HARDEN 365

Protect your data in minutes

Diagnostic de sécurité Microsoft 365

Sommaire

1 OBJECTIFS 2

2 VUE D'ENSEMBLE DE LA SECURITE 3

2.1 Liste des taches d'un diagnostic de securite 3
2.2 Executer le Microsoft 365 Secure Score 3
2.3 Executer le Microsoft Compliance Manager 4
2.4 Lancer le script PowerShell SCUBAGEAR (outil du CISA : agence americaine). 6
2.5 Lancer l'outil Harden 365 9

3 AZURE AD 10

3.1 Determiner si le parametre Security Default est applique sur le Tenant Microsoft 365 10
3.2 Domaine DNS 10
3.3 Affectation des licences 10
3.4 Les roles Azure AD 10
3.5 Les applications Azure AD et les permissions 11
3.6 Lancer Microsoft Azure AD Identity Score 11
3.7 Lancer le Microsoft Azure AD Assessment 11
3.7.1 Vue générale 11
3.7.2 Etape 1 : sur la machine qui va collecter les données 11
3.7.3 Sur la machine qui va interpréter les éléments remontés 12
3.8 Lancer PingCastle Cloud 14
3.9 Lancer l'outil Semperis Purple Knight 15
3.10 Regles d'acces conditionnelles 18
3.11 Strategie de mots de passe 18
3.12 Les comptes invites 18

4 EXCHANGE ONLINE 19

4.1 Lancer Microsoft Orca 19
4.2 Boites aux lettres (permissions, transfert automatique) 19
4.3 Parametres de l'antispam 20
4.4 Mode hybride 20

5 ONEDRIVE, SHAREPOINT ONLINE, ET TEAMS : 21

5.1 Lancer Microsoft Orca 21
5.2 Lister les liens anonymes et supprimer ceux qui ne sont plus utiles 21

6 MICROSOFT AZURE AD CONNECT 22

6.1 Configuration de l'annuaire Active Directory 22
6.2 Utiliser Azure AD Connect Configuration Documenter 22
6.3 Verifier que tous les comptes Azure avec des roles sont des comptes InCloud 22

7 ANALYSE DES PARAMETRES MICROSOFT PURVIEW INFORMATION PROTECTION ET MICROSOFT DLP 23

7.1 Script d'audit 23
7.2 Utilisation du module PowerShell CAMP 24

1 Objectifs

Ce document présente la procédure pour réaliser un diagnostic de sécurité d'un Tenant Microsoft 365.

2 Vue d'ensemble de la sécurité

2.1 Liste des tâches d'un diagnostic de sécurité

Pour réaliser un diagnostic de sécurité Microsoft 365, il est nécessaire d'effectuer les actions suivantes :

- Analyse des paramètres de l'annuaire Azure AD : comptes avec des rôles, applications avec des permissions, règles d'accès conditionnelles, stratégie de mots de passe, paramètres de fédération d'identité, lister les comptes invités.
- Analyse des paramètres Exchange Online : utilisation du mode hybride, permissions sur les boîtes aux lettres, permissions sur les dossiers publics, paramètres de l'antispam.
- Analyse des paramètres SharePoint Online et des solutions qui s'appuient sur cette solution (*OneDrive* et *Teams*) : accès des comptes invités, utilisation de liens avec un accès anonyme.
- Analyse des paramètres du serveur de synchronisation d'annuaire *Azure AD Connect*. Ce serveur doit être dans une unité d'organisation Tier 0. Le *Soft matching* et le *Hard Matching* doivent être désactivées. La synchronisation des stratégies de mots de passe doit être activé.
- Analyse des paramètres de la solution *Microsoft Purview Information Protection* (anciennement Azure Information Protection) et des règles *Microsoft DLP*. Ces 2 solutions permettent de classifier et protéger les données et d'empêcher la fuite de données (DLP).

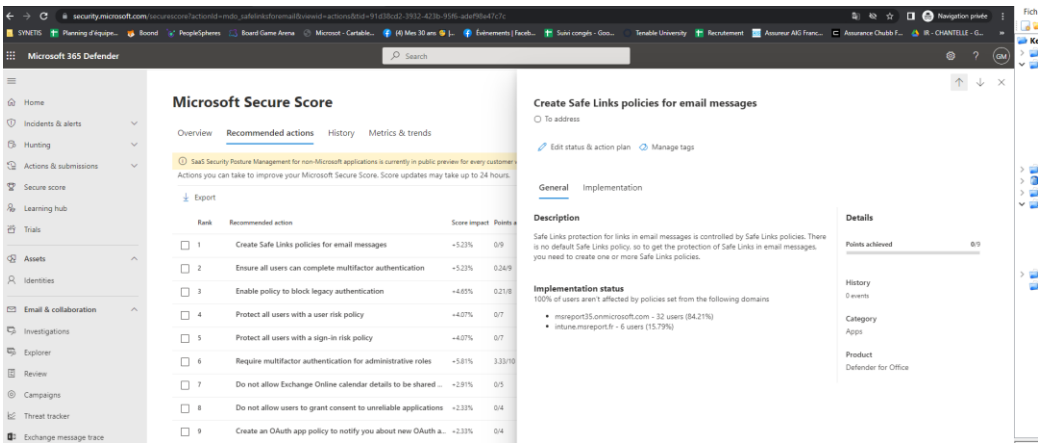
Il existe de nombreux outils pour faire un bilan de sécurité d'un Tenant Microsoft 365

- Harden 365
- Microsoft Azure AD Identity Score
- Microsoft 365 Secure Score
- Microsoft Compliance Manager
- PingCastle Cloud
- Semperis Purple Knight

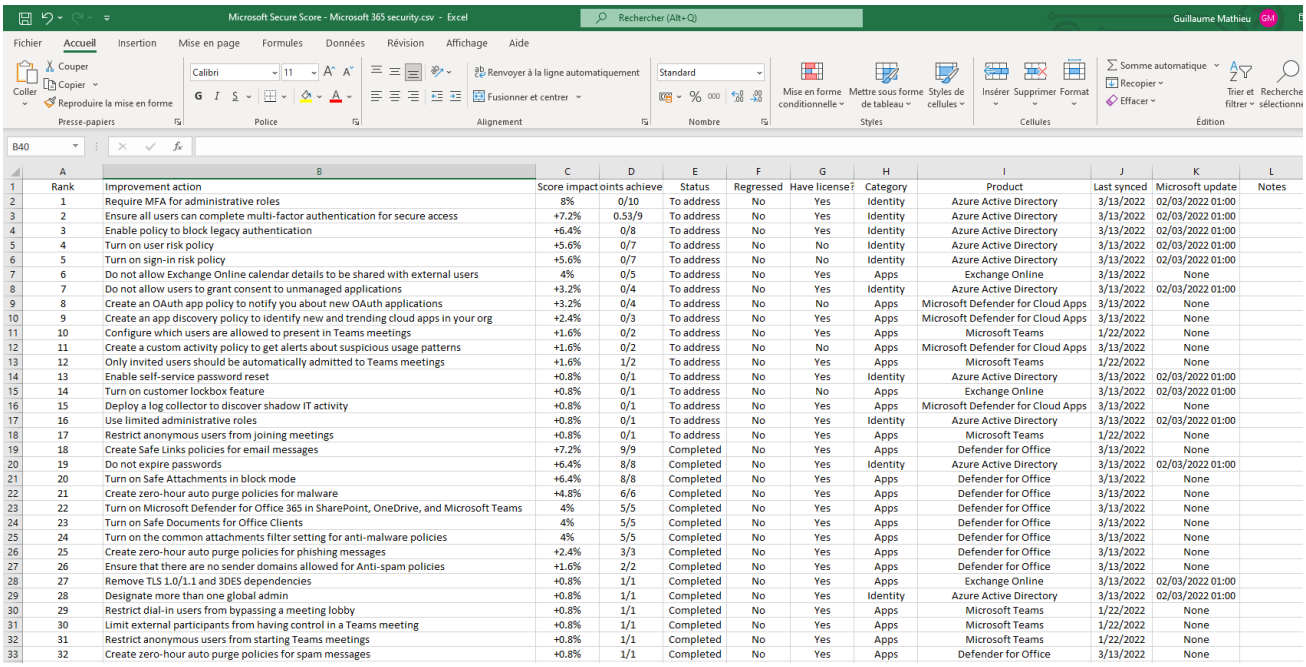
Ce document présente comment les utiliser.

