AYI NEDJIMI Consultants

Durcissement Exchange Online : Bloquer Basic Auth et

Catégorie : Microsoft 365 Lecture : 9 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide de durcissement Exchange Online : désactivation Basic Auth, anti-phishing, Safe Links, Safe Attachments, SPF/DKIM/DMARC et protection contre le.

Ce guide technique de durcissement couvre l'ensemble des mesures essentielles pour securiser Exchange Online : de la desactivation de l'authentification basique (Basic Auth) a la mise en place de politiques anti-phishing avancees avec Microsoft Defender for Office 365, en passant par la configuration complete de SPF, DKIM et DMARC, la protection contre les fraudes BEC, les regles de transport et de prevention des fuites de donnees (DLP), et le monitoring continu des flux de messagerie. Guide de durcissement Exchange Online : désactivation Basic Auth, anti-phishing, Safe Links, Safe Attachments, SPF/DKIM/DMARC et protection contre le. Ce guide couvre les aspects essentiels de durcissement exchange online anti phishing : méthodologie structurée, outils recommandés et retours d'expérience opérationnels. Les professionnels y trouveront des recommandations directement applicables.

L'objectif est de fournir aux administrateurs Microsoft 365, aux equipes SOC et aux RSSI un plan d'action concret et progressif, avec des commandes PowerShell pretes a l'emploi, des configurations detaillees et une checklist de validation en 15 points. Chaque section articule la menace, la mesure de protection et la verification de la mise en oeuvre.

Prerequis

Ce guide suppose un tenant Microsoft 365 avec au minimum des licences Microsoft 365 Business Premium ou Microsoft Defender for Office 365 Plan 2. Les commandes PowerShell necessitent le module `ExchangeOnlineManagement` v3+ et les droits Global Administrator ou Security Administrator.

Avant de plonger dans les configurations techniques, il est utile de comprendre la chaine d'attaque typique par email. Un attaquant envoie un message contenant soit un lien vers un site de phishing (voir notre article sur le phishing sans piece jointe), soit une piece jointe malveillante, soit une combinaison des deux. Le message peut exploiter des techniques de SMTP smuggling pour contourner les filtres. L'objectif final est souvent le vol d'identifiants, l'installation d'un infostealer, ou l'etablissement d'une persistance dans le tenant Microsoft 365.

```
# Creation d'une politique Conditional Access bloquant les clients legacy
# Via le portail Entra ID :
# 1. Entra ID > Protection > Conditional Access > New Policy
# 2. Name : "Block Legacy Authentication"
# 3. Users : All users (exclure un break-glass account)
# 4. Cloud apps : All cloud apps
# 5. Conditions > Client apps > Configure: Yes
#    - Exchange ActiveSync clients : Checked
#    - Other clients : Checked
#    - (Decocher Browser et Mobile apps)
# 6. Grant : Block access
# 7. Enable policy : On

# Verification via PowerShell (module Microsoft.Graph)
Connect-MgGraph -Scopes "Policy.Read.All"
Get-MgIdentityConditionalAccessPolicy |
    Where-Object { $_.DisplayName -like "*Legacy*" -or $_.DisplayName -like "*Basic*" } |
    Select-Object DisplayName, State, CreatedDateTime
```

2.4 Authentication Policies Exchange Online

En complement du Conditional Access, configurez des Authentication Policies directement dans Exchange Online pour une defense en profondeur :

```
# Creer une politique bloquant tous les protocoles legacy
New-AuthenticationPolicy -Name "Block-Basic-Auth-All" `
    -AllowBasicAuthActiveSync:$false `
    -AllowBasicAuthAutodiscover:$false `
    -AllowBasicAuthImap:$false `
    -AllowBasicAuthMapi:$false `
    -AllowBasicAuthOfflineAddressBook:$false `
    -AllowBasicAuthOutlookService:$false `
    -AllowBasicAuthPop:$false `
    -AllowBasicAuthPowerShell:$false `
    -AllowBasicAuthReportingWebServices:$false `
    -AllowBasicAuthRpc:$false `
    -AllowBasicAuthSmtp:$false `
    -AllowBasicAuthWebServices:$false

# Appliquer comme politique par defaut du tenant
Set-OrganizationConfig -DefaultAuthenticationPolicy "Block-Basic-Auth-All"

# Verifier l'application
Get-OrganizationConfig | Select-Object DefaultAuthenticationPolicy
```

