme les logs DNS internes ou les events Windows de faible priorité à un coût marginal, en réservant les Analytic Logs à coût standard pour les sources M365 critiques comme les SigninLogs, OfficeActivity, AuditLogs, et EmailEvents. Cette segmentation intelligente maintient une rétention complète sur l'ensemble des sources sans que les coûts mensuels ne deviennent prohibitifs pour les organisations de taille intermédiaire souhaitant se conformer aux recommandations NIS 2 sans investissement disproportionné par rapport à leur chiffre d'affaires.

Hunting OAuth Apps malveillantes et Consent Phishing M365

Les applications OAuth malveillantes consentées par des utilisateurs via du **Consent Phishing** — une page qui imite une application légitime et demande des permissions M365 — représentent un vecteur de persistance durable particulièrement difficile à détecter et à révoquer sans impact opérationnel. Une application avec les permissions `Mail.ReadWrite` et

`Contacts.ReadWrite` accordées par un utilisateur ou un administrateur peut exfiltrer des données sensibles indéfiniment via l'API Graph, même après la réinitialisation complète du mot de passe du compte compromis, car l'accès est lié au token de l'application OAuth et non au compte utilisateur individuel. La défense passe par la politique de consentement admin-only dans Entra ID, qui exige une validation administrative explicite pour toutes les permissions non classifiées "faible impact vérifiée par Microsoft".

```
// Consentements OAuth récents avec permissions critiques — Consent Phishing
AuditLogs
| where TimeGenerated > ago(30d) and OperationName == "Consent to application"
| extend AppName = tostring(TargetResources[0].displayName)
| extend Perms = tostring(AdditionalDetails)
| where Perms has_any ("Mail.ReadWrite","Files.ReadWrite.All","Directory.ReadWrite.All",
    "RoleManagement.ReadWrite.Directory","MailboxSettings.ReadWrite")
| project TimeGenerated, InitiatedBy=tostring(InitiatedBy.user.userPrincipalName), AppName,
| order by TimeGenerated desc
```

Playbook d'investigation M365 : séquence de réponse opérationnelle

Face à une compromission M365 confirmée, la séquence d'investigation doit être méthodique et dans un ordre précis. La règle absolue est : **capturer avant de contenir, contenir avant de remédier, remédier avant de communiquer**. Une action prématurée de containment — notamment désactiver le compte ou changer le mot de passe avant d'avoir exporté tous les artefacts forensiques — peut faire fuir l'attaquant vers d'autres comptes compromis avant qu'on ait compris l'étendue complète de la compromission, ou détruire des preuves essentielles pour la plainte pénale et pour satisfaire aux obligations de documentation NIS 2. La phase de capture forensique doit précéder systématiquement toute action : export des règles inbox actives, liste des applications OAuth consenties avec permissions effectives, historique complet des connexions sur 30 jours, délégations Exchange FullAccess et SendAs actuelles, et transport rules Exchange Online modifiées récemment.

Microsoft Graph API : visibilité défensive complète sur le tenant

L'**API Microsoft Graph** offre une visibilité sur le tenant M365 que les interfaces de hunting classiques n'atteignent pas toujours directement. Pour le hunting défensif, Graph permet de requêter les permissions effectives actuelles des applications enregistrées, les membres en temps réel des groupes privilégiés Entra ID, les appareils non conformes dans Intune, et les politiques de Conditional Access avec l'intégralité de leurs exclusions potentiellement exploitables par des attaquants. Un attaquant sophistiqué qui réalise une phase de reconnaissance dans un tenant M365 cible utilise systématiquement l'API Graph — le défenseur doit donc utiliser exactement les mêmes outils dans une démarche d'assumed breach proactive, pour identifier les failles avant que l'attaquant ne les découvre lors de sa propre reconnaissance.

```
 # Audit applications avec permissions Directory.ReadWrite via Microsoft Graph
$token = (Get-AzAccessToken -ResourceUrl "https://graph.microsoft.com").Token
$headers = @{ Authorization = "Bearer $token" }
$spns = (Invoke-RestMethod -Uri "https://graph.microsoft.com/v1.0/servicePrincipals" -Heade
$spns | Where-Object { $_.appRoles.value -contains "Directory.ReadWrite.All" } |
    Select-Object displayName, appId, createdDateTime | Format-Table
```

