AYI NEDJIMI Consultants

Microsoft Secure Score : Guide d'Optimisation de votre

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

Guide complet Microsoft Secure Score : comprendre le score, actions d'amélioration prioritaires, benchmarking, automatisation et stratégie.

Architecture et calcul du score

Le Secure Score est exprimé en pourcentage et repose sur un système de points. Chaque **action d'amélioration** (improvement action) possède un nombre de points maximum, reflétant son impact sur la posture globale. Le score se calcule ainsi : Guide complet Microsoft Secure Score : comprendre le score, actions d'amélioration prioritaires, benchmarking, automatisation et stratégie. Microsoft 365 est omniprésent en entreprise et sa surface d'attaque ne cesse de s'étendre. La sécurisation de microsoft secure score optimisation posture nécessite une approche structurée et des outils adaptés. Nous abordons notamment : stratégie d'optimisation : quick wins, medium et long-terme, automatisation et apis et gouvernance et reporting. 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.

```
Score (%) = (Points obtenus / Points maximum possibles) x 100
```

Les points maximum dépendent des licences activées sur le tenant. Un tenant avec E5 aura plus d'actions disponibles (donc plus de points possibles) qu'un tenant E3. Cela signifie que le pourcentage reste comparable entre organisations de tailles et licences différentes.

Les cinq catégories

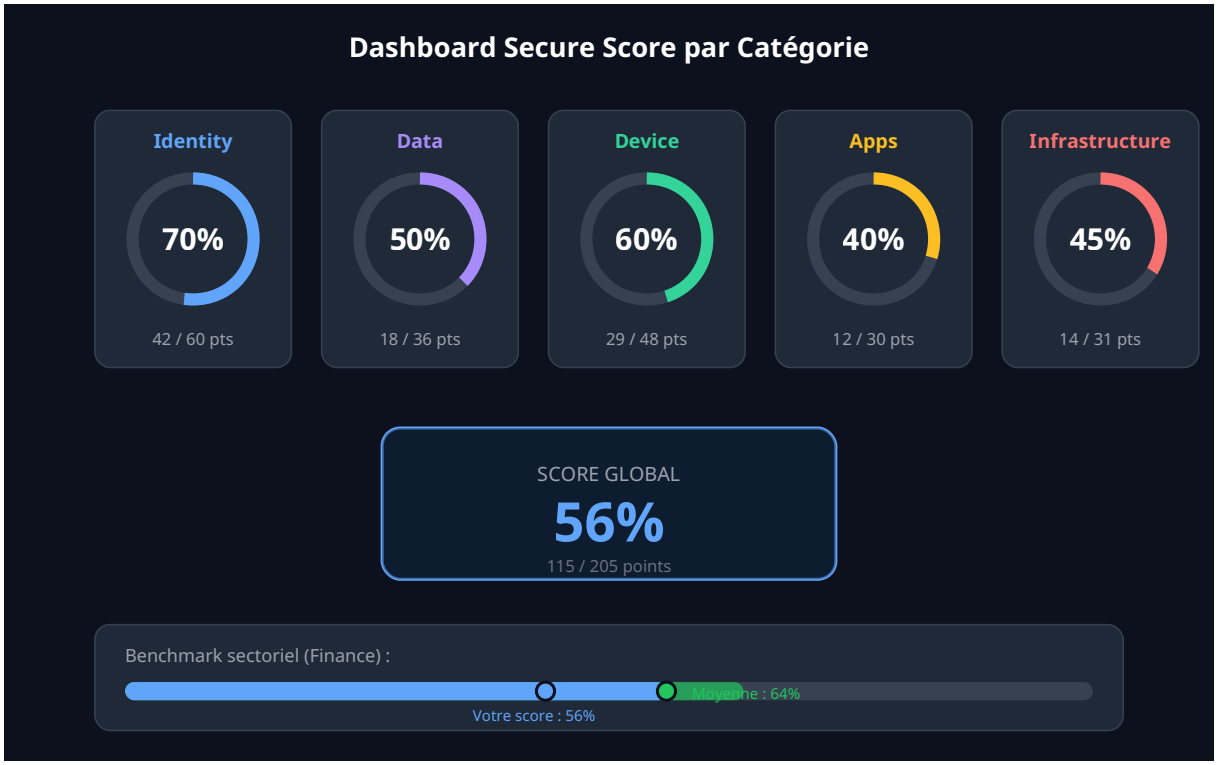
Microsoft organise les actions d'amélioration en cinq catégories principales, chacune couvrant un domaine de sécurité distinct :