Bonnes pratiques pour la migration

- Commencez par activer la politique en mode **Report-Only** dans Conditional Access pendant 2 a 4 semaines pour identifier les impacts.
- Migrez les applications legacy vers OAuth 2.0 (SMTP OAuth, EWS avec tokens bearer).
- Pour les imprimantes et peripheriques ne supportant pas OAuth, utilisez un relais SMTP authentifie (connecteur Direct Send ou SMTP relay).
- Conservez un compte break-glass exclu de toutes les politiques, protege par FIDO2 et supervise en temps reel.

- Documentez chaque exception avec un proprietaire, une date de revue et un plan de migration.

2.5 Verification et monitoring continu

Apres la desactivation, surveillez en continu les tentatives de connexion Basic Auth pour detecter des contournements ou des applications non migrees :

```
# Alerte dans Microsoft Sentinel (KQL)
SigninLogs
| where TimeGenerated > ago(24h)
| where ClientAppUsed in ("Exchange ActiveSync", "IMAP4",
    "MAPI Over HTTP", "Offline Address Book",
    "Other clients", "POP3", "SMTP")
| where ResultType == 0  // Connexions reussies uniquement
| summarize Count=count() by UserPrincipalName, ClientAppUsed,
    IPAddress, Location=tostring(LocationDetails.city)
| where Count > 0
| order by Count desc
```

Savez-vous quelles applications tierces ont accès aux données de votre tenant ?

Le parametre `AllowClickThrough $false` est critique : il empeche les utilisateurs de contourner l'avertissement et d'acceder quand meme a une URL detectee comme malveillante. Le parametre `DeliverMessageAfterScan $true` retient le message jusqu'a ce que l'analyse des URL soit terminee, eliminant la fenetre de vulnerabilite entre la livraison et l'analyse.

3.5 Safe Attachments : sandbox dynamique

Safe Attachments ouvre chaque piece jointe dans un environnement sandbox isole pour detecter les comportements malveillants, meme pour des malwares zero-day inconnus des signatures antivirus :

```
# Configurer Safe Attachments
New-SafeAttachmentPolicy -Name "Strict-SafeAttach" `
    -Enable $true `
    -Action DynamicDelivery `
    -QuarantineTag DefaultFullAccessPolicy `
    -ActionOnError $true `
    -Redirect $false

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

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

Le mode `DynamicDelivery` est recommande : il livre immediatement le corps du message a l'utilisateur avec un placeholder pour la piece jointe, puis remplace le placeholder par la piece jointe reelle une fois l'analyse sandbox terminee. Cela minimise l'impact sur la productivite tout en maintenant la protection.

3.6 Zero-hour Auto Purge (ZAP)

ZAP est un mecanisme retroactif qui supprime automatiquement les messages deja livres dans les boites de reception lorsqu'un verdique ulterieur les identifie comme malveillants. Cela couvre le scenario ou un email passe les filtres initiaux mais est ensuite detecte comme phishing grace a de nouvelles signatures ou a l'intelligence collective du reseau Microsoft :

```
# Verifier que ZAP est active (il l'est par defaut)
Get-MalwareFilterPolicy | Select-Object Name, ZapEnabled
Get-HostedContentFilterPolicy | Select-Object Name,
    ZapEnabled, PhishZapEnabled, SpamZapEnabled

# S'assurer que ZAP n'est pas desactive
Set-HostedContentFilterPolicy -Identity Default `
    -ZapEnabled $true `
    -PhishZapEnabled $true `
    -SpamZapEnabled $true
```

Point cle : ZAP
ZAP fonctionne sur les messages deja livres dans la boite de reception ou le dossier Junk. Il ne fonctionne pas si l'utilisateur a deja lu et deplace le message dans un autre dossier, ou si une regle de boite mail a deplace le message. Formez vos utilisateurs a ne pas creer de regles qui deplacent automatiquement les emails suspects vers des dossiers personnalises.