2.2 Exécuter le Microsoft 365 Secure Score

Cet outil est accessible via le portail d'administration *Microsoft 365 Defender* (https://security.microsoft.com). Il permet de lister les actions de sécurité à mettre en place. Les préconisations sont orientés sur la sécurité des Azure AD et des services Exchange Online, SharePoint Online et Teams.



Il est possible d'exporter les préconisations au format CSV.



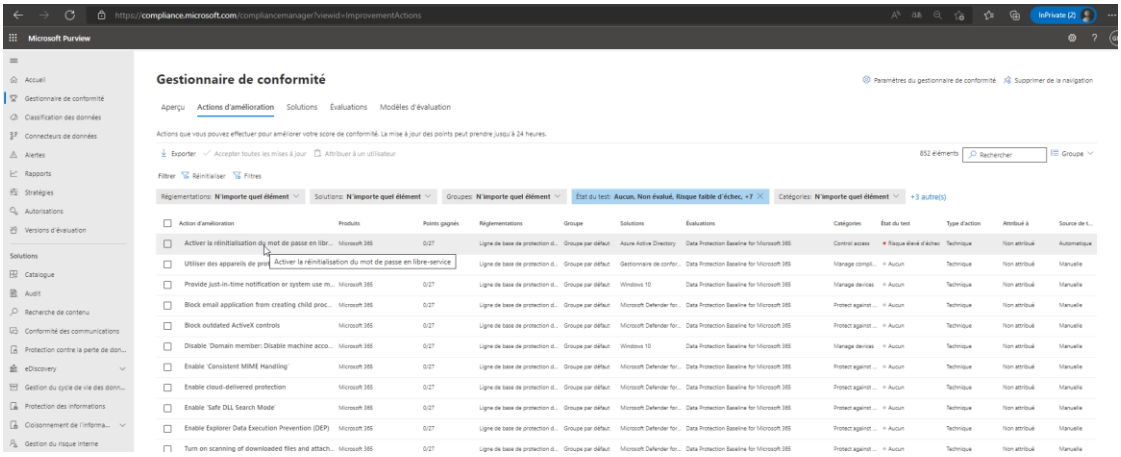
Rank	Improvement action	Score impact	oints achieve	Status	Regressed	Have license?	Category	Product	Last synced	Microsoft update	Notes
1	Require MFA for administrative roles	8%	0/10	To address	No	Yes	Identity	Azure Active Directory	3/13/2022	02/03/2022 01:00	
2	Ensure all users can complete multi-factor authentication for secure access	+7.2%	0.53/9	To address	No	Yes	Identity	Azure Active Directory	3/13/2022	02/03/2022 01:00	
3	Enable policy to block legacy authentication	+6.4%	0/8	To address	No	Yes	Identity	Azure Active Directory	3/13/2022	02/03/2022 01:00	
4	Turn on user risk policy	+5.6%	0/7	To address	No	No	Identity	Azure Active Directory	3/13/2022	02/03/2022 01:00	
5	Turn on sign-in risk policy	+5.6%	0/7	To address	No	No	Identity	Azure Active Directory	3/13/2022	02/03/2022 01:00	
6	Do not allow Exchange Online calendar details to be shared with external users	4%	0/5	To address	No	Yes	Apps	Exchange Online	3/13/2022	None	
7	Do not allow users to grant consent to unmanaged applications	+3.2%	0/4	To address	No	Yes	Identity	Azure Active Directory	3/13/2022	02/03/2022 01:00	
8	Create an OAuth app policy to notify you about new OAuth applications	+3.2%	0/4	To address	No	No	Apps	Microsoft Defender for Cloud Apps	3/13/2022	None	
9	Create an app discovery policy to identify new and trending cloud apps in your org	+2.4%	0/3	To address	No	Yes	Apps	Microsoft Defender for Cloud Apps	3/13/2022	None	
10	Configure which users are allowed to present in Teams meetings	+1.6%	0/2	To address	No	Yes	Apps	Microsoft Teams	1/22/2022	None	
11	Create a custom activity policy to get alerts about suspicious usage patterns	+1.6%	0/2	To address	No	No	Apps	Microsoft Defender for Cloud Apps	3/13/2022	None	
12	Only invited users should be automatically admitted to Teams meetings	+1.6%	1/2	To address	No	Yes	Apps	Microsoft Teams	1/22/2022	None	
13	Enable self-service password reset	+0.8%	0/1	To address	No	Yes	Identity	Azure Active Directory	3/13/2022	02/03/2022 01:00	
14	Turn on customer lockbox feature	+0.8%	0/1	To address	No	No	Apps	Exchange Online	3/13/2022	02/03/2022 01:00	
15	Deploy a log collector to discover shadow IT activity	+0.8%	0/1	To address	No	Yes	Apps	Microsoft Defender for Cloud Apps	3/13/2022	None	
16	Use limited administrative roles	+0.8%	0/1	To address	No	Yes	Identity	Azure Active Directory	3/13/2022	02/03/2022 01:00	
17	Restrict anonymous users from joining meetings	+0.8%	0/1	To address	No	Yes	Apps	Microsoft Teams	1/22/2022	None	
18	Create Safe Links policies for email messages	+7.2%	9/9	Completed	No	Yes	Apps	Defender for Office	3/13/2022	None	
19	Do not expire passwords	+6.4%	8/8	Completed	No	Yes	Identity	Azure Active Directory	3/13/2022	02/03/2022 01:00	
20	Turn on Safe Attachments in block mode	+6.4%	8/8	Completed	No	Yes	Apps	Defender for Office	3/13/2022	None	
21	Create zero-hour auto purge policies for malware	+4.8%	6/6	Completed	No	Yes	Apps	Defender for Office	3/13/2022	None	
22	Turn on Microsoft Defender for Office 365 in SharePoint, OneDrive, and Microsoft Teams	4%	5/5	Completed	No	Yes	Apps	Defender for Office	3/13/2022	None	
23	Turn on Safe Documents for Office Clients	4%	5/5	Completed	No	Yes	Apps	Defender for Office	3/13/2022	None	
24	Turn on the common attachments filter setting for anti-malware policies	4%	5/5	Completed	No	Yes	Apps	Defender for Office	3/13/2022	None	
25	Create zero-hour auto purge policies for phishing messages	+2.4%	3/3	Completed	No	Yes	Apps	Defender for Office	3/13/2022	None	
26	Ensure that there are no sender domains allowed for Anti-spam policies	+1.6%	2/2	Completed	No	Yes	Apps	Defender for Office	3/13/2022	None	
27	Remove TLS 1.0/1.1 and 3DES dependencies	+0.8%	1/1	Completed	No	Yes	Apps	Exchange Online	3/13/2022	02/03/2022 01:00	
28	Designate more than one global admin	+0.8%	1/1	Completed	No	Yes	Identity	Azure Active Directory	3/13/2022	02/03/2022 01:00	
29	Restrict dial-in users from bypassing a meeting lobby	+0.8%	1/1	Completed	No	Yes	Apps	Microsoft Teams	1/22/2022	None	
30	Limit external participants from having control in a Teams meeting	+0.8%	1/1	Completed	No	Yes	Apps	Microsoft Teams	1/22/2022	None	
31	Restrict anonymous users from starting Teams meetings	+0.8%	1/1	Completed	No	Yes	Apps	Microsoft Teams	1/22/2022	None	
32	Create zero-hour auto purge policies for spam messages	+0.8%	1/1	Completed	No	Yes	Apps	Defender for Office	3/13/2022	None	