Catégorie	Périmètre	Poids typique	Exemples d'actions
Identity	Entra ID, authentification, accès	~35%	MFA, Conditional Access, PIM
Data	Protection de l'information	~15%	DLP, sensitivity labels, encryption
Device	Postes, endpoints	~20%	Intune compliance, BitLocker, ASR
Apps	Applications cloud	~15%	OAuth app governance, shadow IT
Infrastructure	Azure, réseau, serveurs	~15%	NSG, Just-in-Time, Azure Firewall

Benchmarking et comparaison sectorielle

Microsoft fournit un **benchmark sectoriel** permettant de comparer votre score avec des organisations de taille et secteur similaires. En 2026, les benchmarks typiques observés sont :

- **Score moyen global** : 45-55% (la majorité des organisations n'exploitent pas tout le potentiel)
- **Secteur financier** : 55-70% (réglementations fortes type DORA)
- **Santé** : 40-55% (contraintes opérationnelles limitant certaines actions)
- **Organisations matures** : 75-85% (cible réaliste pour un programme structuré)
- **Score > 85%** : Rare, nécessite E5 + Defender for Endpoint + gouvernance stricte



10 **Activer Safe Links et Safe Attachments** (jusqu'a 5 points). Defender for Office 365 réécriture les URLs en temps réel (Safe Links) et détone les pièces jointes dans un sandbox (Safe Attachments). Activez ces protections pour Exchange, Teams et SharePoint.

Endpoints et Appareils

11 **Enroler les appareils dans Intune avec politiques de conformité** (jusqu'a 6 points). Définissez des politiques de conformité exigeant le chiffrement BitLocker, un antivirus actif, les mises à jour Windows à jour, et un code PIN minimal. Les appareils non conformes sont bloqués par Conditional Access.

12 **Activer Attack Surface Reduction (ASR) Rules** (jusqu'a 5 points). Les règles ASR de Defender for Endpoint bloquent les comportements malveillants courants : exécution de scripts obfusqués, création de processus enfants par les applications Office, exploitation WMI/PSExec. Déployez d'abord en mode audit puis en mode block. C'est un complément essentiel aux stratégies d'évasion EDR/XDR.

13 **Configurer Defender for Endpoint avec EDR activé** (jusqu'a 5 points). Enrolez tous les postes Windows, macOS et serveurs dans Defender for Endpoint. Activez l'EDR en mode block, le Tamper Protection et l'Automated Investigation & Response (AIR).

Applications et Cloud

14 **Déployer Microsoft Defender for Cloud Apps (MCAS)** (jusqu'a 4 points). MCAS offre une visibilité sur le shadow IT, le controle des sessions et la détection d'anomalies comportementales sur les applications SaaS connectées. Configurez les alertes pour les connexions depuis des pays inhabituels et les téléchargements massifs.

15 **Configurer les politiques d'accès conditionnel avancées** (jusqu'a 5 points). Au-dela du MFA basique, implémentez des politiques basées sur le risque utilisateur (Identity Protection), la conformité de l'appareil, la localisation réseau et le niveau de risque de la session. Exigez un appareil conforme pour accéder à SharePoint et Exchange.

Infrastructure et Réseau

16 **Activer les journaux d'audit unifiés** (jusqu'a 3 points). L'Unified Audit Log capture les activités dans Exchange, SharePoint, OneDrive, Teams, Entra ID et Defender. Configurez la rétention sur 1 an minimum (E5 permet 10 ans) et exportez vers un SIEM externe.

17 **Configurer les alertes Defender for Identity** (jusqu'a 4 points). Defender for Identity surveille Active Directory on-premises et détecte les attaques comme le pass-the-hash, le Kerberoasting et les mouvements latéraux. Installez les capteurs sur tous les contrôleurs de domaine.

18 **Configurer Azure AD Identity Protection** (jusqu'a 4 points). Activez les politiques de risque utilisateur et de risque de connexion. Configurez le blocage automatique ou la demande de MFA/changement de mot de passe pour les connexions à risque élevé.

