AYI NEDJIMI Consultants

# Microsoft Defender for Office 365 : Configuration : Guide

Catégorie : Microsoft 365 Lecture : 11 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

*Guide avancé Microsoft Defender for Office 365 : policies anti-phishing, Safe Links, Safe Attachments, Threat Explorer, simulation d'attaques et.*

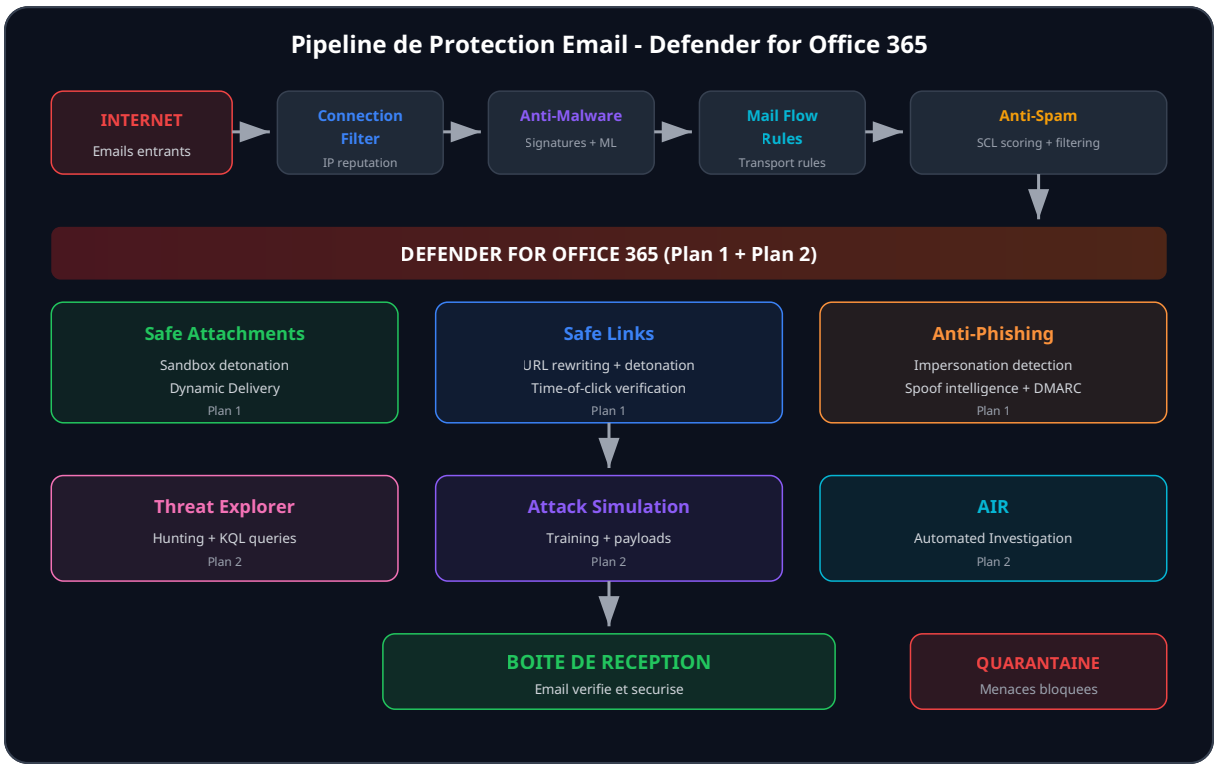
La combinaison avec DMARC est essentielle. Lorsque `HonorDmarcPolicy` est active, Defender respecte les enregistrements DMARC des domaines expediteurs. Un email echouant l'alignement DMARC avec une policy `p=reject` sera rejete. Cela impose que votre propre domaine ait un enregistrement DMARC valide en mode `p=quarantine` ou `p=reject` (pas `p=none` qui n'offre aucune protection effective). Guide avancé Microsoft Defender for Office 365 : policies anti-phishing, Safe Links, Safe Attachments, Threat Explorer, simulation d'attaques et. Microsoft 365 est omniprésent en entreprise et sa surface d'attaque ne cesse de s'étendre. La sécurisation de defender office 365 anti phishing nécessite une approche structurée et des outils adaptés. Nous abordons notamment : 2. safe links : protection des url en temps reel, 3. safe attachments : sandbox et dynamic delivery et 4. threat explorer et hunting avance. 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.

### 1.3 Seuils de phishing (PhishThresholdLevel)

Le `PhishThresholdLevel` controle l'agressivite de la detection de phishing. Microsoft propose quatre niveaux :

| Niveau | Comportement | Faux positifs | Recommandation |
|---|---|---|---|
| **1 - Standard** | Detection basique, seuil eleve | Tres faible | Non recommande (trop permissif) |
| **2 - Aggressive** | Detection renforcee | Faible | Minimum acceptable |
| **3 - More Aggressive** | Detection proactive | Modere | Recommande pour la plupart des organisations |
| **4 - Most Aggressive** | Detection maximale | Eleve | Environnements haute securite uniquement |

**Attention : migration progressive des seuils**
Ne passez jamais directement du niveau 1 au niveau 4. Commencez par le niveau 2 pendant deux semaines, analysez les faux positifs dans la quarantaine, ajustez les exceptions (Tenant Allow/Block List), puis montez au niveau 3. Le passage au niveau 4 doit etre reserve aux organisations avec un SOC capable de traiter le volume d'alertes supplementaire.