```
# Etape 1 : Recuperer les enregistrements CNAME a creer
Get-DkimSigningConfig -Identity contoso.com |
    Select-Object Domain, Selector1CNAME, Selector2CNAME

# Etape 2 : Creer les enregistrements CNAME dans votre DNS
# selector1._domainkey.contoso.com  CNAME
#   selector1-contoso-com._domainkey.contoso.onmicrosoft.com
# selector2._domainkey.contoso.com  CNAME
#   selector2-contoso-com._domainkey.contoso.onmicrosoft.com

# Etape 3 : Activer DKIM apres propagation DNS (24-48h)
Set-DkimSigningConfig -Identity contoso.com -Enabled $true

# Etape 4 : Verification
Get-DkimSigningConfig -Identity contoso.com |
    Select-Object Domain, Enabled, Status,
    Selector1CNAME, Selector2CNAME, LastChecked

# Rotation des cles DKIM (recommandee tous les 6-12 mois)
Rotate-DkimSigningConfig -KeySize 2048 -Identity contoso.com
```

4.4 Deploiement progressif de DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) est la piece maitresse qui articule SPF et DKIM. Il definit la politique que le serveur recepteur doit appliquer lorsqu'un email echoue a l'authentification, et fournit des rapports sur les tentatives d'usurpation. Le deploiement doit etre progressif pour eviter de bloquer des emails legitimes :

```
# Phase 1 : Mode monitoring (4 a 8 semaines)
# Collecte des rapports sans impact sur la delivrabilite
_dmarc.contoso.com  TXT  "v=DMARC1; p=none; rua=mailto:dmarc-agg@contoso.com;
ruf=mailto:dmarc-fail@contoso.com; fo=1"

# Phase 2 : Quarantine progressif (4 semaines)
# 25% des emails non authentifies sont mis en quarantaine
_dmarc.contoso.com  TXT  "v=DMARC1; p=quarantine; pct=25; rua=mailto:dmarc-
agg@contoso.com; ruf=mailto:dmarc-fail@contoso.com; fo=1"

# Phase 3 : Quarantine complet (4 semaines)
_dmarc.contoso.com  TXT  "v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc-
agg@contoso.com; ruf=mailto:dmarc-fail@contoso.com; fo=1"

# Phase 4 : Reject (objectif final)
# Tous les emails non authentifies sont rejetes
_dmarc.contoso.com  TXT  "v=DMARC1; p=reject; pct=100; rua=mailto:dmarc-agg@contoso.com;
ruf=mailto:dmarc-fail@contoso.com; fo=1; adkim=s; aspf=s"
```

Les parametres `adkim=s` et `aspf=s` imposent un alignement strict (le domaine du From: doit correspondre exactement au domaine SPF/DKIM, pas seulement au domaine parent). C'est la configuration la plus securisee mais elle peut bloquer des sous-domaines legitimes non declares.

4.5 Analyseurs et outils de suivi DMARC

Les rapports DMARC agreges (RUA) sont au format XML et peuvent representer des volumes importants. Utilisez un outil d'analyse pour les interpreter efficacement :

Outil	Type	Fonctionnalites cles
DMARC Analyzer (Mimecast)	SaaS payant	Dashboard, alertes, assistant deploiement
Valimail	SaaS payant	Automatisation SPF/DKIM, rapports avances
dmarcian	SaaS (free tier)	Visualisation rapports, timeline
PowerDMARC	SaaS payant	TI integration, BIMI support
parsedmarc (open-source)	Self-hosted	Parser Python, export Elasticsearch/Splunk
MXToolbox	Freemium	Verification DNS, monitoring SPF/DKIM/DMARC

Conseil : BIMI (Brand Indicators for Message Identification)
Une fois DMARC en mode `p=reject` ou `p=quarantine`, vous pouvez deployer BIMI pour afficher le logo de votre organisation dans les clients mail supportes (Gmail, Apple Mail, Yahoo). BIMI renforce la confiance des destinataires et reduit l'efficacite du phishing utilisant votre marque. Il necessite un certificat VMC (Verified Mark Certificate) delivre par DigiCert ou Entrust.

