AYI NEDJIMI Consultants

Forensique Microsoft 365 : Analyse du Unified Audit Log

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

Guide de forensique Microsoft 365 : Unified Audit Log, investigation de compromission de compte, analyse d'activité suspecte, eDiscovery et réponse à.

L'investigation forensique M365 presente des defis uniques par rapport a la forensique traditionnelle sur endpoint. L'analyste n'a pas acces au systeme de fichiers, a la memoire vive ou aux artefacts systeme classiques. Tout repose sur les **journaux d'audit** fournis par Microsoft, dont la completude, la retention et l'accessibilite dependent du niveau de licence. Comprendre ces contraintes est la premiere etape d'une investigation reussie. Guide de forensique Microsoft 365 : Unified Audit Log, investigation de compromission de compte, analyse d'activité suspecte, eDiscovery et réponse à. L'investigation numérique exige rigueur et méthodologie. Forensique Microsoft 365 : Analyse du Unified Audit Log couvre les aspects pratiques que les analystes forensics rencontrent sur le terrain. Nous abordons notamment : questions frequentes, conclusion. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

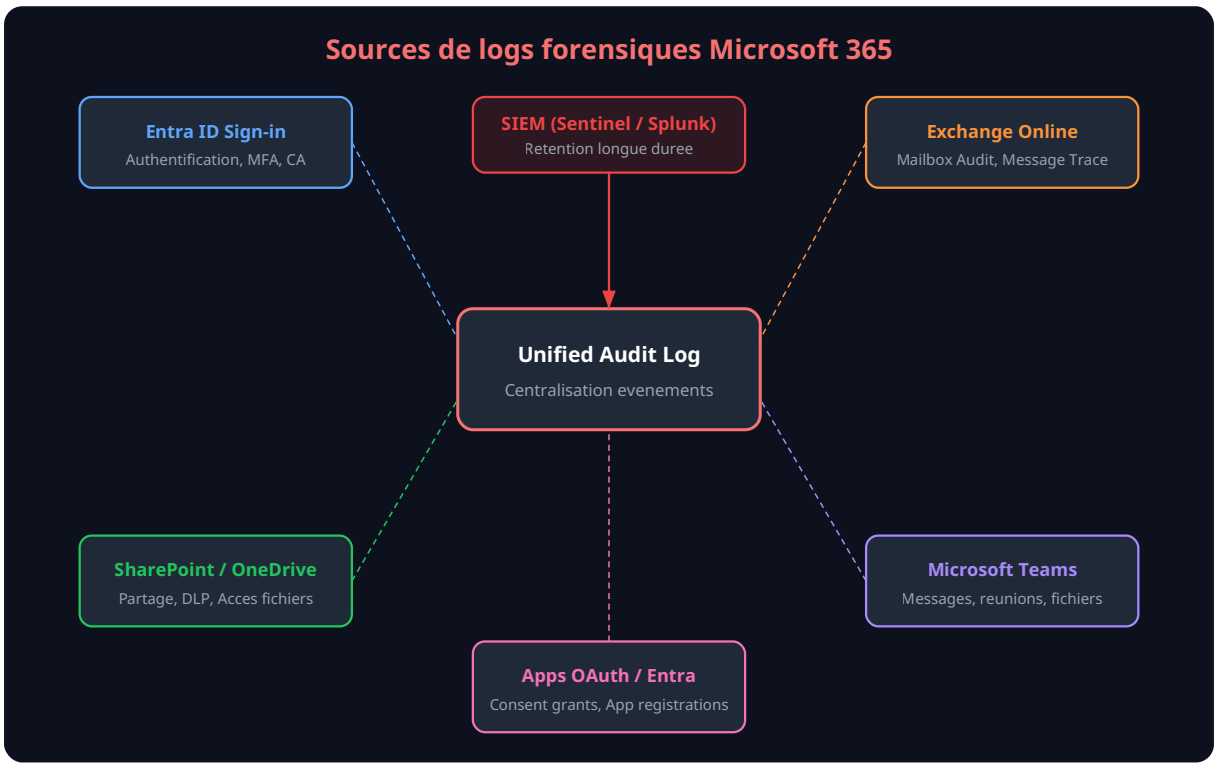
Point critique : Licence et retention des logs
La retention par defaut du Unified Audit Log est de **180 jours** pour les licences E5 et de **90 jours** pour les licences E3/E1. Depuis 2024, Microsoft propose Audit (Premium) avec une retention de 365 jours. En l'absence de licence adequate ou d'export SIEM, les preuves peuvent etre irremediablement perdues apres cette periode. Il est imperatif de configurer l'export des logs vers un SIEM (Sentinel, Splunk, Elastic) des le deploiement du tenant.