**Notre avis d'expert**

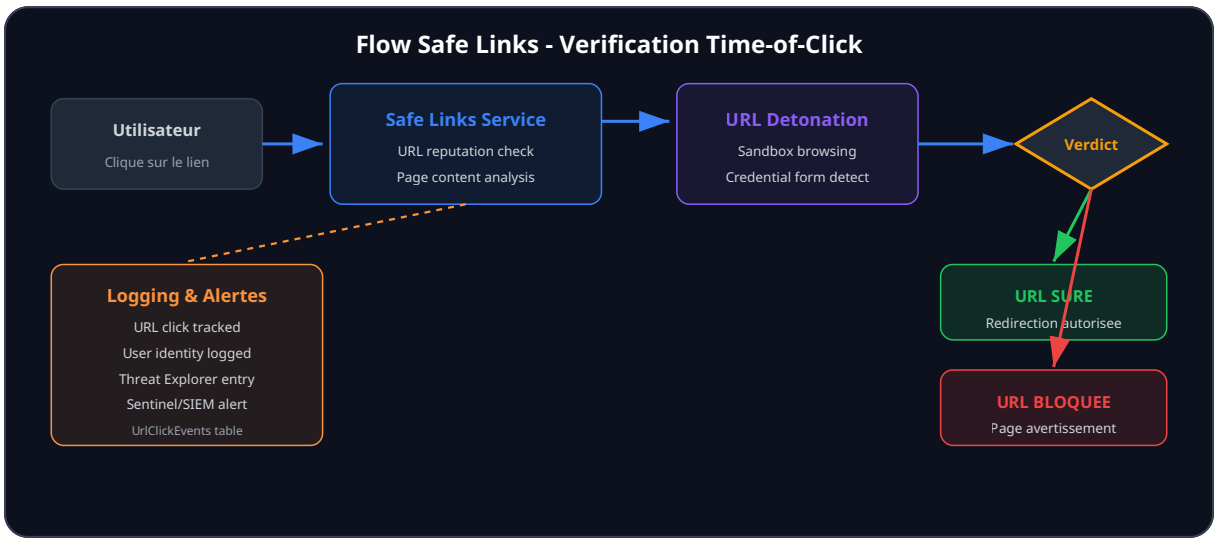
L'accès conditionnel Azure AD est probablement la fonctionnalité de sécurité la plus sous-exploitée de l'écosystème Microsoft. Correctement configuré, il offre un contrôle granulaire qui rend obsolètes de nombreuses solutions de sécurité tierces coûteuses.

## 2. Safe Links : Protection des URL en Temps Reel

### 2.1 Fonctionnement de Safe Links

Safe Links reecrit les URL contenues dans les emails pour les faire transiter par le service de verification Microsoft lors du clic. Cette approche "time-of-click" est fondamentalement superieure a la verification statique au moment de la reception de l'email. Les attaquants utilisent de plus en plus des techniques de **URL staging** : l'URL est inoffensive au moment de la livraison de l'email (et passe donc les filtres), puis est modifiee quelques heures apres pour pointer vers une page de phishing ou un malware.

Lorsqu'un utilisateur clique sur un lien reecrit, Safe Links effectue une verification en temps reel : reputation de l'URL, analyse du contenu de la page de destination, detection de formulaires de credential harvesting, et detonation dans un environnement sandbox si necessaire. Si l'URL est jugee malveillante, l'utilisateur est redirige vers une page d'avertissement bloquante.




## 2.2 Configuration Safe Links

```
# Creer une policy Safe Links stricte
New-SafeLinksPolicy -Name "SafeLinks-Stricte" `
    -EnableSafeLinksForEmail $true `
    -EnableSafeLinksForTeams $true `
    -EnableSafeLinksForOffice $true `
    -TrackClicks $true `
    -AllowClickThrough $false `
    -ScanUrls $true `
    -EnableForInternalSenders $true `
    -DeliverMessageAfterScan $true `
    -DisableUrlRewrite $false `
    -EnableOrganizationBranding $true

# Appliquer a tout le domaine
New-SafeLinksRule -Name "Rule-SafeLinks-Stricte" `
    -SafeLinksPolicy "SafeLinks-Stricte" `
    -RecipientDomainIs "contoso.com" `
    -Priority 0

# Ajouter des URL a ne jamais reecrire (whitelist)
Set-SafeLinksPolicy -Identity "SafeLinks-Stricte" `
    -DoNotRewriteUrls @{Add="https://intranet.contoso.com/*","https://erp.contoso.com/*"}
```

Le parametre `AllowClickThrough $false` est critique : il empeche l'utilisateur de contourner l'avertissement et de poursuivre vers l'URL malveillante. Sans ce parametre, un utilisateur determine peut ignorer l'avertissement et acceder quand meme a la page de phishing. Le `TrackClicks $true` enregistre chaque clic dans les logs, ce qui permet au SOC de savoir exactement qui a clique sur quoi et quand.

# 3. Safe Attachments : Sandbox et Dynamic Delivery

## 3.1 Modes de fonctionnement

Safe Attachments ouvre chaque piece jointe dans un environnement sandbox Microsoft pour detecter les comportements malveillants : execution de macros, telechargement de payload secondaire, tentative d'escalade de privileges, communication C2. Quatre modes sont disponibles :