2.3 Exécuter le Microsoft Compliance Manager

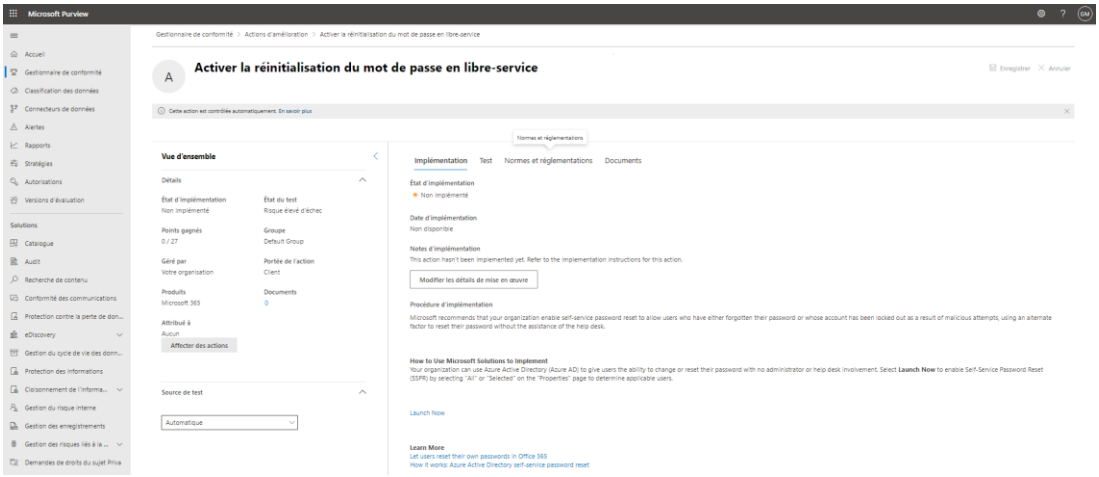
Cet outil est accessible depuis le portail *Microsoft Purview* (https://compliance.microsoft.com).

Les recommandations du portail de compliance portent sur les respects des réglementations (RGPD) mais aussi sur des paramètres de configuration :

- Annuaire AD (avec *Microsoft Defender for Identity*).
- Annuaire Azure AD (activation d'*Azure SSPR*, blocage des anciens protocoles d'authentification, utilisation de l'authentification à 2 facteurs *Azure MFA* pour les comptes utilisateurs et les comptes d'administration…) ;
- La détection du Shadow IT (avec *Microsoft Defender for Cloud Apps*) ;
- La restriction des personnes abilitées à faire des recherches dans le contenu des boîtes aux lettres selon des mots clés, des destinataires ou des émetteurs (avec la fonctionnalité eDiscovery) ;
- Le paramétrage de l'antivius *Microsoft Defender for Endpoint* ;
- Le paramétrage de Microsoft Defender for Office 365 (analyse des liens / pièces jointes malveillants, …) ;
- Le paramétrage de SharePoint Online (expiration pour les liens anonymes).
- Le paramétrage des machines Windows (via Microsoft Intune).
- L'utilisation des *Sensitivity labels* pour protéger les données sensibles de l'entreprise (*Microsoft Information protection*).



Pour chaque élément, le Compliance Manager va renvoyer vers un lien et des explications sur comment implémenter la solution (bouton *Launch now*).



Il est aussi possible d'exporter l'ensemble des recommandations sous forme d'un fichier CSV.

2.4 Lancer le script PowerShell SCUBAGEAR (outil du CISA : agence américaine).

Cet outil permet d'avoir une vue générale sur un Tenant Microsoft 365.

https://github.com/cisagov/ScubaGear

Le module PowerShell Microsoft Teams est requis mais doit être en version 4.99 maximum (la version à) dare es la 5.0.0).

```
PS C:\_adm\ScubaGear-v0-2-1\ScubaGear-0.2.1> .\Setup.ps1 #Installs the required modules
Setting PSGallery repository to trusted.
 PowerShellGet:1.0.0.1 updated to version 2.2.5.
DEBUG: MicrosoftTeams:5.0.0 already has latest installed.
DEBUG: ExchangeOnlineManagement:3.1.0 already has latest installed.
Installed latest version of Microsoft.Online.SharePoint.PowerShell
Installed latest version of Microsoft.PowerApps.Administration.PowerShell
Installed latest version of Microsoft.PowerApps.PowerShell
DEBUG: Microsoft.Graph.Applications:1.23.0 already has latest installed.
DEBUG: Microsoft.Graph.Authentication:1.23.0 already has latest installed.
DEBUG: Microsoft.Graph.DeviceManagement:1.23.0 already has latest installed.
DEBUG: Microsoft.Graph.DeviceManagement.Administration:1.23.0 already has latest installed.
DEBUG: Microsoft.Graph.DeviceManagement.Enrolment:1.23.0 already has latest installed.
DEBUG: Microsoft.Graph.Devices.CorporateManagement:1.23.0 already has latest installed.
DEBUG: Microsoft.Graph.Groups:1.23.0 already has latest installed.
DEBUG: Microsoft.Graph.Identity.DirectoryManagement:1.23.0 already has latest installed.
DEBUG: Microsoft.Graph.Identity.Governance:1.23.0 already has latest installed.
DEBUG: Microsoft.Graph.Identity.SignIns:1.23.0 already has latest installed.
DEBUG: Microsoft.Graph.Planner:1.23.0 already has latest installed.
DEBUG: Microsoft.Graph.Teams:1.23.0 already has latest installed.
DEBUG: Microsoft.Graph.Users:1.23.0 already has latest installed.
DEBUG: ScubaGear setup time elapsed:  82 seconds.
PS C:\_adm\ScubaGear-v0-2-1\ScubaGear-0.2.1> Import-Module -Name .\PowerShell\ScubaGear #Imports the tool into your sess
ion
Import-Module : No acceptable installed version found for module: MicrosoftTeams
        Required Min Version: 4.8.0 | Max Version: 4.99.99999
        Run Get-InstalledModule to see a list of currently installed modules
        Run SetUp.ps1 or Install-Module MicrosoftTeams -force to install the latest version of MicrosoftTeams
At line:1 char:1
+ Import-Module -Name .\PowerShell\ScubaGear #Imports the tool into you ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationStopped: (:) [Import-Module], FileNotFoundException
    + FullyQualifiedErrorId : No acceptable installed version found for module: MicrosoftTeams
        Required Min Version: 4.8.0 | Max Version: 4.99.99999
        Run Get-InstalledModule to see a list of currently installed modules
            Run SetUp.ps1 or Install-Module MicrosoftTeams -force to install the latest version of MicrosoftTeams,Micr
  osoft.PowerShell.Commands.ImportModuleCommand
```

Il faut donc désinstaller la dernière version et relancer la procédure d'installation.