```
# Via le portail Microsoft Purview Compliance :
# 1. Compliance Portal > Data Loss Prevention > Policies
# 2. Create Policy > Custom policy
# 3. Name : "DLP-RGPD-Email-Protection"
# 4. Locations : Exchange email
# 5. Conditions : Content contains sensitive info types :
#    - France National ID Card (CNI)
#    - France Social Security Number (NIR)
#    - Credit Card Number
#    - IBAN (International Bank Account Number)
#    - EU Passport Number
#    - EU Driver's License Number
# 6. Actions :
#    - Low volume (1-9) : Notify user + encrypt email
#    - High volume (10+) : Block sending + notify admin
# 7. User notifications : On (policy tip in Outlook)
# 8. Override : Allow with business justification

# Verification des politiques DLP actives
Get-DlpCompliancePolicy | Select-Object Name, Mode,
    Enabled, ExchangeLocation | Format-Table

# Rapport des incidents DLP
Get-DlpDetailReport -StartDate (Get-Date).AddDays(-30) `
    -EndDate (Get-Date) |
    Group-Object PolicyName, SensitiveInformationType |
    Select-Object Name, Count
```

6.4 Etiquettes de confidentialite (Sensitivity Labels)

Les etiquettes de confidentialite Microsoft Information Protection (MIP) permettent de classifier et proteger les emails selon leur niveau de sensibilite. Combinees aux politiques DLP, elles offrent une protection granulaire et automatisee :

- **Public** : aucune restriction, l'email peut etre envoye a l'exterieur sans chiffrement.
- **Interne** : avertissement lors de l'envoi externe, pas de chiffrement force.
- **Confidentiel** : chiffrement automatique (Azure RMS), restriction des droits (pas de transfert, pas de copie, expiration).
- **Hautement confidentiel** : chiffrement force, pas de transfert possible, filigrane "CONFIDENTIEL" sur les pieces jointes, revocation possible par l'expediteur.

```
# Activer le chiffrement automatique pour l'etiquette "Confidentiel"
# Via PowerShell (module Security & Compliance)
Connect-IPPSSession

# Politique d'auto-labeling pour les emails contenant des IBAN
New-AutoSensitivityLabelPolicy -Name "AutoLabel-IBAN-Confidential" `
    -ExchangeLocation All `
    -ApplySensitivityLabel "Confidentiel" `
    -Mode Enforce

New-AutoSensitivityLabelRule -Name "Rule-IBAN-Detection" `
    -Policy "AutoLabel-IBAN-Confidential" `
    -ContentContainsSensitiveInformation @{
        Name = "International Banking Account Number (IBAN)";
        MinCount = 1
    }
```

Integration avec la Supply Chain

Les etiquettes de confidentialite protegent egalement contre les risques lies a la supply chain applicative : un email confidentiel chiffre avec Azure RMS ne peut pas etre lu par un tiers, meme s'il est intercepte ou redirige. La protection suit le document, pas le canal de transmission.

7.3 Integration SIEM et regles de detection

L'integration des logs Exchange Online dans un SIEM (Microsoft Sentinel, Splunk, Elastic) est essentielle pour la detection proactive des menaces et la correlation avec d'autres sources de telemetrie. Les principaux evenements a surveiller sont les suivants :

```
# ===== MICROSOFT SENTINEL - KQL Queries =====

# 1. Detection de creation de regles de transfert suspectes
OfficeActivity
| where TimeGenerated > ago(24h)
| where Operation in ("New-InboxRule", "Set-InboxRule", "Enable-InboxRule")
| where Parameters has_any ("ForwardTo", "ForwardAsAttachmentTo", "RedirectTo")
| project TimeGenerated, UserId, Operation, Parameters, ClientIP
| extend ForwardTarget = extract(@'"ForwardTo":\s*"([^"]+)"', 1, Parameters)

# 2. Vague de phishing (meme expediteur ciblant plusieurs utilisateurs)
EmailEvents
| where TimeGenerated > ago(1h)
| where ThreatTypes has "Phish"
| summarize TargetCount=dcount(RecipientEmailAddress),
    Targets=make_set(RecipientEmailAddress) by SenderFromAddress
| where TargetCount > 5
| order by TargetCount desc