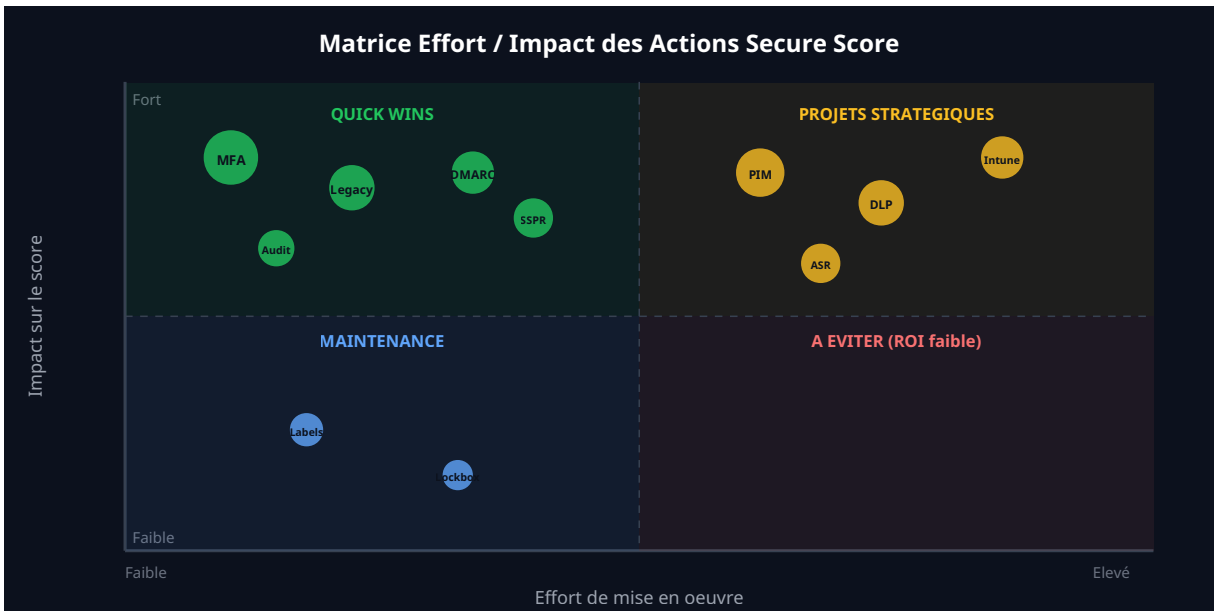
19 **Restreindre les rôles d'administration** (jusqu'a 3 points). Appliquez le principe du moindre privilège : maximum 5 Global Admins, utilisation de roles spécialisés (Exchange Admin, SharePoint Admin), et revue trimestrielle des attributions via Access Reviews.

20 **Activer le Customer Lockbox** (jusqu'a 2 points). Customer Lockbox exige votre approbation explicite avant que le support Microsoft n'accède à vos données. C'est une exigence pour de nombreuses certifications de conformité.

Avez-vous vérifié les permissions effectives de vos comptes de service Azure AD ?

Stratégie d'Optimisation : Quick Wins, Medium et Long-Terme

Une approche structurée en trois phases permet d'obtenir des résultats rapides tout en construisant une posture durable. La clé est de prioriser par **ratio effort/impact**, en commençant par les actions à fort gain et faible complexité.



Phase 1 : Quick Wins (Semaines 1-4) -- Gain : +15 a +25 points

Les Quick Wins sont des actions à faible effort et fort impact, réalisables en quelques heures ou jours sans perturbation majeure de la production :

- **MFA pour tous les admins** via Security Defaults ou Conditional Access (immédiat)
- **Bloquer Legacy Authentication** via Conditional Access (1 jour, après analyse des sign-in logs)
- **Configurer SPF/DKIM/DMARC** sur les domaines principaux (2-3 jours)
- **Activer les journaux d'audit unifiés** et configurer la rétention (immédiat)
- **Désactiver le consentement utilisateur aux applications** (immédiat, mais prévoir workflow admin consent)
- **Activer Safe Links et Safe Attachments** dans Defender for Office 365 (1 jour)

Phase 2 : Projets Structurés (Mois 2-3) -- Gain : +15 a +20 points

- **Déployer PIM** pour les roles Global Admin, Exchange Admin, Security Admin (nécessite P2)
- **Enroler les appareils dans Intune** avec politiques de conformité et Conditional Access basé sur l'appareil
- **Configurer les politiques DLP** pour Exchange, SharePoint et Teams (mode audit puis block)
- **Déployer Defender for Identity** sur les contrôleurs de domaine
- **Configurer Azure AD Identity Protection** avec politiques de risque automatisées
- **Activer les règles ASR** (Attack Surface Reduction) en mode audit puis block

Phase 3 : Maturité Avancée (Mois 4-12) -- Gain : +10 a +15 points

- **Sensitivity Labels avec auto-labelling** basé sur le contenu et le contexte
- **Defender for Cloud Apps** avec politiques de session et contrôle d'accès conditionnel aux applications SaaS

- **Access Reviews automatisées** trimestrielles pour les roles privilégiés et les groupes sensibles
- **Customer Lockbox** et gestion des clés client (BYOK)
- **Intégration SIEM/SOAR** avec Microsoft Sentinel pour la corrélation multi-source
- **Zero Trust complet** avec Continuous Access Evaluation (CAE) et Token Protection