- **Off :** Desactive. Les pieces jointes ne sont pas analysees par Safe Attachments (l'anti-malware classique reste actif).
- **Monitor :** Les pieces jointes sont analysees mais jamais bloquees. Utile pour la phase d'evaluation initiale.
- **Block :** Les pieces jointes detectees comme malveillantes sont mises en quarantaine. L'email est livre sans la piece jointe, avec une notification.
- **Dynamic Delivery :** Le mode recommande. L'email est livre immediatement avec un placeholder a la place de la piece jointe. Une fois l'analyse terminee (generalement 1 a 2 minutes), la piece jointe originale remplace le placeholder si elle est jugee sure, ou reste bloquee si elle est malveillante.

```
# Policy Safe Attachments en Dynamic Delivery
New-SafeAttachmentPolicy -Name "SafeAttach-DynamicDelivery" `
    -Enable $true `
    -Action "DynamicDelivery" `
    -ActionOnError $true `
    -Redirect $true `
    -RedirectAddress "securite-soc@contoso.com"

New-SafeAttachmentRule -Name "Rule-SafeAttach-Global" `
    -SafeAttachmentPolicy "SafeAttach-DynamicDelivery" `
    -RecipientDomainIs "contoso.com" `
    -Priority 0

# Activer Safe Attachments pour SharePoint, OneDrive et Teams
Set-AtpPolicyForO365 -EnableATPForSPOTeamsODB $true `
    -EnableSafeDocs $true `
    -AllowSafeDocsOpen $false
```

## 3.2 Safe Documents pour Office

Safe Documents etend la protection sandbox aux fichiers ouverts en Protected View dans les applications Office (Word, Excel, PowerPoint). Lorsqu'un utilisateur tente de quitter la Protected View pour editer un document telecharge d'Internet ou recu par email, Safe Documents envoie le fichier au cloud Microsoft pour analyse. Si le fichier est malveillant, l'utilisateur est empeche de quitter la Protected View. Le parametre `AllowSafeDocsOpen $false` empeche meme les utilisateurs d'ignorer l'avertissement.

**Cas concret**
L'exploitation de la fonctionnalité de consentement OAuth dans Azure AD a permis à des attaquants de créer des applications malveillantes obtenant un accès persistant aux données Microsoft 365 des victimes. Cette technique de "consent phishing" contourne le MFA puisque l'utilisateur autorise lui-même l'accès.

Votre MFA est-il résistant aux attaques de type adversary-in-the-middle ?

# 4. Threat Explorer et Hunting Avance

## 4.1 Threat Explorer (Plan 2)

Threat Explorer est l'outil d'investigation et de hunting de Defender for Office 365 Plan 2. Il permet de rechercher, analyser et remedier les emails malveillants dans l'ensemble du tenant. Les vues principales incluent : All email, Malware, Phish, Content malware, et URL clicks. Chaque vue offre des filtres granulaires : expediteur, destinataire, sujet, detection technology, delivery action, et plus.

La puissance de Threat Explorer reside dans sa capacite de remediation post-delivery. Meme si un email malveillant a atteint la boite de reception (parce que l'URL etait inoffensive au moment de la livraison, par exemple), l'analyste SOC peut identifier tous les destinataires ayant recu cet email et executer un "soft delete" ou "hard delete" en masse. Cette capacite de "purge" est essentielle dans la reponse a incident.

## 4.2 Hunting avec KQL dans Advanced Hunting

Advanced Hunting dans le portail Microsoft 365 Defender permet d'ecrire des requetes KQL (Kusto Query Language) sur les tables de telemetrie email. Les tables principales pour le hunting email sont : `EmailEvents`, `EmailUrlInfo`, `EmailAttachmentInfo`, `EmailPostDeliveryEvents`, et `UrlClickEvents`.

```
// Detecter les emails de phishing ayant atteint la boite de reception
EmailEvents
| where Timestamp > ago(7d)
| where ThreatTypes has "Phish"
| where DeliveryAction == "Delivered"
| summarize Count=count(), Recipients=make_set(RecipientEmailAddress)
    by SenderFromAddress, Subject, ThreatTypes
| sort by Count desc

// Identifier les URL cliquees malgre un avertissement Safe Links
UrlClickEvents
| where Timestamp > ago(7d)
| where ActionType == "ClickAllowed" or ActionType == "ClickBlocked"
| where IsClickedThrough == true
| project Timestamp, AccountUpn, Url, ActionType, NetworkMessageId
| join kind=inner (
    EmailEvents | project NetworkMessageId, SenderFromAddress, Subject
) on NetworkMessageId
| project Timestamp, AccountUpn, SenderFromAddress, Subject, Url

// Campagnes de phishing : regrouper par patterns d'URL
EmailUrlInfo
| where Timestamp > ago(30d)
| where UrlDomain !in ("microsoft.com","office.com","sharepoint.com")
| join kind=inner (
    EmailEvents | where ThreatTypes has "Phish"
) on NetworkMessageId
| summarize EmailCount=dcount(NetworkMessageId),
    UniqueRecipients=dcount(RecipientEmailAddress),
    Senders=make_set(SenderFromAddress)
    by UrlDomain
| where EmailCount > 5
| sort by EmailCount desc

// Pieces jointes suspectes : types inhabituels
EmailAttachmentInfo
| where Timestamp > ago(7d)
| where FileType in ("iso","img","vhd","vhdx","one","wsf","hta","js","vbs")
| join kind=inner EmailEvents on NetworkMessageId
| project Timestamp, SenderFromAddress, RecipientEmailAddress,
    Subject, FileName, FileType, SHA256, ThreatTypes
| sort by Timestamp desc
```

**Bonne pratique : detection rules personnalisees**
Transformez vos requetes KQL de hunting en Custom Detection Rules pour automatiser la detection. Une rule peut generer une alerte, declencher un playbook Logic App, ou creer un incident dans Microsoft Sentinel. Priorisez les detections de credential phishing (formulaires de login Microsoft 365 clones) et de BEC (Business Email Compromise).