# 3. Connexion depuis un pays inhabituel apres reception de phishing
let PhishRecipients = EmailEvents
    | where TimeGenerated > ago(24h)
    | where ThreatTypes has "Phish" and DeliveryAction == "Delivered"
    | distinct RecipientEmailAddress;
SigninLogs
| where TimeGenerated > ago(24h)
| where UserPrincipalName in (PhishRecipients)
| where Location !in ("FR", "BE", "CH")  // Pays attendus
| project TimeGenerated, UserPrincipalName, Location,
    IPAddress, AppDisplayName, ResultType

# 4. Volume anormal d'emails sortants (exfiltration potentielle)
EmailEvents
| where TimeGenerated > ago(24h)
| where EmailDirection == "Outbound"
| summarize EmailCount=count(),
    UniqueRecipients=dcount(RecipientEmailAddress) by SenderFromAddress,
bin(TimeGenerated, 1h)
| where EmailCount > 100 or UniqueRecipients > 50

# 5. Modification des permissions de boite mail
OfficeActivity
| where TimeGenerated > ago(24h)
| where Operation in ("Add-MailboxPermission", "Add-RecipientPermission",
    "Set-Mailbox", "Add-MailboxFolderPermission")
| project TimeGenerated, UserId, Operation, Parameters, ClientIP
```

7.4 Alertes et rapports automatises

Configurez des alertes automatisees dans Microsoft Defender pour les evenements critiques. Les attaquants utilisent souvent des techniques de tunneling DNS pour exfiltrer les donnees collectees via les emails compromis, ce qui rend la correlation multi-sources indispensable :

- **Email detected as phishing post-delivery** : alerte haute priorite lorsque ZAP detecte un phishing deja livre.
- **Email messages containing phish URLs removed after delivery** : suivi de l'efficacite de ZAP.

- **Suspicious email forwarding activity** : creation ou modification de regles de transfert externe.
- **Unusual volume of email reported as phishing** : pic de signalements utilisateurs indiquant une campagne en cours.
- **User impersonation detected** : tentative d'usurpation d'identite des utilisateurs proteges.
- **Tenant Allow/Block List modification** : modification des listes d'autorisation/blocage pouvant indiquer une compromission admin.

8. Checklist de durcissement Exchange Online en 15 points

Utilisez cette checklist comme reference pour valider la securite de votre tenant Exchange Online. Chaque point correspond a une mesure detaillee dans les sections precedentes. Cochez les elements au fur et a mesure de leur implementation :

#	Mesure de durcissement	Priorite	Statut
1	Basic Auth desactivee via Conditional Access (tous les protocoles legacy bloques)	Critique	[ ]
2	Authentication Policy Exchange "Block-Basic-Auth-All" appliquee comme defaut du tenant	Critique	[ ]
3	Politique anti-phishing avec PhishThresholdLevel 3 ou 4 et impersonation protection active	Critique	[ ]
4	Utilisateurs VIP (CEO, CFO, DRH) proteges contre l'impersonation (TargetedUserProtection)	Critique	[ ]
5	Safe Links active avec AllowClickThrough $false et DeliverMessageAfterScan $true	Critique	[ ]
6	Safe Attachments en mode DynamicDelivery avec sandbox pour SPO/OneDrive/ Teams	Critique	[ ]
7	SPF configure avec -all (hard fail) et moins de 10 lookups DNS	Critique	[ ]
8	DKIM active avec rotation des cles planifiee (6-12 mois)	Critique	[ ]
9	DMARC en mode p=reject (ou p=quarantine minimum) avec rapports RUA actifs	Haute	[ ]
10	Transfert automatique externe bloque (RemoteDomain + Transport Rule)	Critique	[ ]
11	Tag [EXTERNE] actif sur tous les emails entrants depuis l'exterieur	Haute	[ ]
12	Politiques DLP configurees pour les donnees sensibles (RGPD, cartes bancaires, IBAN)	Haute	[ ]
13	Etiquettes de confidentialite deployees avec chiffrement automatique pour "Confidentiel"	Moyenne	[ ]
14	Logs Exchange integres au SIEM avec regles de detection (forwarding, phishing, exfiltration)	Haute	[ ]
15	Simulations de phishing mensuelles avec Attack Simulation Training et suivi des metriques	Haute	[ ]

Plan de mise en oeuvre recommande

- **Semaine 1-2** : Points 1-2 (Basic Auth) + Points 7-8 (SPF/DKIM) -- fondations techniques.
- **Semaine 3-4** : Points 3-6 (Anti-phishing, Safe Links, Safe Attachments) -- protection active.
- **Semaine 5-8** : Point 9 (DMARC progressif) + Points 10-11 (Transport Rules) -- durcissement du flux.