Automatisation et APIs

Microsoft Graph API pour le Secure Score

L'API Microsoft Graph expose le Secure Score et les actions d'amélioration, permettant l'automatisation de la surveillance, du reporting et de la remédiation. Voici les endpoints clés :

```
# Récupérer le score actuel
GET https://graph.microsoft.com/v1.0/security/secureScores?$top=1

# Récupérer les actions d'amélioration
GET https://graph.microsoft.com/v1.0/security/secureScoreControlProfiles

# Récupérer l'historique du score (90 jours)
GET https://graph.microsoft.com/v1.0/security/secureScores?
$top=90&$orderby=createdDateTime desc
```

Script PowerShell d'audit automatisé

```
# Module Microsoft Graph PowerShell
Install-Module Microsoft.Graph.Security -Force
Connect-MgGraph -Scopes "SecurityEvents.Read.All"

# Récupérer le score actuel
$score = Get-MgSecuritySecureScore -Top 1
Write-Host "Score actuel: $($score.CurrentScore) / $($score.MaxScore)" -ForegroundColor
Cyan
Write-Host "Pourcentage: $([math]::Round(($score.CurrentScore / $score.MaxScore) * 100,
1))%"

# Lister les actions non implémentées triées par impact
$controls = Get-MgSecuritySecureScoreControlProfile
$notImplemented = $controls | Where-Object {
    $_.ImplementationStatus -ne "implemented"
} | Sort-Object MaxScore -Descending | Select-Object -First 20

$notImplemented | ForEach-Object {
    [PSCustomObject]@{
        Action     = $_.Title
        Impact     = "$($_.MaxScore) pts"
        Catégorie  = $_.ControlCategory
        Statut     = $_.ImplementationStatus
        Complexité = $_.UserImpact
    }
} | Format-Table -AutoSize

# Export CSV pour reporting
$notImplemented | Export-Csv -Path "SecureScore-Actions-$(Get-Date -Format yyyyMMdd).csv"
-NoTypeInformation -Encoding UTF8
```

Azure Workbooks pour le monitoring continu

Microsoft Sentinel propose des **Azure Workbooks** pré-construits pour visualiser l'évolution du Secure Score dans le temps. Vous pouvez créer un workbook personnalisé exploitant les données via le connecteur Microsoft 365 Defender :

```
// KQL - Evolution du Secure Score sur 90 jours
SecureScore
| where TimeGenerated > ago(90d)
| summarize Score=max(CurrentScore), MaxScore=max(MaxScore) by bin(TimeGenerated, 1d)
| extend Percentage = round(todouble(Score) / todouble(MaxScore) * 100, 1)
| project TimeGenerated, Score, MaxScore, Percentage
| order by TimeGenerated asc
| render timechart with (title="Evolution du Secure Score")
```

Pour aller plus loin dans l'automatisation, configurez des **Logic Apps** déclenchées par la baisse du score sous un seuil défini. L'alerte peut créer automatiquement un ticket ServiceNow ou envoyer une notification Teams au SOC avec les actions impactées.

Gouvernance et Reporting

Reporting pour la direction

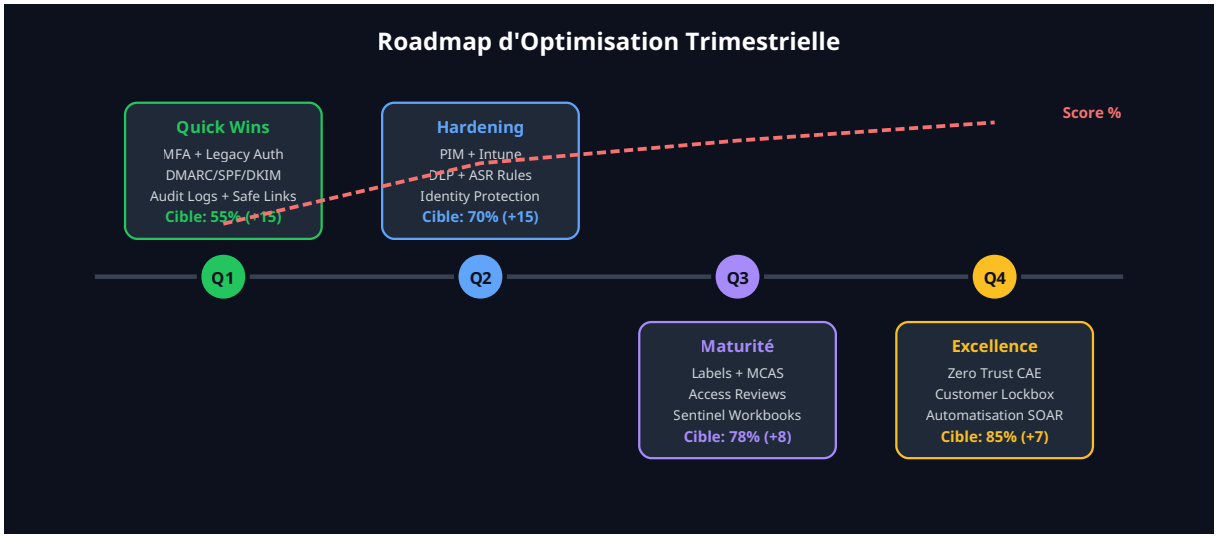
Le Secure Score est un outil puissant de communication avec la direction et le comité de sécurité. Structurez vos rapports mensuels avec les éléments suivants :