## 5. Attack Simulation Training

### 5.1 Types de simulations

Attack Simulation Training (Plan 2) permet de lancer des campagnes de phishing simulees contre les employes pour mesurer leur niveau de vigilance et les former de maniere continue. Microsoft propose plusieurs types de simulations :

| Type de simulation | Description | Objectif de mesure |
|---|---|---|
| **Credential Harvest** | Page de login clonee (Microsoft, Google, etc.) | Taux de soumission de credentials |
| **Malware Attachment** | Piece jointe simulant un document piege | Taux d'ouverture de pieces jointes suspectes |
| **Link in Attachment** | Document avec lien vers une page de phishing | Taux de clic sur liens dans des documents |
| **Link to Malware** | Lien direct vers un telechargement simule | Taux de telechargement de fichiers suspects |
| **Drive-by URL** | Lien vers une page avec contenu dynamique | Taux de visite de pages suspectes |
| **OAuth Consent Grant** | Demande de consentement OAuth malveillant | Taux d'acceptation de permissions excessives |

## 5.2 Payloads et templates

Microsoft fournit une bibliotheque de payloads pre-construits imitant des scenarios reels : notification de messagerie vocale, demande de reinitialisation de mot de passe, notification de partage SharePoint, confirmation de commande, alerte de securite. Les payloads sont regulierement mis a jour pour refleter les tendances actuelles du phishing. Il est egalement possible de creer des payloads personnalises utilisant le contexte specifique de l'organisation (logo, noms de projets, outils internes) pour des simulations plus realistes.

Les meilleures pratiques pour les simulations incluent : lancer des campagnes mensuelles avec des niveaux de difficulte progressifs, varier les types de simulation d'un mois a l'autre, cibler l'ensemble des employes (pas seulement les equipes non techniques), et coupler chaque simulation avec un module de formation interactif qui s'affiche automatiquement lorsqu'un employe "tombe dans le piege".

## 5.3 Metriques de maturite

Les indicateurs cles a suivre dans le temps pour mesurer la maturite anti-phishing de l'organisation :

- **Compromise Rate :** Pourcentage d'utilisateurs ayant soumis leurs credentials. Cible : inferieur a 5 % apres 6 mois de programme.
- **Click Rate :** Pourcentage d'utilisateurs ayant clique sur le lien de phishing. Cible : inferieur a 15 %.
- **Report Rate :** Pourcentage d'utilisateurs ayant signale l'email via le bouton "Report Phishing". Cible : superieur a 30 %. C'est la metrique la plus importante car elle mesure le comportement proactif.
- **Repeat Offenders :** Utilisateurs compromis dans plusieurs campagnes consecutives. Ces utilisateurs necessitent une formation individuelle renforcee.

- **Time to Report :** Duree moyenne entre la reception de l'email et le signalement. Cible : inferieur a 10 minutes pour les premiers signalements.

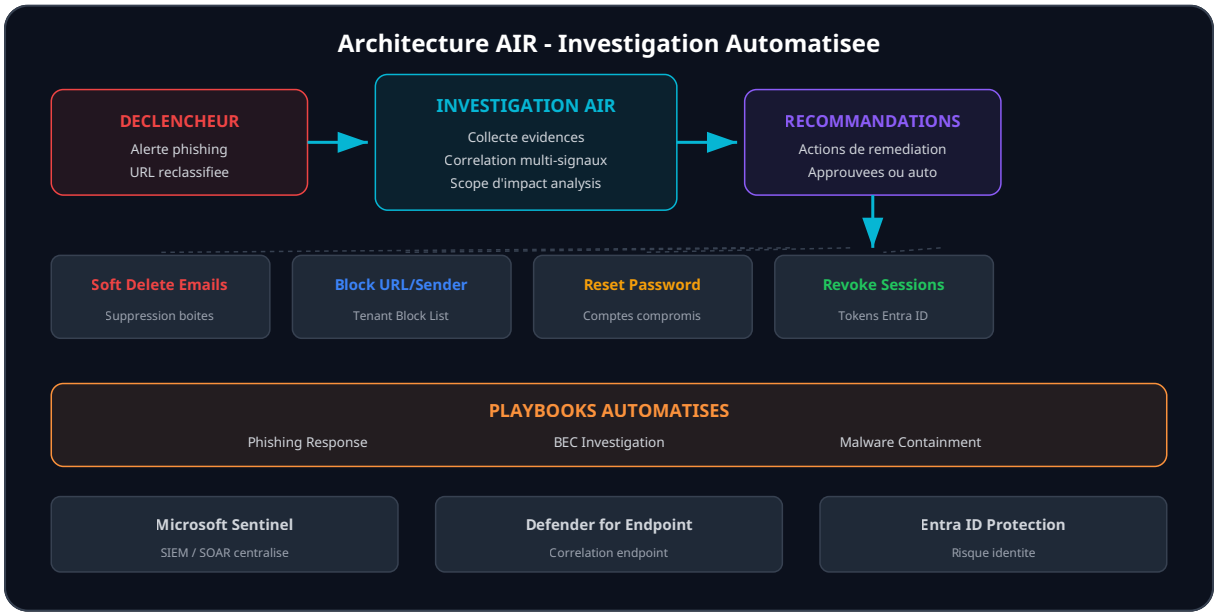
```
# Recuperer les resultats des simulations via Graph API
$simulations = Invoke-MgGraphRequest -Method GET `
    -Uri "https://graph.microsoft.com/v1.0/security/attackSimulation/simulations" `
    -OutputType PSObject

foreach ($sim in $simulations.value) {
    Write-Output "Simulation: $($sim.displayName)"
    Write-Output "  Status: $($sim.status)"
    Write-Output "  Compromise Rate: $
($sim.report.simulationEventsContent.compromisedRate)%"
    Write-Output "  Click Rate: $($sim.report.simulationEventsContent.actualClickedRate)%"
    Write-Output "  Report Rate: $($sim.report.simulationEventsContent.reportedRate)%"
    Write-Output "---"
}
```

# 6. AIR : Automated Investigation and Response

## 6.1 Fonctionnement de l'investigation automatisee

AIR (Automated Investigation and Response) est la capacite d'investigation automatisee de Defender for Office 365 Plan 2. Lorsqu'une alerte de securite est generee (email de phishing detecte post-delivery, URL reclassifiee comme malveillante, piece jointe retrogradee), AIR declenche automatiquement une investigation qui analyse l'ensemble du scope d'impact : quels utilisateurs ont recu l'email, qui a clique sur les liens, quelles actions similaires existent dans le tenant.