Analyse des lacunes Conditional Access : identifier les bypass de configuration

Le **Conditional Access** est la première ligne de défense de l'identité M365, mais sa configuration complexe génère fréquemment des lacunes que les attaquants exploitent méthodiquement et efficacement. Les lacunes les plus courantes que nous découvrons lors de nos audits de sécurité Microsoft 365 chez les clients français : exclusions de comptes de service excessives (ces comptes sans MFA deviennent des cibles prioritaires pour les attaquants car ils combinent des droits étendus et l'absence de protection MFA), politiques CAP en mode Report-Only jamais passées en Enforced après la période de test initiale, et authentification legacy (IMAP, POP3, SMTP Auth, EWS) non bloquée permettant de contourner entièrement le MFA sur Exchange Online depuis n'importe quelle connexion réseau avec simplement un identifiant et un mot de passe.

```
 // Connexions legacy auth réussies — bypass MFA potentiel systématique
SigninLogs
| where TimeGenerated > ago(7d)
| where ClientAppUsed in ("Exchange ActiveSync","IMAP4","POP3","SMTP Auth",
    "Exchange Web Services","Other clients")
| where ResultType == 0
| summarize Count=count(), UniqueIPs=dcount(IPAddress) by UserPrincipalName, ClientAppUsed
| where Count > 5
| order by Count desc
```

Questions fréquentes — Threat Hunting Microsoft 365 en 2026

Quelle est la différence entre le hunting proactif et réactif dans M365 ?

Le hunting **réactif** démarre sur une alerte existante — IOC connu ou règle analytique ayant tiré sur un seuil dépassé. Le hunting **proactif** part d'une hypothèse basée sur les TTPs connues d'un groupe ciblant votre secteur et cherche des preuves sans alerte préalable. Les organisations avec uniquement du hunting réactif seront systématiquement en retard de plusieurs semaines sur des attaquants sophistiqués. Un programme hybride — 80% réactif, 20% proactif — génère des détections 45 jours plus tôt en moyenne selon notre expérience terrain dans les SOC français que nous accompagnons.

Peut-on faire du threat hunting M365 efficacement sans licence E5 ?

Oui, mais avec des limitations importantes qui réduisent significativement la capacité de détection. En E3 : Unified Audit Logs sur 90 jours, SigninLogs Entra ID basiques, logs Exchange standard. Ce qui manque : Defender for Identity, MCAS, Entra ID Protection risk-based, audit avancé avec MailItemsAccessed, et Advanced Hunting Defender XDR complète. Pour des données sensibles ou une obligation NIS 2, la licence E5 Security est un investissement justifié au regard du coût moyen d'un incident BEC non détecté en France, estimé à 280 000 euros par Cybermalveillance.gouv.fr en 2024.

Comment intégrer les logs M365 dans un SIEM on-premise Splunk ou QRadar existant ?

Trois approches disponibles selon l'architecture : l'API Management Activity Office 365 avec un connecteur SIEM dédié (Splunk Add-on for Microsoft Office 365, IBM QRadar DSM M365), Azure Event Hub comme relai haute disponibilité pour les volumes importants dépassant 100 Go par jour, ou Microsoft Sentinel en mode hybride qui redistribue les alertes enrichies vers le SIEM on-premise via CEF/Syslog. L'Event Hub est recommandé pour les grands volumes car il garantit la non-perte de données avec une rétention intégrée de 7 jours même en cas d'indisponibilité temporaire du SIEM.

Quels IOC sont les plus fiables pour détecter une compromission M365 active ?