Uninstall-module MicrosoftTeams

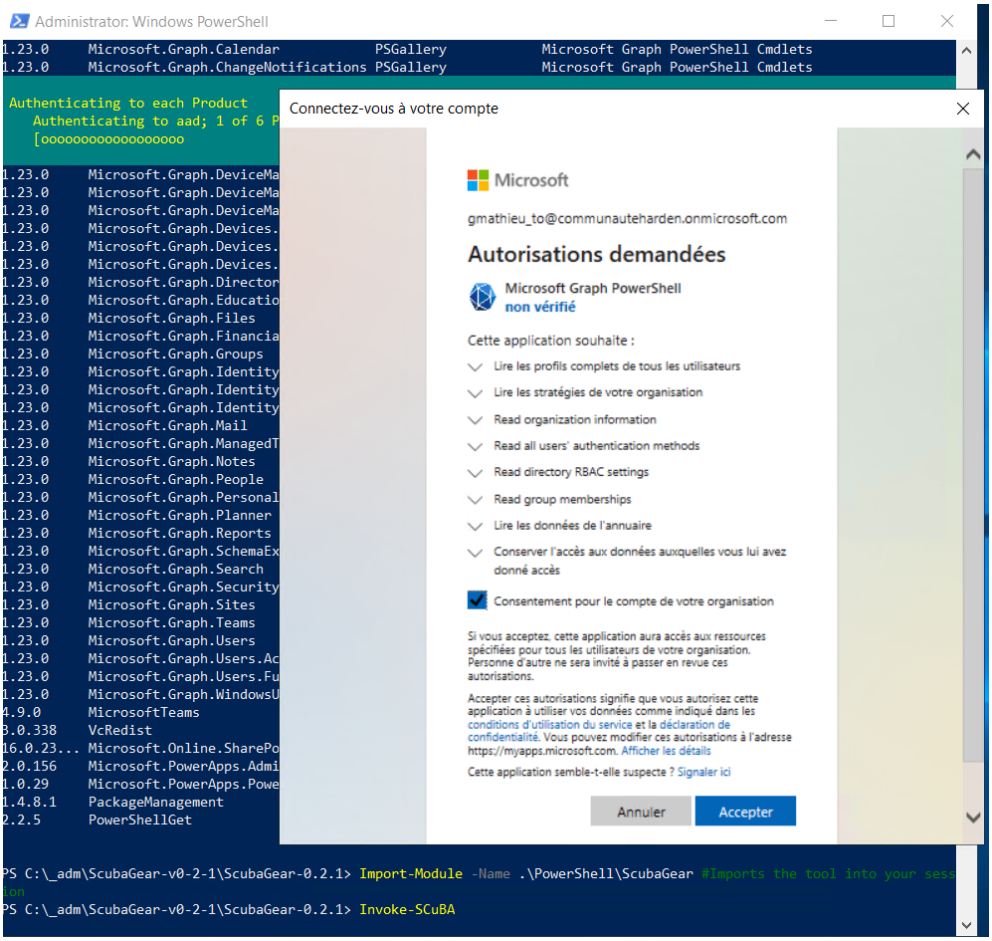
Install-Module -Name MicrosoftTeams -RequiredVersion 4.9.0

L'application s'appuie sur l'application *Microsoft Graph PowerShell*.

Pour lancer le scan du Tenant

Import-Module -Name .\PowerShell\ScubaGear

Invoke-SCuBA



Nous obtenons le résultat suivant.

Secure Cloud Business Applications (SCuBA) Baseline Documents

SCuBA M365 Security Baseline Conformance Reports

Tenant Display Name	Tenant Domain Name	Tenant ID	Report Date
Harden	communauteharden.onmicrosoft.com	9e2165c8-f76f-4441-8e99-6c4b540008b8	03/13/2023 08:29:09 Romance Standard Time

Baseline Conformance Reports	Details			
Azure Active Directory	7 tests passed	4 warnings	11 tests failed	8 manual checks needed
Microsoft 365 Defender	38 tests passed	15 warnings	26 tests failed	5 manual checks needed
Exchange Online	7 tests passed	2 warnings	5 tests failed	23 manual checks needed
OneDrive for Business	1 tests passed	4 warnings	1 test failed	2 manual checks needed
SharePoint Online	1 tests passed	3 warnings	1 test failed	2 manual checks needed
Microsoft Teams	7 tests passed	5 warnings	4 tests failed	9 manual checks needed

Tous les rapports sont créés dans un répertoire appelé *M365BaselineConformance_XXXX_MM_DD_hh_mm_ss*.

Secure Cloud Business Applications (SCuBA) Baseline Documents

Exchange Online Baseline Report

Tenant Display Name	Report Date	Baseline Version	Module Version
Harden	03/13/2023 08:29:09 Romance Standard Time	0.1	0.2.1

EXO 2.1 Automatic Forwarding to External Domains SHALL Be Disabled

Requirement	Result	Criticality	Details
Automatic forwarding to external domains SHALL be disabled	Fail	Shall	1 remote domain(s) that allows automatic forwarding: *

EXO 2.2 Sender Policy Framework SHALL Be Enabled

Requirement	Result	Criticality	Details
A list of approved IP addresses for sending mail SHALL be maintained	N/A	Shall/Not-Implemented	Currently cannot be checked automatically. See Exchange Online Secure Configuration Baseline policy 2.# for instructions on manual check
An SPF policy(s) that designates only these addresses as approved senders SHALL be published	Pass	Shall	Requirement met

EXO 2.3 DomainKeys Identified Mail SHOULD Be Enabled

Requirement	Result	Criticality	Details
DKIM SHOULD be enabled for any custom domain	Warning	Should	4 of 4 agency domain(s) found in violation: harden-community.org, harden365.net, hardenad.com, hardenad.net

Un exemple de rapport est disponible ci-dessous (renommé le fichier .txt au format .zip).

M365BaselineConfor
mance_2023_03_13_08

2.5 Lancer l'outil Harden 365

Cet outil intègre de nombreux scripts pour analyser la sécurité de votre Tenant. Il permet :

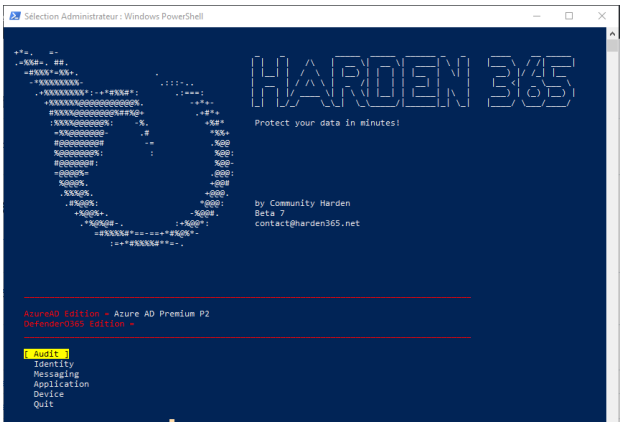
- De générer un rapport Orca
- De lister les comptes Azure AD avec des rôles
- De lister les comptes Azure AD avec des licences
- De lister toutes les boîtes aux lettres avec des paramètres de transfert automatique des emails
- De lister les boîtes aux lettres avec des permissions personnalisées
- De vérifier que toutes les entrées DNS pour tous les domaines ont été créées.