Vos journaux d'événements sont-ils conservés suffisamment longtemps pour une investigation ?

```
# Recherche basique sur un utilisateur compromis
Search-UnifiedAuditLog -StartDate "2026-01-01" -EndDate "2026-02-15" `
    -UserIds "victim@contoso.com" -ResultSize 5000

# Recherche des connexions suspectes
Search-UnifiedAuditLog -StartDate "2026-01-15" -EndDate "2026-02-15" `
    -Operations "UserLoggedIn","UserLoginFailed" `
    -UserIds "victim@contoso.com" -ResultSize 5000

# Recherche des regles de boite aux lettres creees
Search-UnifiedAuditLog -StartDate "2026-01-01" -EndDate "2026-02-15" `
    -Operations "New-InboxRule","Set-InboxRule","Enable-InboxRule" `
    -ResultSize 5000

# Recherche des consentements OAuth
Search-UnifiedAuditLog -StartDate "2026-01-01" -EndDate "2026-02-15" `
    -Operations "Consent to application" -ResultSize 5000

# Recherche avec pagination pour des resultats volumineux
$results = @()
$sessionId = [Guid]::NewGuid().ToString()
do {
    $batch = Search-UnifiedAuditLog -StartDate "2026-01-01" `
        -EndDate "2026-02-15" -SessionId $sessionId `
        -SessionCommand ReturnLargeSet -ResultSize 5000
    $results += $batch
} while ($batch.Count -eq 5000)

# Export en CSV pour analyse
$results | Select-Object CreationDate, UserIds, Operations, AuditData |
    Export-Csv -Path "C:\Investigation\UAL_Export.csv" -NoTypeInformation

# Extraction des donnees JSON imbriquees
$results | ForEach-Object {
    $audit = $_.AuditData | ConvertFrom-Json
    [PSCustomObject]@{
        Timestamp   = $audit.CreationTime
        User        = $audit.UserId
        Operation   = $audit.Operation
        ClientIP    = $audit.ClientIP
        UserAgent   = $audit.ExtendedProperties |
                      Where-Object { $_.Name -eq "UserAgent" } |
                      Select-Object -ExpandProperty Value
        ResultStatus = $audit.ResultStatus
    }
} | Export-Csv -Path "C:\Investigation\UAL_Parsed.csv" -NoTypeInformation
```

Bonne pratique : Export continu vers un SIEM

Ne vous reposez pas uniquement sur la retention native de l'UAL. Configurez un export continu vers votre SIEM via l'API Office 365 Management Activity ou via le connecteur Microsoft Sentinel. Cela garantit une retention a long terme, permet des correlations croisees avec d'autres sources, et offre des capacites de detection en temps reel. L'API Management Activity offre des webhooks pour une ingestion en quasi temps reel des evenements.




```
# Rechercher les consentements OAuth dans l'UAL
Search-UnifiedAuditLog -StartDate "2026-01-01" -EndDate "2026-02-15" `
    -Operations "Consent to application" -ResultSize 5000 |
    ForEach-Object {
        $data = $_.AuditData | ConvertFrom-Json
        [PSCustomObject]@{
            Date       = $data.CreationTime
            User       = $data.UserId
            AppName    = $data.Target[0].ID
            Permissions = ($data.ModifiedProperties |
                Where-Object {$_.Name -eq "ConsentContext.IsAdminConsent"}).NewValue
            ClientIP   = $data.ClientIP
        }
    }

# Lister les applications avec des permissions elevees
Get-MgServicePrincipal -All | ForEach-Object {
    $sp = $_
    $appRoles = Get-MgServicePrincipalAppRoleAssignment -ServicePrincipalId $sp.Id
    if ($appRoles) {
        [PSCustomObject]@{
            AppName     = $sp.DisplayName
            AppId       = $sp.AppId
            Created     = $sp.AdditionalProperties.createdDateTime
            Permissions = ($appRoles | Select-Object -ExpandProperty AppRoleId) -join ", "
        }
    }
} | Where-Object { $_.AppName -notmatch "Microsoft|Office|Azure" }
```