Par ordre de fiabilité décroissante dans notre expérience terrain : (1) règle de redirection email externe créée dans les 48 dernières heures, (2) connexion sans MFA pour un compte protégé par une règle CAP qui devrait l'exiger, (3) ajout d'une méthode MFA non reconnue par l'organisation dans les 2 heures suivant une connexion inhabituelle, (4) activité Exchange entre 2h et 5h du matin sans justification métier documentée, (5) download de plus de 100 fichiers en moins d'une heure via OneDrive, (6) consentement OAuth avec permissions élevées accordé par un non-administrateur.

Comment les attaquants sophistiqués effacent-ils leurs traces dans M365 ?

Les techniques APT anti-forensics M365 incluent : utilisation de proxys résidentiels (Luminati, Bright Data) pour imiter des connexions légitimes géographiquement cohérentes avec le profil de la victime, opérations concentrées sur les plages de non-surveillance comme les nuits et les jours fériés français, suppression des règles inbox immédiatement après l'action BEC finale pour effacer les traces de l'infrastructure de redirection, et création d'applications OAuth avant de réinitialiser le mot de passe du compte pour maintenir un accès persistant. La défense ultime : stockage immuable des logs en mode WORM (Sentinel avec Azure Blob WORM) qu'un administrateur compromis ne peut pas modifier ou supprimer rétroactivement.

Quelle fréquence recommandez-vous pour les sessions de hunting proactif M365 ?

Pour une organisation de 200 à 2000 utilisateurs avec des données sensibles : sessions **hebdomadaires** de 2 à 4 heures, avec rotation sur 8 à 10 scénarios de TTPs MITRE ATT&CK actuelles. Pour les OIV et OSE soumis à NIS 2 : sessions bi-hebdomadaires ciblant spécifiquement les vecteurs identité, email et applications cloud. Un programme de hunting mature génère en moyenne 3 à 5 nouvelles détections non couvertes par les règles analytiques existantes par trimestre, justifiant amplement l'investissement en temps.

Intégration Threat Intelligence : CERT-FR, TAXII et MDTI pour le hunting

Le hunting sans threat intelligence est aveugle et inefficace. L'intégration des feeds TI dans Sentinel enrichit automatiquement les logs M365 avec les IOC connus actuels : IP malveillantes actives, domaines de phishing en cours de campagne, hash de fichiers malveillants associés à des groupes spécifiques. Microsoft Defender Threat Intelligence (MDTI, ex-RiskIQ) fournit des IOC Microsoft-native directement intégrables dans les règles analytiques Sentinel via le connecteur natif, avec une mise à jour en quasi-temps réel basée sur la télémétrie globale Microsoft couvrant des centaines de millions de machines Windows dans le monde.

Pour les SOC français, les publications régulières du CERT-FR sur cert.ssi.gouv.fr concernant les IOC actifs ciblant les organisations françaises constituent une ressource primordiale souvent sous-exploitée par les équipes de sécurité qui se concentrent sur les feeds internationaux. Ces bulletins CERT-FR contiennent des IOC spécifiques aux campagnes visant des secteurs stratégiques français, publiés plusieurs semaines avant les feeds commerciaux internationaux grâce aux remontées directes des victimes françaises vers l'ANSSI. Les publications MITRE ATT&CK sur les tactiques de collection permettent de structurer les hypothèses de hunting en lien avec les TTPs documentées des groupes actifs ciblant l'Europe.