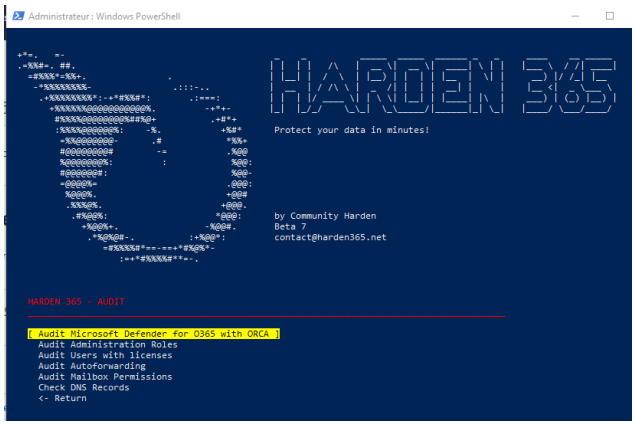
L'outil est gratuit et accessible à ces adresses :

https://hardenad.net

https://github.com/Harden365/Harden365

https://github.com/Harden365/Harden365/releases/tag/Harden365-0.8





L'outil permet aussi de déployer des règles de sécurités au niveau du Tenant Microsoft 365.

3 Azure AD

3.1 Déterminer si le paramètre Security Default est appliqué sur le Tenant Microsoft 365

Ce paramètre permet d'appliquer des règles de sécurité par défaut.

Ces règles ne sont cependant pas configurables ce qui est très problématique pour les sociétés qui disposent de comptes de service qui ne doivent pas appliquer le MFA.

https://help.protectedtrust.com/enabling-security-defaults-for-azure-active-directory-in-office-365

Il sera donc nécessaire de désactiver cette option sur de très nombreux Tenants et d'implémenter les règles de sécurité du modèle de sécurité via un outil comme *Harden 365*.

3.2 Domaine DNS

Vérifier que toutes les entrées DNS sont créés pour chaque domaine DNS ajouté sur le Tenant Microsoft 365.

En effet, les entrées pour Skype for Business ou Microsoft Intune ne sont pas toujours créés.

Déterminer qui a accès à ses entrées DNS (l'équipe qui peut modifier les entrées sur les serveurs DNS public).

Déterminer pour chaque domaine AD si ce dernier est managé ou fédéré (utilisation d'un IDP).

Si la société dispose d'un IDP et que ce dernier est hébergé sur une machine membre d'un domaine AD, le serveur IDP doit être dans une unité d'organisation Tier 0 (voir standard AD) et sécurisé comme un serveur Tier 0.

3.3 Affectation des licences

Déterminer les abonnements sur le Tenant Microsoft 365.

Déterminer les outils accessibles avec les licences et ceux qui sont utilisés.

Certaines fonctionnalités nécessitent qu'une seule licence pour être accessible comme *PIM*.

Les comptes d'administration n'ont pas besoin de licences pour fonctionner. Il est possible de supprimer les licences pour ces comptes pour réaliser des économies.

3.4 Les rôles Azure AD

Lister les comptes Azure AD avec les rôles d'administration en utilisant l'outil *Harden 365*. Ce dernier alerte si un compte d'administration ne dispose pas d'Azure MFA.

Les rôles ci-dessous peuvent escalader vers le rôle *Global Admins*. Ils doivent donc être supervisés :

- Application Administrator : permet d'autoriser une application et de définir des permissions au niveau des API. En donnant un accès en lecture / écriture Azure AD, un attaquant peut se donner les droits sur des comptes avec un rôle d'admnistration.
- Privileged Identity Administrator : ce rôle permet d'assigner un utilisateur à tous les rôles y compris *Global Administrator*.

- Directory writers : ce rôle a des accès très importants au niveau de l'annuaire Azure AD.

3.5 Les applications Azure AD et les permissions

Lister les applications Azure AD (*Registred Application*) avec des permissions.

Ce point est très critique car de nombreuses applications malveillantes disposent de permissions très importantes sur les Tenant Microsoft 365.

Sur les anciens Tenant Microsoft 365, les utilisateurs pouvaient ajouter et autoriser eux-mêmes des applications. Ces dernières pouvaient accéder aux contenus accessibles dans le contexte de ces comptes utilisateurs.

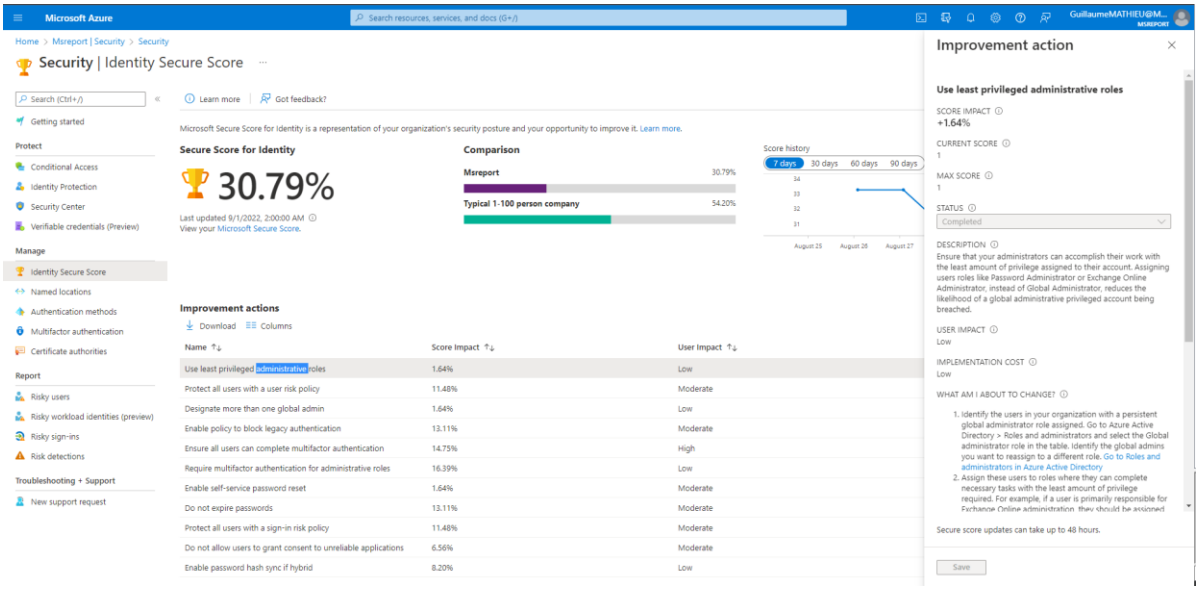
Utiliser *PingCastle Cloud* et/ou *Purple Knight* pour cela.

Voir le guide *Harden* sur les applications Azure AD.

3.6 Lancer Microsoft Azure AD Identity Score

Cet outil est accessible depuis le portail de sécurité Azure AD : https://aad.portal.azure.com.

Aller dans *Security | Identity Security Score*. L'outil va alors afficher les préconisations, les préconisations et un score de sécurité. Il est possible de connaître l'évolution de ce score sur plusieurs mois.



3.7 Lancer le Microsoft Azure AD Assessment

3.7.1 Vue générale

Ce module PowerShell permet de faire un bilan de sécurité de son annuaire Azure AD :

https://github.com/AzureAD/AzureADAssessment

https://github.com/AzureAD/AzureADAssessment/wiki

3.7.2 Etape 1 : sur la machine qui va collecter les données

Créer le répertoire c:_adm3

Lancer PowerShell V5.