- **Score actuel vs objectif trimestriel** avec courbe d'évolution
- **Benchmark sectoriel** pour positionner l'organisation
- **Top 5 actions planifiées** avec gain attendu, responsable et date cible
- **Actions bloquées** (raisons techniques, budgétaires, organisationnelles) avec plan de déblocage
- **Incidents évités** grace aux actions mises en oeuvre (corrélation avec les alertes Defender)

Alignement NIS 2 et ISO 27001

Le Secure Score peut servir d'indicateur de performance pour les exigences de NIS 2 et ISO 27001 :

Exigence NIS 2 / ISO 27001	Actions Secure Score associées	Mesure
Gestion des accès (A.9 ISO)	MFA, PIM, Conditional Access, Access Reviews	Score Identity > 70%
Protection des données (Art. 21 NIS 2)	DLP, Sensitivity Labels, chiffrement	Score Data > 60%
Gestion des incidents (Art. 23 NIS 2)	Unified Audit Log, Defender alerts, SIEM	Rétention > 1 an
Sécurité des endpoints (A.12 ISO)	Intune, ASR, EDR, BitLocker	Score Device > 65%
Continuité d'activité (A.17 ISO)	Rétention, archivage, sauvegarde	Politiques actives



Pièges et Limitations du Secure Score

Malgré sa valeur, le Secure Score comporte des limitations importantes qu'il faut comprendre pour éviter les faux sentiments de sécurité :

Limitations critiques a connaître

- **Score != Sécurité réelle** : Un score de 85% ne signifie pas que vous etes protégé a 85%. Le score mesure la configuration, pas la résilience face à des attaques poussées. Un attaquant compétent peut compromettre un tenant à score élevé via un phishing ciblé ou une vulnérabilité zero-day.
- **Biais de licences** : Les actions E5/P2 pèsent lourd dans le score. Un tenant E3 est mécaniquement plafonné. Ne confondez pas le pourcentage avec le niveau de protection absolu.
- **Actions "Third-party resolved"** : Certaines actions peuvent etre marquées manuellement comme résolues par un outil tiers (EDR, SIEM), sans vérification automatisée. Cela peut gonfler artificiellement le score.
- **Délai de mise à jour** : Le score peut prendre 24 a 48 heures pour refléter les changements de configuration. Ne vous fiez pas au score en temps réel.
- **Périmètre limité** : Le Secure Score ne couvre pas la sécurité applicative custom, les configurations on-premises avancées, ni la posture de sécurité des partenaires tiers.
- **Regression silencieuse** : Des modifications de configuration (nouvel admin qui désactive une politique, exception ajoutée au Conditional Access) peuvent faire baisser le score sans alerte. Automatisez le monitoring.

Compléments indispensables au Secure Score

Pour une posture de sécurité complète, complétez le Secure Score avec :

- **Tests d'intrusion réguliers** (pentest M365 + AD) pour valider la résistance réelle
- **Exercices de phishing simulés** (Attack Simulator dans Defender for Office 365)
- **Revue de la configuration par un tiers** (audit indépendant annuel)
- **Monitoring comportemental** avec Microsoft Sentinel et des règles de détection personnalisées
- **Exercices de réponse a incident** (tabletop exercises) pour tester les procédures

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 Microsoft Secure Score dans un environnement de production ?

La mise en place de Microsoft Secure Score 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 Secure Score est-il essentiel pour la securite des systemes d'information ?

Microsoft Secure Score 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 Microsoft Secure Score : Guide d'Optimisation de votre ?

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.

Pour approfondir, consultez les ressources de NIST Cybersecurity et de CERT-FR.