Verification du mailbox forwarding

Outre les regles de boite aux lettres, les attaquants configurent souvent le **forwarding SMTP** au niveau de la boite aux lettres elle-meme. Ce forwarding est different des inbox rules : il est configure au niveau du transport Exchange et redirige *tous* les emails entrants vers une adresse externe sans laisser de copie dans la boite d'origine. C'est une technique furtive utilisee dans les attaques BEC pour intercepter les communications financieres.

```
# Verifier le forwarding configure sur une boite aux lettres
Get-Mailbox -Identity "victim@contoso.com" |
    Select-Object ForwardingAddress, ForwardingSmtpAddress,
    DeliverToMailboxAndForward

# Verifier le forwarding sur TOUTES les boites aux lettres du tenant
Get-Mailbox -ResultSize Unlimited |
    Where-Object { $_.ForwardingSmtpAddress -ne $null -or
                   $_.ForwardingAddress -ne $null } |
    Select-Object DisplayName, PrimarySmtpAddress,
    ForwardingSmtpAddress, ForwardingAddress,
    DeliverToMailboxAndForward | Export-Csv "C:\Investigation\Forwarding.csv"

# Rechercher les modifications de forwarding dans l'UAL
Search-UnifiedAuditLog -StartDate "2026-01-01" -EndDate "2026-02-15" `
    -Operations "Set-Mailbox" -ResultSize 5000 |
    ForEach-Object {
        $data = $_.AuditData | ConvertFrom-Json
        $fwd = $data.Parameters | Where-Object {
            $_.Name -match "ForwardingSmtpAddress|ForwardingAddress"
        }
        if ($fwd) {
            [PSCustomObject]@{
                Date     = $data.CreationTime
                User     = $data.UserId
                Mailbox  = $data.ObjectId
                Param    = $fwd.Name
                Value    = $fwd.Value
                ClientIP = $data.ClientIP
            }
        }
    }
```

Analyse des enregistrements d'applications

Les applications enregistrees dans Entra ID constituent un vecteur de persistance avance. Un attaquant avec des droits Global Admin ou Application Administrator peut enregistrer une application avec des permissions Graph API elevees, generer un secret client, et utiliser ces credentials pour maintenir un acces meme apres la remediation du compte initial. Les attaques sur les identity providers comme Entra ID exploitent frequemment ce mecanisme.

```
# Rechercher les enregistrements d'applications recents
Search-UnifiedAuditLog -StartDate "2026-01-01" -EndDate "2026-02-15" `
    -Operations "Add application","Add service principal",
    "Add app role assignment to service principal",
    "Add service principal credentials" -ResultSize 5000

# Lister les applications avec des secrets recemment crees
Get-MgApplication -All | ForEach-Object {
    $app = $_
    $secrets = $app.PasswordCredentials | Where-Object {
        $_.StartDateTime -gt (Get-Date).AddDays(-90)
    }
    if ($secrets) {
        [PSCustomObject]@{
            AppName   = $app.DisplayName
            AppId     = $app.AppId
            Created   = $secrets.StartDateTime
            Expires   = $secrets.EndDateTime
            KeyId     = $secrets.KeyId
        }
    }
}
```

Examiner les regles de boite aux lettres, le forwarding SMTP, les consentements OAuth, les applications enregistrees, les modifications de role et les delegations. Rechercher les indicateurs de persistance et de mouvement lateral. Verifier si d'autres comptes ont ete compromis a partir du compte initial.

Phase 5 : Evaluation de l'impact sur les donnees

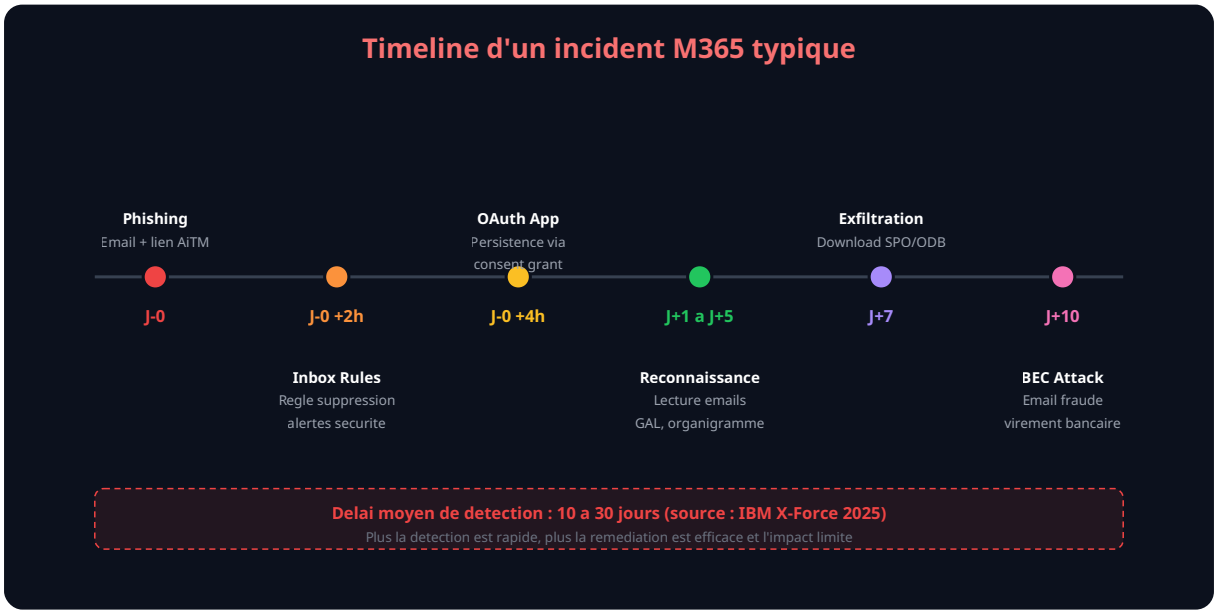
Quantifier l'acces aux donnees : emails lus (MailItemsAccessed), fichiers telecharges (FileDownloaded), partages crees (SharingSet), donnees DLP detectees. Evaluer si des donnees sensibles, personnelles ou reglementees ont ete exposees. Cette evaluation determine les obligations de notification (RGPD, NIS2).