Cd c:_adm3

Taper la commande suivante :

Install-Module AzureADAssessment -Force -Scope CurrentUser

Fermer et ouvrir de nouveau PowerShell V5 et taper les commandes suivantes :

Connect-AADAssessment

Invoke-AADAssessmentDataCollection

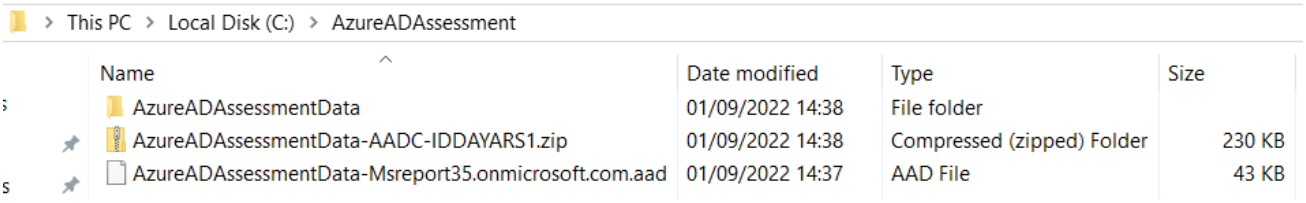
Invoke-AADAssessmentHybridDataCollection

```
PS C:\_adm3> Connect-AADAssessment
PS C:\_adm3> Invoke-AADAssessmentDataCollection


    Directory: C:\AzureADAssessment\AzureADAssessmentData


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        01/09/2022     14:36                AAD-Msreport35.onmicrosoft.com
Exporting applications: Completed 3 in 00:00:00
Exporting appRoleAssignments: Completed 12 in 00:00:00
Exporting oauth2PermissionGrants: Completed 7 in 00:00:00
Exporting servicePrincipals (JSON): Completed 11 in 00:00:00
Exporting servicePrincipals (CSV): Completed 11 in 00:00:00
Exporting groups: Completed 0 in 00:00:00
Loading users in lookup cache
Loading users registration details in lookup cache
Exporting UserReport: Completed 5 in 00:00:00
Loading groups in lookup cache
Exporting NotificationsEmailsReport: Completed 14 in 00:00:00
Loading groups in lookup cache
Loading administrative units in lookup cache
Loading applications in lookup cache
Loading service principals in lookup cache
Exporting RoleAssignmentReport: Completed 13 in 00:00:00
Exporting AppCredentialsReport: Completed 6 in 00:00:00
Exporting ConsentGrantReport: Completed 26 in 00:00:00
```

Cela génère le répertoire suivant.



3.7.3 Sur la machine qui va interpréter les éléments remontés

Installer PowerShell 7 (PowerShell-7.2.6-win-x64.zip) :

https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell-on-windows?view=powershell-7.2

Installer Power Bi Desktop :

https://www.microsoft.com/en-us/download/details.aspx?id=58494

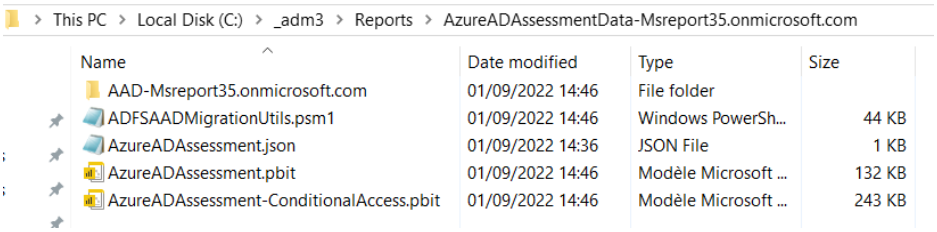
Installer Azure AD Connect Sync Configuration Documenter :

https://github.com/microsoft/AADConnectConfigDocumenter/releases

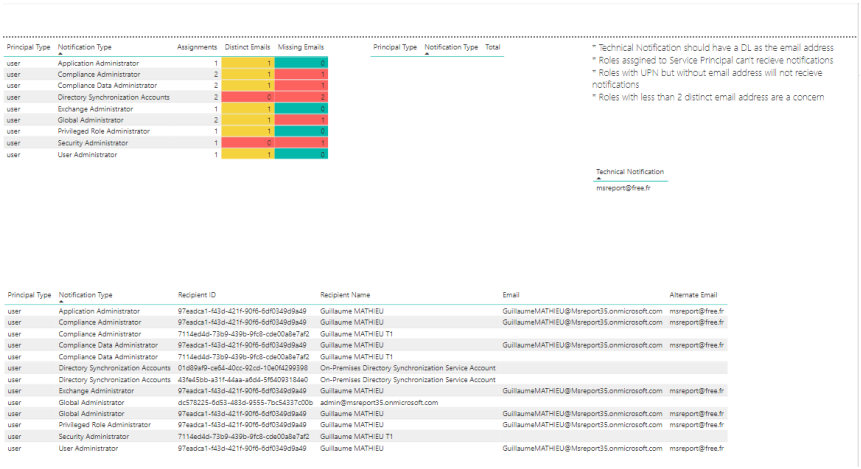
Déplacer les éléments générés à l'étape précédente dans le dossier C:_adm3 (le créer si nécessaire).
Créer le dossier *C:_adm3\Reports*.
Exécuter la commande suivante depuis in invite de commande PowerShell V5

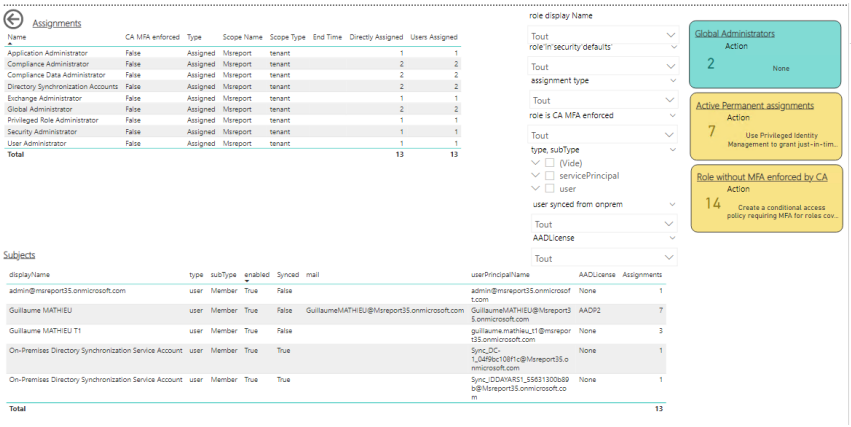
```
Complete-AADAssessmentReports `
 -Path C:\_adm3\AzureADAssessmentData-Msreport35.onmicrosoft.com.aad `
 -OutputDirectory C:\_adm3\Reports
```

Nous obtenons les fichiers résultats suivants.

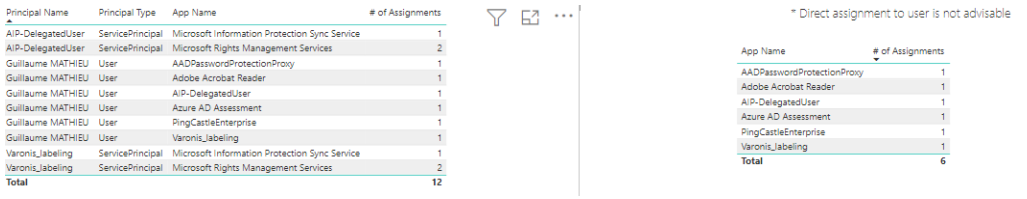


Ouvrir les fichiers Power Bi (*pbit*). Cela va ouvrir Power BI et permettre d'afficher le rapport.
Nous obtenons alors un rapport complet sur les rôles Azure AD assignés.





L'outil permet aussi les applications enregistrées sur le Tenant.