Containment immédiat : playbook PowerShell de réponse M365 en 30 minutes

Quand le hunting identifie un compte M365 actif compromis en cours, le containment doit être exécuté en moins de 30 minutes pour limiter l'impact. L'opinion que je défends fermement : automatiser ces étapes dans un playbook Logic Apps déclenché automatiquement par une alerte Sentinel haute confiance, sans requérir d'intervention humaine pour les premières actions de containment. L'exécution manuelle à 3h du matin par un analyste de garde fatigué introduit des erreurs critiques — mauvaise séquence des opérations, oubli de la capture forensique préalable, ou notification prématurée qui alerte l'attaquant — que l'automatisation élimine par définition tout en garantissant une réponse cohérente et documentée indépendamment du niveau de l'analyste de garde.

```
 # Containment M365 — 5 étapes séquentielles dans l'ordre exact
$UPN = "victime@entreprise.fr"
# 1. Capture forensique AVANT toute modification (préserver les preuves)
Get-InboxRule -Mailbox $UPN | Export-Csv "/tmp/inbox_$UPN.csv" -NoTypeInformation
Get-MailboxPermission -Identity $UPN | Export-Csv "/tmp/perms_$UPN.csv" -NoTypeInformation
# 2. Révoquer toutes les sessions actives (refresh tokens invalidés)
Revoke-AzureADUserAllRefreshToken -ObjectId (Get-AzureADUser -ObjectId $UPN).ObjectId
# 3. Désactiver le compte pour stopper tout accès actif
Set-AzureADUser -ObjectId $UPN -AccountEnabled $false
# 4. Reset mot de passe sécurisé 24 caractères
$NewPwd = [System.Web.Security.Membership]::GeneratePassword(24, 8)
Set-AzureADUserPassword -ObjectId $UPN -Password (ConvertTo-SecureString $NewPwd -AsPlainTe
# 5. Supprimer règles malveillantes APRÈS capture CSV
Get-InboxRule -Mailbox $UPN | Where-Object {$_.ForwardTo -ne $null -or $_.RedirectTo -ne $n
    Remove-InboxRule -Confirm:$false
```

Hunting exfiltration via Microsoft Teams : vecteur sous-estimé

Microsoft Teams est un vecteur d'exfiltration et de propagation de malware fréquemment sous-estimé dans les programmes de threat hunting. Les attaquants l'utilisent activement pour partager des liens de phishing en interne via des messages de chat — les utilisateurs font instinctivement

davantage confiance aux liens partagés par un collègue via Teams que par email car ils perçoivent Teams comme un canal interne sécurisé — et pour exfiltrer des données confidentielles via des conversations avec des contacts externes dans les organisations où la fédération Teams avec des tenants non managés est autorisée. La détection Teams dans M365 nécessite d'activer explicitement les logs Teams dans l'Unified Audit Log et de configurer le connecteur Teams dans Sentinel, car ces logs sont distincts des logs Exchange Online et ne sont pas collectés automatiquement par le connecteur Office 365 de base.

Le hunting Teams doit se concentrer sur trois patterns prioritaires : les messages contenant des liens externes vers des domaines apparus récemment dans les feeds de threat intelligence (domains âgés de moins de 30 jours, caractéristiques des infrastructures de phishing), les partages de fichiers volumineux vers des participants Teams externes appartenant à des organisations non partenaires connues (signal d'exfiltration), et les créations soudaines de canaux Teams privés avec des invités externes non référencés dans le répertoire de partenaires de l'organisation. Ces trois patterns couvrent les principaux scénarios d'utilisation malveillante de Teams que nous avons observés dans des incidents réels chez des clients français.

```
 // Liens externes partagés via Teams — phishing interne ou exfiltration
OfficeActivity
| where TimeGenerated > ago(7d)
| where RecordType == "MicrosoftTeams"
| where Operation == "MessageCreatedHasLink"
| extend ExtUrl = extract(@"https?://([^/\s""']+)", 1, tostring(AdditionalInfo))
| where ExtUrl !contains "microsoft.com" and ExtUrl !contains "sharepoint.com"
    and ExtUrl !contains "teams.microsoft.com" and ExtUrl !contains "votre-domaine.fr"
| project TimeGenerated, UserId, ExtUrl
| summarize count() by UserId, ExtUrl
| order by count_ desc
```