Sources et références : Microsoft Security Docs · CERT-FR

> Points clés à retenir
>
> • Stratégie d'Optimisation : Quick Wins, Medium et Long-Terme
> • Automatisation et APIs
> • Gouvernance et Reporting
> • Pièges et Limitations du Secure Score
> • Questions frequentes
> • Conclusion

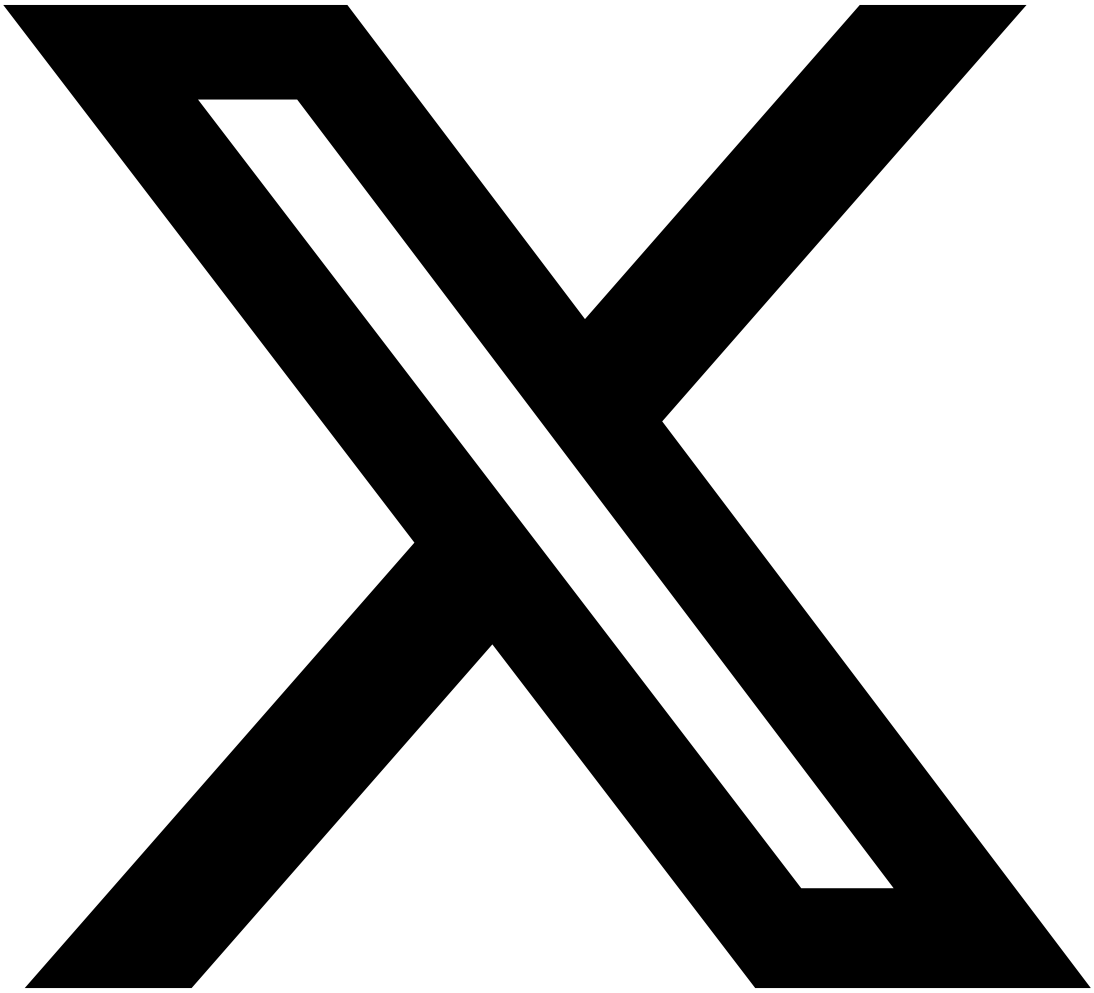
Conclusion

Microsoft Secure Score est bien plus qu'un simple chiffre : c'est un **cadre de gouvernance de la sécurité** qui permet de mesurer, prioriser et démontrer les progrès. En adoptant une approche structurée en trois phases (quick wins, hardening, maturité), en automatisant le suivi via Graph API et PowerShell, et en intégrant le score dans les processus de gouvernance et de conformité, les organisations transforment cet indicateur en véritable levier stratégique.

Rappelons néanmoins que le Secure Score reste un indicateur parmi d'autres. Il doit etre complété par des tests d'intrusion, des exercices de simulation d'attaque et une veille continue sur les menaces. L'objectif n'est pas le score parfait, mais une **amélioration mesurable et continue** de la posture de sécurité, alignée sur les risques métier et les exigences réglementaires.