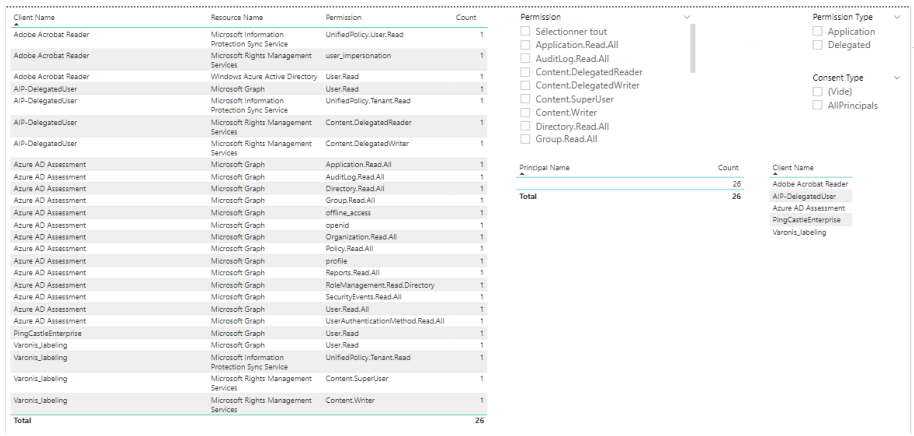
Principal Name	Principal Type	App Name	# of Assignments
AIP-DelegatedUser	ServicePrincipal	Microsoft Information Protection Sync Service	1
AIP-DelegatedUser	ServicePrincipal	Microsoft Rights Management Services	2
Guillaume MATHIEU	User	AADPasswordProtectionProxy	1
Guillaume MATHIEU	User	Adobe Acrobat Reader	1
Guillaume MATHIEU	User	AIP-DelegatedUser	1
Guillaume MATHIEU	User	Azure AD Assessment	1
Guillaume MATHIEU	User	PingCastleEnterprise	1
Guillaume MATHIEU	User	Varonis_labeling	1
Varonis_labeling	ServicePrincipal	Microsoft Information Protection Sync Service	1
Varonis_labeling	ServicePrincipal	Microsoft Rights Management Services	2
Total			**12**

* Direct assignment to user is not advisable

App Name	# of Assignments
AADPasswordProtectionProxy	1
Adobe Acrobat Reader	1
AIP-DelegatedUser	1
Azure AD Assessment	1
PingCastleEnterprise	1
Varonis_labeling	1
Total	**6**

Plus intéressant encore, l'outil permet de connaître les clés secrètes pour accéder aux applications et les consentements qui ont été fait côté Tenant avec les permissions qui ont été donnés.

Nous voyons par exemple les permissions assignées à l'application appelée *AIP-DelegatedUser*.



Client Name	Resource Name	Permission	Count
Adobe Acrobat Reader	Microsoft Information Protection Sync Service	UnifiedPolicy.User.Read	1
Adobe Acrobat Reader	Microsoft Rights Management Services	user_impersonation	1
Adobe Acrobat Reader	Windows Azure Active Directory	User.Read	1
AIP-DelegatedUser	Microsoft Graph	User.Read	1
AIP-DelegatedUser	Microsoft Information Protection Sync Service	UnifiedPolicy.Tenant.Read	1
AIP-DelegatedUser	Microsoft Rights Management Services	Content.DelegatedReader	1
AIP-DelegatedUser	Microsoft Rights Management Services	Content.DelegatedWriter	1
Azure AD Assessment	Microsoft Graph	Application.Read.All	1
Azure AD Assessment	Microsoft Graph	AuditLog.Read.All	1
Azure AD Assessment	Microsoft Graph	Directory.Read.All	1
Azure AD Assessment	Microsoft Graph	Group.Read.All	1
Azure AD Assessment	Microsoft Graph	offline_access	1
Azure AD Assessment	Microsoft Graph	openid	1
Azure AD Assessment	Microsoft Graph	Organization.Read.All	1
Azure AD Assessment	Microsoft Graph	Policy.Read.All	1
Azure AD Assessment	Microsoft Graph	profile	1
Azure AD Assessment	Microsoft Graph	Reports.Read.All	1
Azure AD Assessment	Microsoft Graph	RoleManagement.Read.Directory	1
Azure AD Assessment	Microsoft Graph	SecurityEvents.Read.All	1
Azure AD Assessment	Microsoft Graph	User.Read.All	1
Azure AD Assessment	Microsoft Graph	UserAuthenticationMethod.Read.All	1
PingCastleEnterprise	Microsoft Graph	User.Read	1
Varonis_labeling	Microsoft Graph	User.Read	1
Varonis_labeling	Microsoft Information Protection Sync Service	UnifiedPolicy.Tenant.Read	1
Varonis_labeling	Microsoft Rights Management Services	Content.SuperUser	1
Varonis_labeling	Microsoft Rights Management Services	Content.Writer	1
Total			**26**

Permission
- Sélectionner tout
- Application.Read.All
- AuditLog.Read.All
- Content.DelegatedReader
- Content.DelegatedWriter
- Content.SuperUser
- Content.Writer
- Directory.Read.All
- Group.Read.All

Permission Type
- Application
- Delegated

Consent Type
- (Vide)
- AllPrincipals

Principal Name	Count
	26
Total	**26**

Client Name
Adobe Acrobat Reader
AIP-DelegatedUser
Azure AD Assessment
PingCastleEnterprise
Varonis_labeling

3.8 Lancer PingCastle Cloud

Vincent Le Toux a mis à disposition l'outil *PingCastle Cloud* pour auditer la configuration des Tenant Microsoft 365. Ce dernier est disponible sur GitHub à l'adresse suivante :
https://github.com/vletoux/PingCastleCloud/releases

L'outil analyse entre autres :

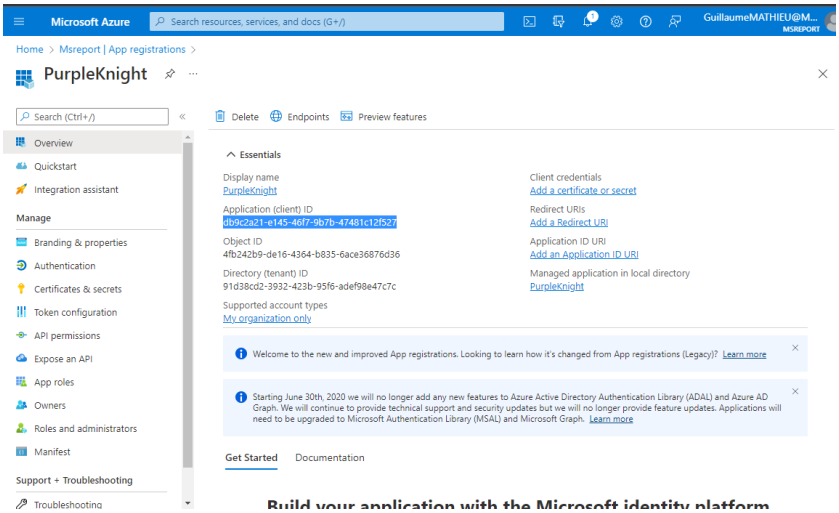
- Les domaines enregistrés sur le Tenant
- Les informations sur les comptes de service Azure AD Connect.
- Les relations entre Tenant Microsoft (Cross Tenants)
- Les comptes Azure AD avec un mot de passe qui n'expirent jamais.
- Les membres des rôles
- Les applications et leurs permissions
- Les transfert email

Nous obtenons alors ce type de rapport. Le rapport doit être ouvert avec Chrome, Firefox ou Edge (mauvais fonctionnement avec Internet Explorer).

