AYI NEDJIMI Consultants

Audit Avancé Microsoft 365 : Corréler Journaux et Logs Azure

Catégorie : Microsoft 365 Lecture : 3 min Publié le : 22/03/2026 Auteur : Ayi NEDJIMI

Corrélation des journaux Microsoft 365 pour l'audit avancé : Azure AD Sign-in, Unified Audit Log, Defender — méthodes KQL et Sentinel incluses.

L'**audit avancé Microsoft 365** requiert la corrélation de journaux issus de multiples sources hétérogènes : le *Unified Audit Log (UAL)* centralise les activités applicatives Exchange, SharePoint, Teams et Azure AD, les *Azure AD Sign-in Logs* tracent chaque événement d'authentification avec contexte IP et Device Compliance, *Microsoft Defender for Office 365* journalise les menaces email (phishing, malware, Safe Links), et *Defender for Endpoint* couvre les activités des terminaux Windows. Ce guide expert d'**Ayi NEDJIMI** présente les méthodes de corrélation avancée exploitant le langage KQL dans **Microsoft Sentinel**, les techniques de détection des compromissions furtives — vol de tokens, règles Inbox malveillantes, délégations suspectes — dans les environnements Microsoft 365 d'entreprise, et les playbooks d'investigation permettant de réduire le MTTR (Mean Time To Respond) lors d'un incident de sécurité M365.

Configuration Avancée UAL

```
# Configuration optimale de l'Unified Audit Log
Set-OrganizationConfig -AuditDisabled:$false
Enable-OrganizationCustomization
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled:$true
```

6 Intégration Microsoft Defender XDR

🛡️ Defender for Office 365

Protection avancée contre le phishing, malwares et liens malicieux avec analyse comportementale intégrée.

🔍 Defender for Identity

Détection des attaques sur les identités hybrides avec corrélation on-premises et cloud.

7 Requêtes KQL pour Threat Hunting

```
// Recherche d'activités suspectes multi-services
OfficeActivity
| where TimeGenerated > ago(24h)
| where Operation in ("FileDownloaded", "MailItemsAccessed", "Send")
| summarize EventCount = count(), UniqueFiles = dcount(OfficeObjectId) by UserId, ClientIP
| where EventCount > 100 or UniqueFiles > 50
```

Articles connexes

Approfondissez vos connaissances en sécurité Microsoft 365 avec ces guides experts :

🔗 API Microsoft Graph Audit

Maîtrisez l'API Microsoft Graph pour développer des solutions d'audit personnalisées et automatiser la corrélation.

🛡️ Threat Hunting M365

Techniques avancées de threat hunting avec Microsoft Defender et Sentinel pour corréler les indicateurs de compromission.

🔐 Automatisation Audit PowerShell

Automatisez l'audit et la corrélation des logs M365 avec PowerShell et l'API Microsoft Graph.

🎯 Outils d'Analyse Sécurité M365

Découvrez les 10 meilleurs outils pour l'analyse et la corrélation des données de sécurité Microsoft 365.

12 Conclusion et Bonnes Pratiques

🎯 Points Clés

- • **Corrélation multi-sources** essentielle
- • **Automatisation** des analyses répétitives
- • **Baseline comportementale** pour la détection
- • **Rétention long terme** pour les investigations
- • **Formation continue** des équipes SOC

📈 Évolution

- • **Intelligence artificielle** pour l'analyse

- • **Corrélation temps réel** avec SOAR
- • **Threat intelligence** contextualisée
- • **Automatisation** de la réponse
- • **Dashboards** exécutifs en temps réel

Points Clés à Retenir

- Le **Unified Audit Log** Microsoft 365 doit être activé explicitement — il n'est pas activé par défaut sur les tenants anciens
- Corrélation KQL entre **SignInLogs** et **AuditLogs** dans Microsoft Sentinel détecte les compromissions d'identité furtives
- Les logs **Defender for Endpoint** et **Defender for Identity** se complètent pour couvrir les vecteurs cloud et AD
- Activez la rétention des logs à 180 jours minimum (nécessite licence M365 E3/E5 ou add-on) pour les investigations forensiques

Tableau Récapitulatif des Sources de Logs Microsoft 365

Source de Logs	Données Couverts	Rétention Défaut	Accès via
Unified Audit Log	Exchange, SharePoint, Teams, Azure AD, Defender	90j (E1/E3), 365j (E5)	Purview, PowerShell, Graph API
Azure AD Sign-in Logs	Authentifications, MFA, Conditional Access	30j (P1), 90j (P2)	Azure Portal, Graph API, Sentinel
Defender for Office 365	Email threats, Safe Links, Safe Attachments	90 jours	Defender Portal, Graph Security API
Defender for Endpoint	Activités terminaux, alertes EDR	6 mois (cloud)	Defender Portal, Advanced Hunting
Azure Activity Log	Opérations Azure Resource Manager	90 jours	Azure Monitor, Log Analytics

- Sécuriser l'accès Microsoft 365 avec Conditional Access et MFA
- Threat Hunting Microsoft 365 avec Defender et Sentinel
- Automatiser l'audit sécurité Microsoft 365 via PowerShell
- Détection des attaques Azure AD et compromission d'identités
- Conformité Microsoft 365 : outils intégrés et audit

Combien de temps sont conservés les logs Microsoft 365 par défaut ?

Par défaut, les logs du **Unified Audit Log** sont conservés 90 jours pour Microsoft 365 Business/E1/E3, et 365 jours pour M365 E5. La rétention étendue (10 ans) est disponible avec le module Audit (Premium). Il est critique d'activer et configurer la rétention avant tout incident.

Comment corréler les logs Azure AD Sign-in avec les logs Defender ?

Via **Microsoft Sentinel** avec les connecteurs Azure AD et Defender, utilisez KQL : joignez la table SignInLogs avec SecurityAlert sur l'UserPrincipalName et la plage temporelle. Le workbook 'Azure AD Sign-in Analysis' de Sentinel automatise cette corrélation.

Quels Event IDs sont critiques dans l'audit Microsoft 365 ?

Les opérations prioritaires dans l'Unified Audit Log : **UserLoggedIn** (connexions), **FileDownloaded** (exfiltration), **Add-MailboxPermission** (BEC), **Set-Mailbox ForwardingSmtpAddress** (règles de transfert), et **Add-RoleGroupMember** (élévation de privilèges).

Conclusion

La corrélation des journaux Microsoft 365 est la clé d'une détection efficace des compromissions avancées. En combinant l'Unified Audit Log, Azure AD Sign-in Logs et Microsoft Defender via KQL dans Sentinel, vous disposez d'une visibilité complète sur les activités suspectes dans votre tenant M365. Téléchargez les requêtes KQL de ce guide et configurez des alertes automatisées pour une supervision continue.

Sources et références : Microsoft Security Docs · CERT-FR

Références et Ressources Officielles

- Microsoft Unified Audit Log — Documentation Officielle
- Microsoft Sentinel — KQL Reference
- ANSSI — Guide de la supervision des SI

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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