L'investigation AIR suit un processus en plusieurs etapes : collecte des evidences (emails, URL, fichiers), correlation avec d'autres signaux (alertes Defender for Endpoint, connexions suspectes Entra ID), analyse des entites impliquees (expediteurs, domaines, IP), et generation de recommandations d'action (suppression d'emails, blocage d'URL, reset de mots de passe).



### 6.2 Configuration AIR

AIR peut fonctionner en deux modes : approbation manuelle (les actions recommandees sont presentees a l'analyste SOC qui les approuve ou les rejette) et approbation automatique (les actions sont executees sans intervention humaine). Pour la plupart des organisations, le mode semi-automatique est recommande pour les actions a faible risque (suppression d'emails de phishing) tandis que les actions a haut impact (reset de mot de passe, blocage de comptes) restent en approbation manuelle.

```
# Configurer les niveaux d'approbation AIR
# Via le portail Microsoft 365 Defender > Settings > Email & collaboration > AIR

# Verifier les investigations AIR recentes via Graph API
$investigations = Invoke-MgGraphRequest -Method GET `
    -Uri "https://graph.microsoft.com/v1.0/security/alerts_v2?`$filter=serviceSource eq
'microsoftDefenderForOffice365'" `
    -OutputType PSObject

foreach ($inv in $investigations.value) {
    Write-Output "Investigation: $($inv.title)"
    Write-Output "  Severity: $($inv.severity)"
    Write-Output "  Status: $($inv.status)"
    Write-Output "  Created: $($inv.createdDateTime)"
    Write-Output "  Category: $($inv.category)"
    Write-Output "---"
}

# Lister les actions de remediation en attente d'approbation
$pendingActions = Invoke-MgGraphRequest -Method GET `
    -Uri "https://graph.microsoft.com/v1.0/security/alerts_v2?`$filter=status eq
'inProgress' and serviceSource eq 'microsoftDefenderForOffice365'" `
    -OutputType PSObject

Write-Output "$($pendingActions.value.Count) actions en attente d'approbation"
```

## 7. Monitoring et KPIs de Securite Email

### 7.1 Dashboard de securite email

Un tableau de bord de securite email efficace doit couvrir les metriques suivantes, mises a jour quotidiennement et revues en comite de securite hebdomadaire :

| KPI | Description | Seuil d'alerte | Source |
|---|---|---|---|
| **Phish Catch Rate** | % d'emails de phishing bloques avant delivery | < 95 % | Threat Explorer |
| **Post-Delivery Removals** | Emails supprimes par ZAP apres delivery | > 50/jour | EmailPostDeliveryEvents |
| **Safe Links Blocks** | URL bloquees par Safe Links (clics) | Tendance haussiere | UrlClickEvents |
| **User Report Rate** | % d'emails phishing signales par les utilisateurs | < 20 % | User submissions |
| **BEC Attempts** | Tentatives de Business Email Compromise detectees | Toute occurrence | Anti-phishing policy |
| **Simulation Compromise Rate** | Taux de compromission dans les simulations | > 10 % | Attack Simulation |
| **AIR Actions Pending** | Actions de remediation en attente | > 5 depuis 4h | AIR dashboard |

## 7.2 Integration avec Microsoft Sentinel

L'integration de Defender for Office 365 avec Microsoft Sentinel via le connecteur natif permet de correler les alertes email avec l'ensemble du contexte de securite : connexions suspectes Entra ID, alertes Defender for Endpoint, activites anormales dans SharePoint ou Teams. Cette correlation est essentielle pour detecter les chaines d'attaque completes : phishing initial → credential compromise → lateral movement → data exfiltration.

```
// Sentinel : correler phishing et connexion suspecte
let phishAlerts = SecurityAlert
| where TimeGenerated > ago(24h)
| where ProductName == "Microsoft Defender for Office 365"
| where AlertName has "phish"
| extend TargetUser = tostring(parse_json(ExtendedProperties).["Users"])
| project PhishTime=TimeGenerated, TargetUser, AlertName;

let suspiciousSignIns = SigninLogs
| where TimeGenerated > ago(24h)
| where ResultType == 0  // successful login
| where RiskLevelDuringSignIn in ("medium", "high")
| project SignInTime=TimeGenerated, UserPrincipalName, IPAddress, Location;

phishAlerts
| join kind=inner suspiciousSignIns on $left.TargetUser == $right.UserPrincipalName
| where SignInTime between (PhishTime .. PhishTime + 4h)
| project PhishTime, SignInTime, TargetUser, AlertName, IPAddress, Location
```

## 8. Liens avec d'Autres Domaines de Securite

La protection anti-phishing ne fonctionne pas en isolation. Elle s'integre dans un ecosysteme de securite plus large couvrant l'ingenierie sociale, la protection des endpoints, et la securite de la supply chain. Voici les articles complementaires :

- Phishing sans piece jointe : les techniques de phishing modernes qui contournent Safe Attachments en utilisant des liens, du HTML smuggling, et des QR codes. Comprendre ces techniques pour mieux configurer les policies Defender.
- Infostealers : la menace silencieuse : les infostealers deployes via des pieces jointes email volent les credentials, cookies et tokens de session. Safe Attachments et Safe Documents sont la premiere ligne de defense.
- Exploitation des protocoles email et SMTP smuggling : les techniques d'exploitation au niveau protocole (SMTP smuggling, header injection) qui peuvent contourner les filtres anti-spam et anti-phishing.
- Supply chain applicative : les attaques de supply chain passant par des emails de mise a jour logicielle compromis ou des newsletters d'editeurs pirates.
- Evasion EDR/XDR : les techniques d'evasion utilisees par les payloads livrees par email pour echapper a la detection sur les endpoints apres avoir contourne Safe Attachments.
- C2 Frameworks : Mythic, Havoc, Sliver : les frameworks de Command & Control utilises apres une compromission initiale par phishing. Comprendre la chaine post-exploitation pour mieux prioriser la detection email.