- **Semaine 9-12** : Points 12-14 (DLP, Labels, SIEM) -- conformite et monitoring.
- **Continu** : Point 15 (Simulations de phishing) -- amelioration continue.

Pour approfondir ce sujet, consultez notre outil open-source m365-security-audit qui facilite l'audit de sécurité de l'environnement Microsoft 365.

Questions frequentes

Comment mettre en place Durcissement Exchange Online dans un environnement de production ?

La mise en place de Durcissement Exchange Online 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 Durcissement Exchange Online est-il essentiel pour la securite des systemes d'information ?

Durcissement Exchange Online 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.

Comment auditer la configuration de sécurité de Durcissement Exchange Online : Bloquer Basic Auth ?

Utilisez Microsoft Secure Score comme point de départ, puis complétez avec un audit CIS Benchmark pour Microsoft 365. Exportez la configuration via PowerShell pour une revue hors ligne.

Sources et références : Microsoft Security Docs · CERT-FR

> Points clés à retenir
>
> - 8. Checklist de durcissement Exchange Online en 15 points
> - Questions frequentes
> - 9. Conclusion

9. Conclusion

Le durcissement d'Exchange Online n'est pas un projet ponctuel mais un processus continu qui evolue avec les menaces. La desactivation de Basic Auth elimine une surface d'attaque majeure, les politiques anti-phishing avancees de Defender for Office 365 protegent contre les techniques d'usurpation les plus abouties, et la trinite SPF/DKIM/DMARC en mode reject constitue le standard de facto pour l'authentification email.

Cependant, la technologie ne represente qu'une partie de l'equation. Les attaques BEC les plus couteuses exploitent la confiance humaine, pas les failles techniques. La formation reguliere des utilisateurs via Attack Simulation Training, combinee a des processus de verification pour les operations sensibles (virements, modifications bancaires), est tout aussi importante que la configuration technique.

Enfin, le monitoring continu via l'integration SIEM et les alertes automatisees garantit que les mesures de protection restent efficaces dans la duree. Les attaquants adaptent constamment leurs techniques : les configurations statiques deviennent obsoletes. Revoyez votre posture de securite email trimestriellement, suivez les recommandations du Microsoft Secure Score, et testez regulierement vos defenses.

La securite email est un maillon essentiel de la chaine de confiance numerique. Un tenant Exchange Online correctement durci protege non seulement votre organisation, mais aussi vos partenaires, vos clients et l'ensemble de votre ecosysteme contre les attaques par email.

Articles connexes

Techniques de Hacking
Phishing sans piece jointe
Techniques modernes de phishing ne necessitant aucune piece jointe malveillante.
Techniques de Hacking
SMTP Smuggling
Exploitation des protocoles email et techniques de SMTP smuggling.
Techniques de Hacking
Attaques DNS
Tunneling DNS, hijacking et poisoning pour l'exfiltration de donnees.
Techniques de Hacking
Exfiltration furtive
Methodes d'exfiltration de donnees discretes et canaux couverts.
Techniques de Hacking
Infostealers
Les infostealers, menace silencieuse du cybercrime moderne.
Techniques de Hacking
Supply Chain applicative
Attaques sur la chaine d'approvisionnement logicielle et ses risques.

Ayi NEDJIMI

Expert en Cybersécurité & 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

Références et ressources externes

- Microsoft - Anti-phishing policies in Defender for Office 365 — Documentation officielle des politiques anti-phishing
- Microsoft - Safe Links in Defender for Office 365 — Documentation Safe Links
- Microsoft - Safe Attachments in Defender for Office 365 — Documentation Safe Attachments
- DMARC.org — Specification et ressources DMARC
- FBI IC3 Report 2023 — Statistiques sur les pertes BEC
- MITRE ATT&CK T1114 - Email Collection — Techniques de collecte email
- NCSC - Email Security — Guide du NCSC britannique sur la securite email

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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