Pour les organisations commençant leur parcours, visez un gain de 20 points sur le premier trimestre avec les quick wins identifiés, puis progressez vers les 75-85% sur 12 mois. C'est un marathon, pas un sprint -- mais chaque point gagné réduit concrètement la surface d'attaque de votre environnement Microsoft 365.

Partager cet article

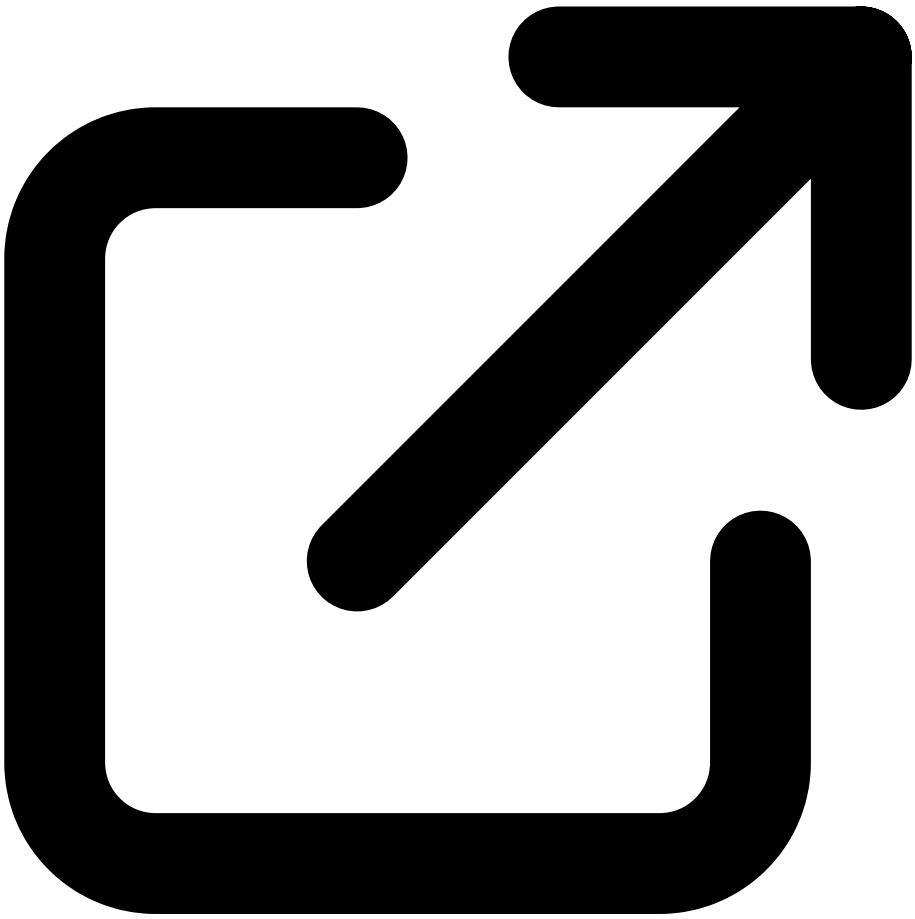


Partager sur X

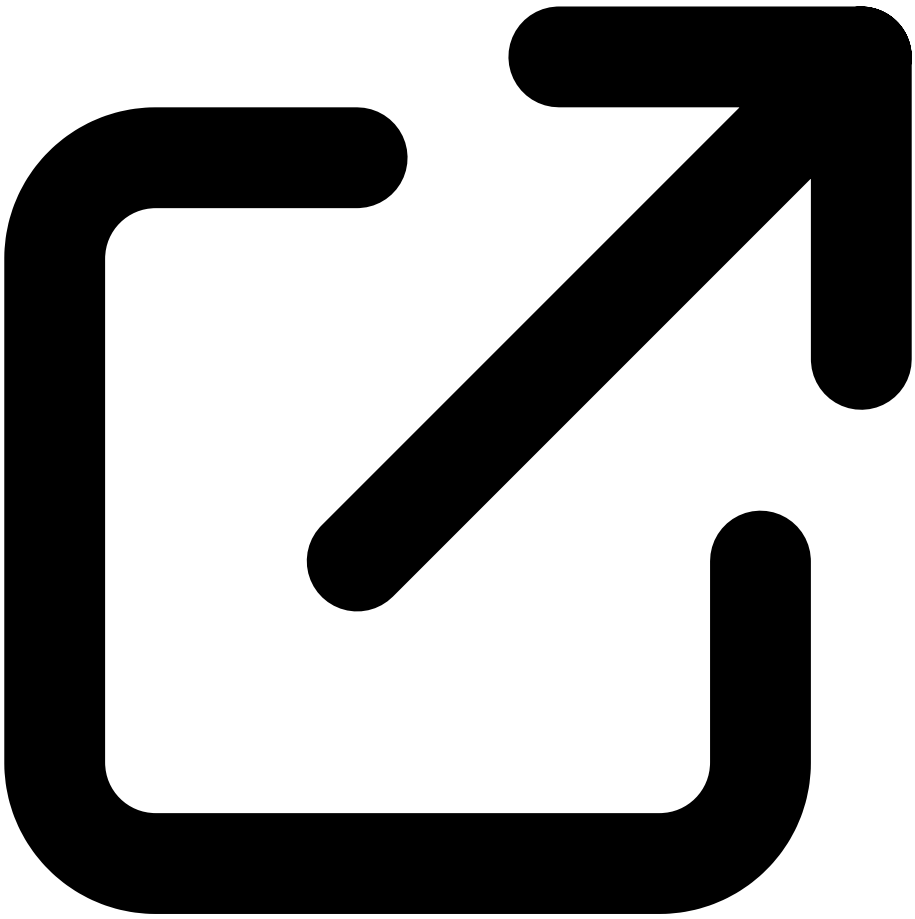
Partager sur LinkedIn

Ressources et Références Officielles

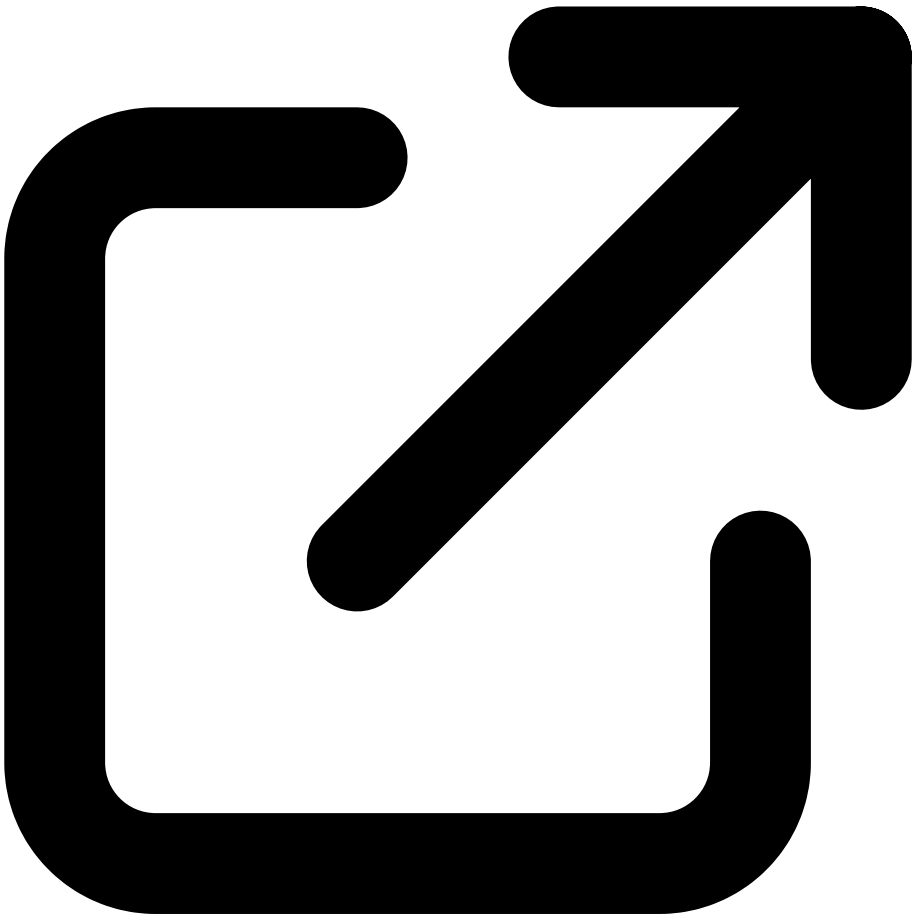
Documentation Microsoft, standards et outils de référence



Microsoft Secure Score Documentation
learn.microsoft.com



Microsoft Graph API - Secure Scores
learn.microsoft.com



CIS Benchmark Microsoft 365
cisecurity.org

Ayi NEDJIMI

Expert en Cybersécurité & Intelligence Artificielle

Consultant senior avec plus de 15 ans d'expérience en sécurité offensive, audit d'infrastructure et développement de solutions IA. Certifié OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer. Intervient sur des missions de pentest Active Directory, sécurité Cloud et conformité réglementaire pour des grands comptes et ETI.

LinkedIn Profil complet Tous ses articles

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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