Pour approfondir ce sujet, consultez notre outil open-source exchange-security-checker qui facilite la vérification de la sécurité Exchange Online.

## Questions frequentes

### Comment mettre en place Microsoft Defender for Office 365 dans un environnement de production ?

La mise en place de Microsoft Defender for Office 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 Microsoft Defender for Office 365 est-il essentiel pour la securite des systemes d'information ?

Microsoft Defender for Office 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.

### Quelles sont les bonnes pratiques pour Microsoft Defender for Office 365 en 2026 ?

Les bonnes pratiques pour Microsoft Defender for Office 365 en 2026 incluent l'adoption d'une approche Zero Trust, l'automatisation des controles de securite, la mise en place d'une veille continue sur les vulnerabilites et l'integration des recommandations des organismes de reference comme l'ANSSI et le NIST.

**Sources et références :** Microsoft Security Docs · CERT-FR

> Points clés à retenir
>
> - 2. Safe Links : Protection des URL en Temps Reel
> - 3. Safe Attachments : Sandbox et Dynamic Delivery
> - 4. Threat Explorer et Hunting Avance
> - 5. Attack Simulation Training
> - 6. AIR : Automated Investigation and Response
> - 7. Monitoring et KPIs de Securite Email

## Conclusion

Microsoft Defender for Office 365 est une plateforme de protection email mature et comprehensive, mais sa valeur depend entierement de la qualite de sa configuration. Les parametres par defaut offrent une protection de base insuffisante face aux menaces actuelles. La configuration avancee presentee dans cet article -- seuils anti-phishing agressifs, Safe Links sans click-through, Safe Attachments en Dynamic Delivery, hunting KQL proactif, simulations regulieres et AIR semi-automatise -- transforme Defender en une veritable forteresse anti-phishing.

L'approche recommandee est iterative : commencez par deployer les policies anti-phishing avec des seuils moderes, puis augmentez progressivement l'agressivite en analysant les faux positifs dans la quarantaine. Lancez les simulations de phishing des le premier mois pour etablir une baseline, puis mesurez l'amelioration trimestre apres trimestre. Integrez les alertes Defender dans votre SIEM pour une visibilite transverse.

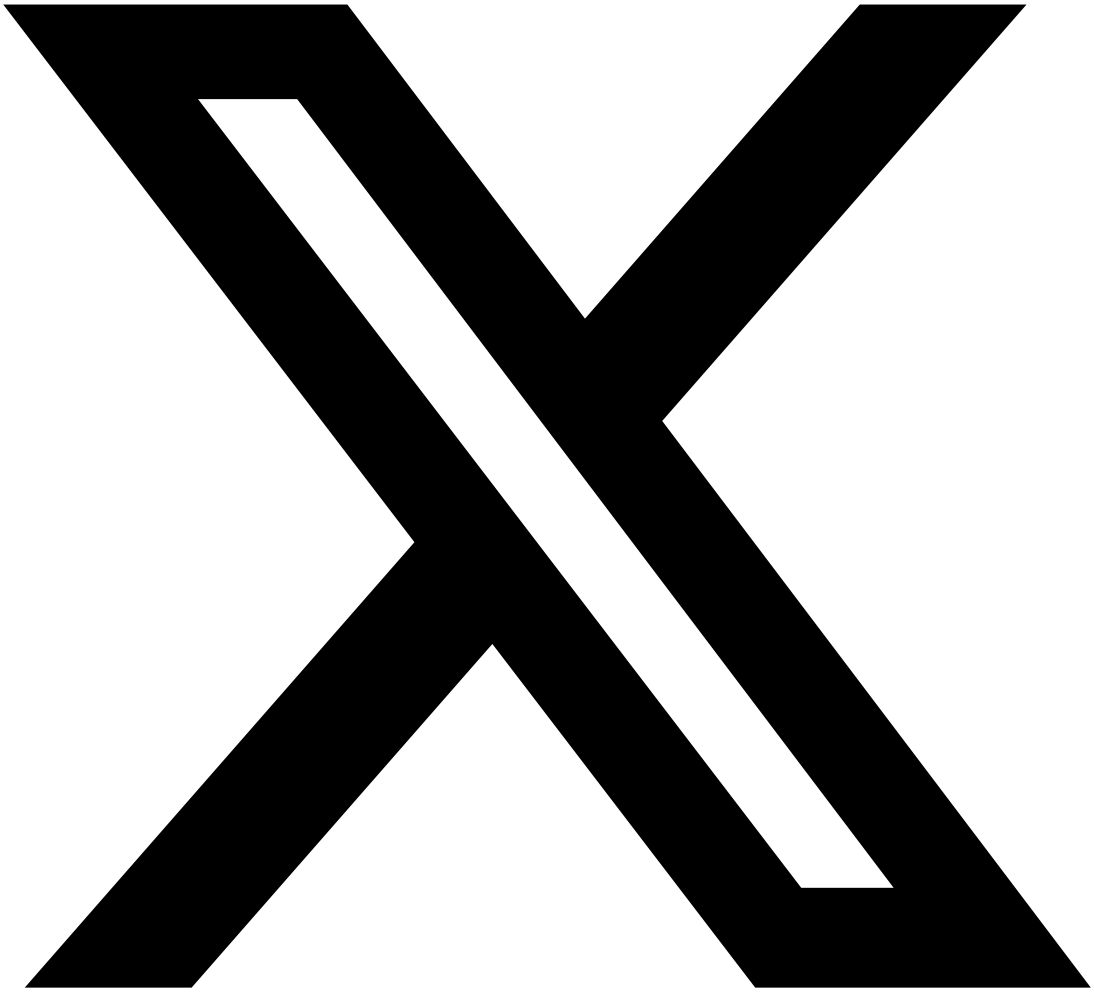
Rappelons que la technologie ne suffit pas. Les utilisateurs restent le maillon le plus expose de la chaine de securite email. Un programme de sensibilisation continu, couple aux simulations Attack Simulation Training et a un processus de signalement d'email suspect simple et rapide (bouton "Report Phishing" dans Outlook), est indispensable. L'objectif final n'est pas d'atteindre zero clic sur les emails de phishing -- c'est illusoire -- mais de reduire le temps entre la reception d'un email malveillant et sa detection/remediation a quelques minutes, grace a la combinaison de l'automatisation AIR et de la vigilance des utilisateurs formes.