Phase 6 : Remediation

Apres la preservation et l'analyse, proceder a la remediation : reset des mots de passe, revocation des sessions et tokens de rafraichissement, suppression des regles malveillantes, revocation des consentements OAuth, suppression des applications frauduleuses, desactivation du forwarding, et verification des politiques d'acces conditionnel.

Phase 7 : Rapport et recommandations

Documenter l'ensemble de l'investigation : timeline de l'incident, indicateurs de compromission (IOCs), comptes impactes, donnees exposees, actions de remediation effectuees. Formuler des recommandations pour prevenir de futurs incidents : activation du MFA resistant au phishing (FIDO2), politiques d'acces conditionnel renforcees, restriction des consentements OAuth, monitoring continu.



Pour approfondir ce sujet, consultez notre outil open-source incident-response-toolkit qui facilite la réponse automatisée aux incidents de sécurité.

Questions frequentes

Comment mettre en place Forensique Microsoft 365 dans un environnement de production ?

La mise en place de Forensique Microsoft 365 en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Pourquoi Forensique Microsoft 365 est-il essentiel pour la securite des systemes d'information ?

Forensique Microsoft 365 constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

Quels outils open source utiliser pour Forensique Microsoft 365 : Analyse du Unified Audit Log ?

Les incontournables sont Autopsy, Volatility 3, Plaso/log2timeline et RegRipper. Ils couvrent l'analyse disque, mémoire, timeline et registre sans coût de licence.

Sources et références : SANS SIFT · MITRE ATT&CK

Conclusion

La forensique Microsoft 365 est une competence devenue indispensable pour toute equipe de reponse a incident. La centralisation des services de collaboration dans le cloud M365 offre aux attaquants une surface d'attaque considerable, mais fournit egalement aux defenseurs des sources de logs riches et detaillees. Le Unified Audit Log, les sign-in logs Entra ID, le message trace Exchange et les outils eDiscovery constituent un arsenal complet pour mener des investigations approfondies.

La cle d'une investigation reussie reside dans la **preparation en amont** : activation de l'audit, configuration de la retention adequate, export continu vers un SIEM, et documentation des procedures d'investigation. Les outils comme HAWK, Sparrow et CRT automatisent une grande partie de la collecte, mais l'expertise de l'analyste reste essentielle pour interpreter les resultats, etablir les correlations et reconstruire la chronologie de l'incident.

Enfin, chaque investigation doit se conclure par des recommandations actionables : activation du MFA resistant au phishing (cles FIDO2, Windows Hello for Business), renforcement des politiques d'acces conditionnel, restriction des consentements OAuth aux applications approuvees, et mise en place d'un monitoring continu des indicateurs de compromission. La forensique n'est pas seulement reactive : elle alimente le cycle d'amelioration continue de la securite du tenant M365.

Articles associes

- Phishing sans piece jointe : techniques avancees -- Vecteur initial le plus courant des compromissions M365
- OAuth Security : attaques et defenses -- Comprendre les abus de consentement OAuth dans Entra ID
- Azure AD : securite des applications enregistrees -- Persistence via les app registrations et service principals
- Attaques sur les Identity Providers -- Techniques d'attaque sur Entra ID, Okta et Keycloak

- Exfiltration furtive de donnees -- Techniques d'exfiltration via SharePoint et OneDrive
- Infostealers : la menace silencieuse -- Vol de credentials et tokens de session M365

References et ressources externes

- Microsoft Learn - Unified Audit Log -- Documentation officielle Microsoft sur l'audit unifie
- HAWK - PowerShell forensics tool -- Outil open source d'investigation M365
- CISA Sparrow -- Outil de detection de compromission Azure AD / M365
- CrowdStrike CRT -- Cloud Response Toolkit pour Azure
- MITRE ATT&CK T1114 - Email Collection -- Technique de collecte d'emails dans le framework ATT&CK

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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