KPIs et métriques du programme de threat hunting M365

Un programme de threat hunting mature se mesure avec des KPIs précis revus mensuellement en COPIL sécurité pour maintenir l'engagement de la direction. Les indicateurs clés pour un SOC M365 français : le **MTTD (Mean Time to Detect)** des compromissions mesuré en comparant la

date réelle de compromission reconstruite forensiquement post-incident et la date effective de détection par l'équipe SOC ; le ratio nouvelles menaces détectées par hunting proactif versus alertes automatiques (objectif : dépasser les 20% par le hunting proactif pour justifier l'investissement en temps) ; et le taux de faux positifs des règles analytiques Sentinel (objectif : maintenir en dessous de 5% pour préserver la vigilance des analystes et éviter l'alert fatigue qui est l'ennemi numéro un de l'efficacité SOC). L'expérience terrain dans les SOC que nous accompagnons montre que les équipes consacrant 20% de leur temps au hunting proactif détectent les compromissions 45 jours plus tôt que les équipes 100% réactives. Pour les OIV et OSE soumis aux obligations de notification ANSSI dans le cadre de la directive NIS 2, ce délai fait la différence entre une notification volontaire dans les 72 heures réglementaires et une notification contrainte après incident public médiatisé.

Service de threat hunting M365 externalisé et formation des équipes

La mise en place d'un programme de threat hunting M365 mature nécessite des compétences rares — KQL avancé, connaissance approfondie des TTPs Microsoft-specific, capacité à corréler des millions d'événements et à distinguer les vrais signaux du bruit ambiant — et du temps dédié que les équipes de sécurité internes ont rarement, accaparées par les alertes quotidiennes et la gestion des incidents courants. Notre service RSSI externalisé intègre un programme de hunting mensuel complet : revue et mise à jour des règles Sentinel sur les nouvelles TTPs documentées par Microsoft Security Research et MITRE ATT&CK, sessions de hunting proactif de 4 heures couvrant les scénarios BEC, AiTM et pré-ransomware les plus actifs en France, et rapport d'investigation mensuel aligné sur les exigences de documentation ANSSI pour les organisations OIV et OSE.

Notre équipe Red Team simule régulièrement des attaques AiTM et BEC dans les environnements M365 de nos clients pour valider la détection en conditions réelles, avec les mêmes outils et techniques que les vrais attaquants. C'est le seul moyen de confirmer qu'un programme de hunting fonctionne réellement avant qu'un vrai attaquant ne le teste à votre place — et dans notre expérience, ces exercices de Red Team révèlent systématiquement des angles morts que ni les règles analytiques ni les sessions de hunting théoriques n'avaient identifiés.

Contactez-nous via le diagnostic NIS 2 pour évaluer votre maturité actuelle en threat hunting M365 et définir une roadmap adaptée à vos ressources et à votre profil de risque spécifique.

Pour les organisations qui souhaitent internaliser progressivement ces compétences, nous proposons également des ateliers de formation KQL dédiés aux analystes SOC, axés sur des scénarios de hunting réels extraits d'incidents français récents. Ces ateliers de 2 à 3 jours permettent aux équipes de monter en compétences sur les requêtes de hunting BEC, AiTM et pré-ransomware spécifiques à Microsoft 365, avec des exercices pratiques sur un environnement de lab M365 dédié. La formation inclut la mise en place d'un programme de hunting hebdomadaire structuré, avec une bibliothèque de 30 requêtes KQL de hunting couvrant les principales TTPs MITRE ATT&CK applicables à M365, prêtes à être intégrées dans votre instance Sentinel et adaptées au contexte de votre organisation et de votre secteur d'activité. Investir dans la montée en compétences KQL de vos analystes SOC est aujourd'hui l'un des retours sur investissement les plus élevés en matière de cybersécurité défensive pour les organisations qui opèrent dans un environnement Microsoft 365.

© Ayi NEDJIMI Consultants — Tous droits réservés