Enfin, gardez a l'esprit que Defender for Office 365 n'est qu'un composant de la securite Microsoft 365. La protection email doit etre completee par une securite des identites robuste (Conditional Access, passwordless authentication), une securite des donnees (DLP, Sensitivity

Labels sur SharePoint), et une detection comportementale (Defender for Cloud Apps, Sentinel). Seule cette approche holistique permet de contrer les attaques multi-vecteurs qui commencent par un email de phishing et se terminent par une exfiltration de donnees ou un ransomware.

## Partagez cet Article

Cet article vous a ete utile ? Partagez-le avec votre reseau professionnel !

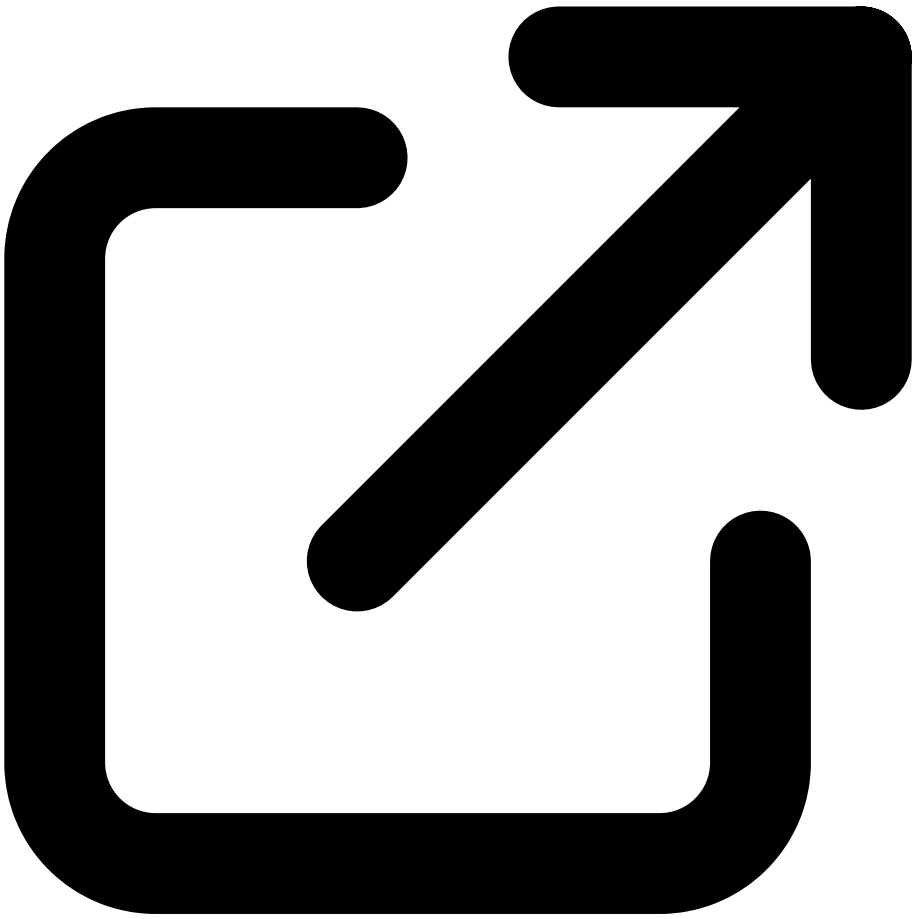


Partager sur X

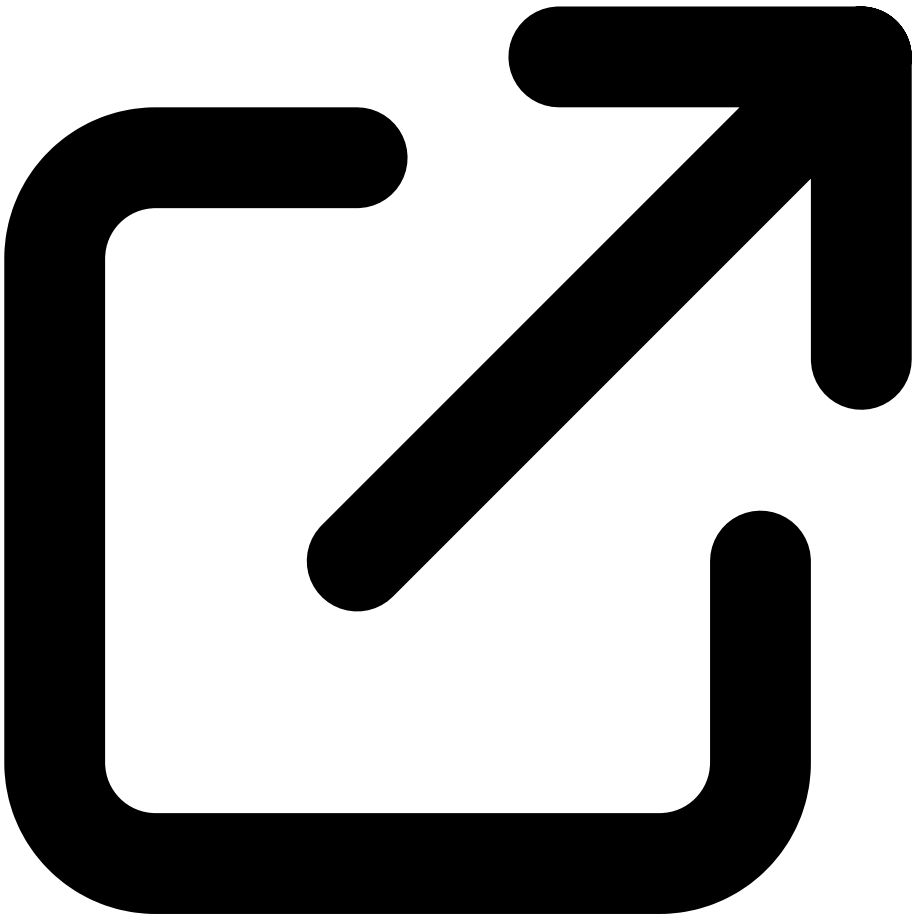
Partager sur LinkedIn

## Ressources & References Officielles

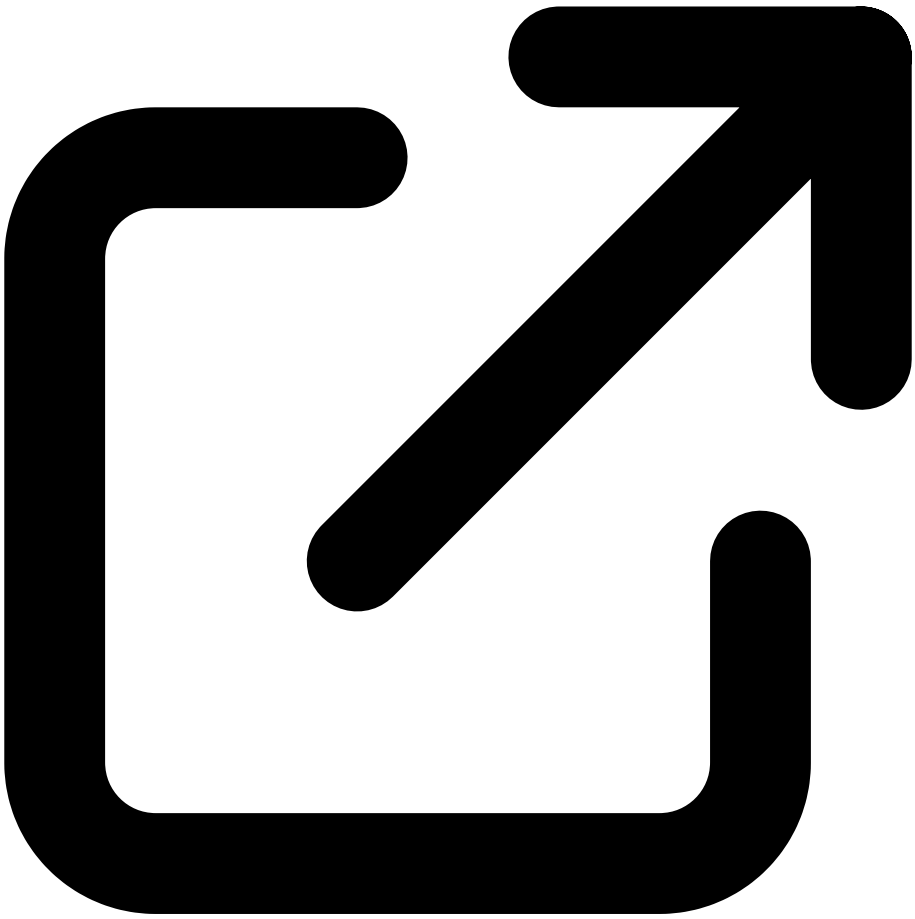
Documentations officielles et ressources de la communaute



Microsoft - Anti-Phishing Policies
learn.microsoft.com



Microsoft - Safe Links
learn.microsoft.com



Microsoft - Automated Investigation (AIR)
learn.microsoft.com

## Ayi NEDJIMI

Expert en Cybersecurite & Intelligence Artificielle

Consultant senior avec plus de 15 ans d'experience en securite offensive, audit d'infrastructure et developpement de solutions IA. Certifie OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer. Intervient sur des missions de pentest Active Directory, securite Cloud et conformite reglementaire pour des grands comptes et ETI.

LinkedIn Profil complet Tous ses articles

## References et ressources externes


- Microsoft Defender for Office 365 Overview -- Documentation officielle complete
- Microsoft - Recommended Settings -- Parametres recommandes par Microsoft (Strict/ Standard)
- MITRE ATT&CK T1566 - Phishing -- Tactiques et techniques de phishing documentees
- Verizon DBIR -- Data Breach Investigations Report annuel



**Ayi NEDJIMI Consultants** — Expert cybersécurité offensive & intelligence artificielle

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