pingcastlecloud_Msre
port35.onmicrosoft.cc

3.9 Lancer l'outil Semperis Purple Knight

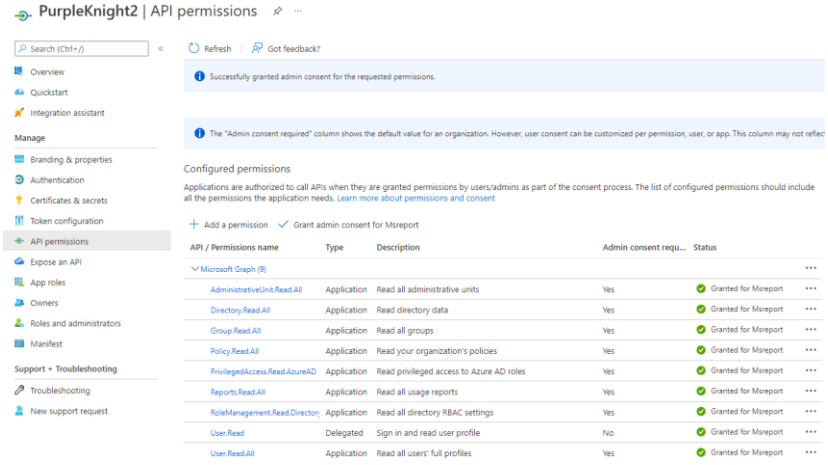
La solution *Semperis Purple Knight* permet d'auditer un annuaire Active Directory et Azure Active Directory.
Elle est téléchargeable gratuitement à l'adresse suivante :
https://www.purple-knight.com/
L'outil nécessite la création d'une application Azure AD avec les permissions suivantes :
https://docs.purple-knight.com/community/purpleknight/pk-create-configure-app-registration.htm



Créer l'application *PurpleKnight*.

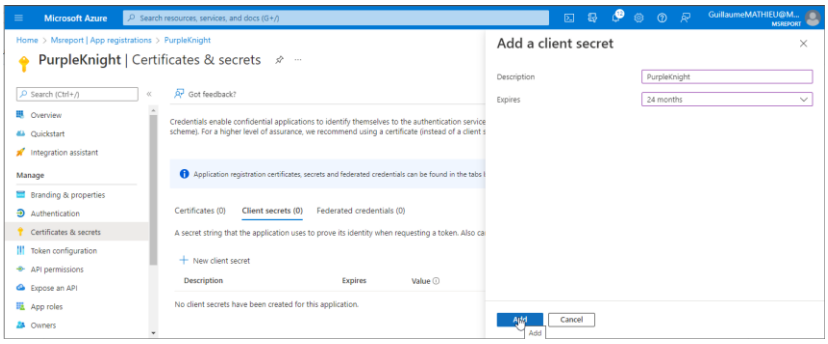
Copier l'ID du Tenant / Directory

Copier l'ID de l'application (ClientID)

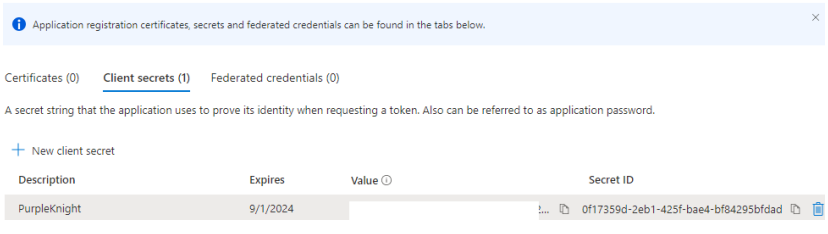


Déléguer ensuite les permissions Microsoft Graph requises par *Purple Knight*.

Voir permission du Starter Guide dans les sources de l'application.

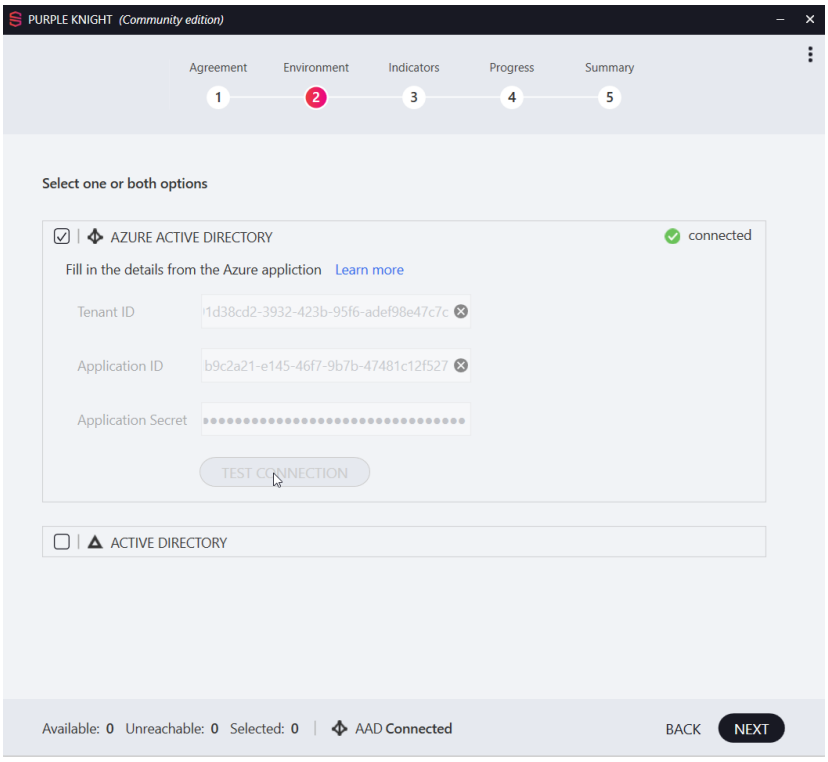


Créer un Secret pour l'application.



Copier le champ *Value*.

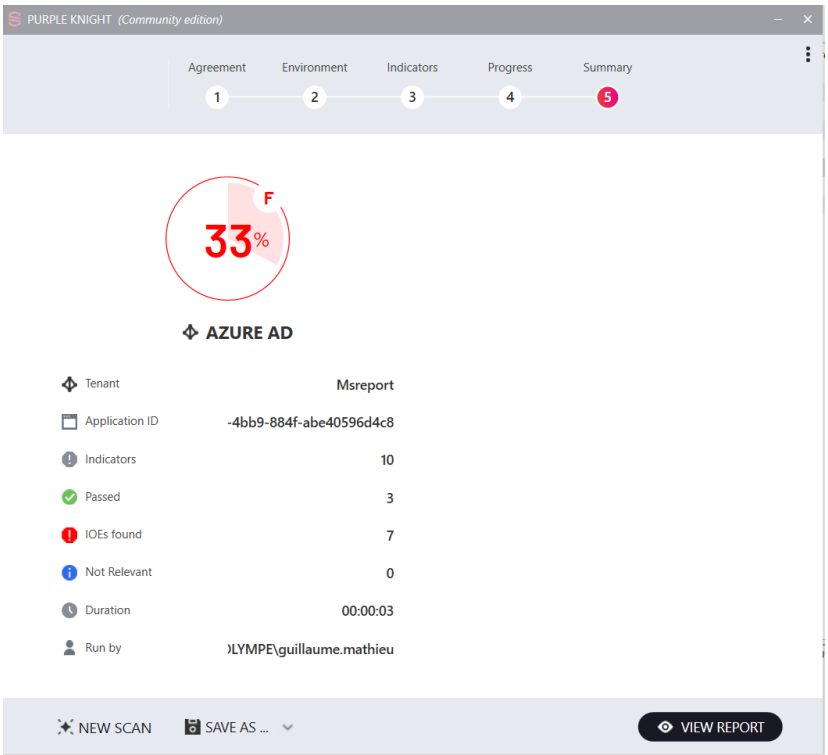
Cette valeur doit être sauvegarder dans un Keepass car elle ne sera plus affichable sur le Tenant.



Accepter la licence.

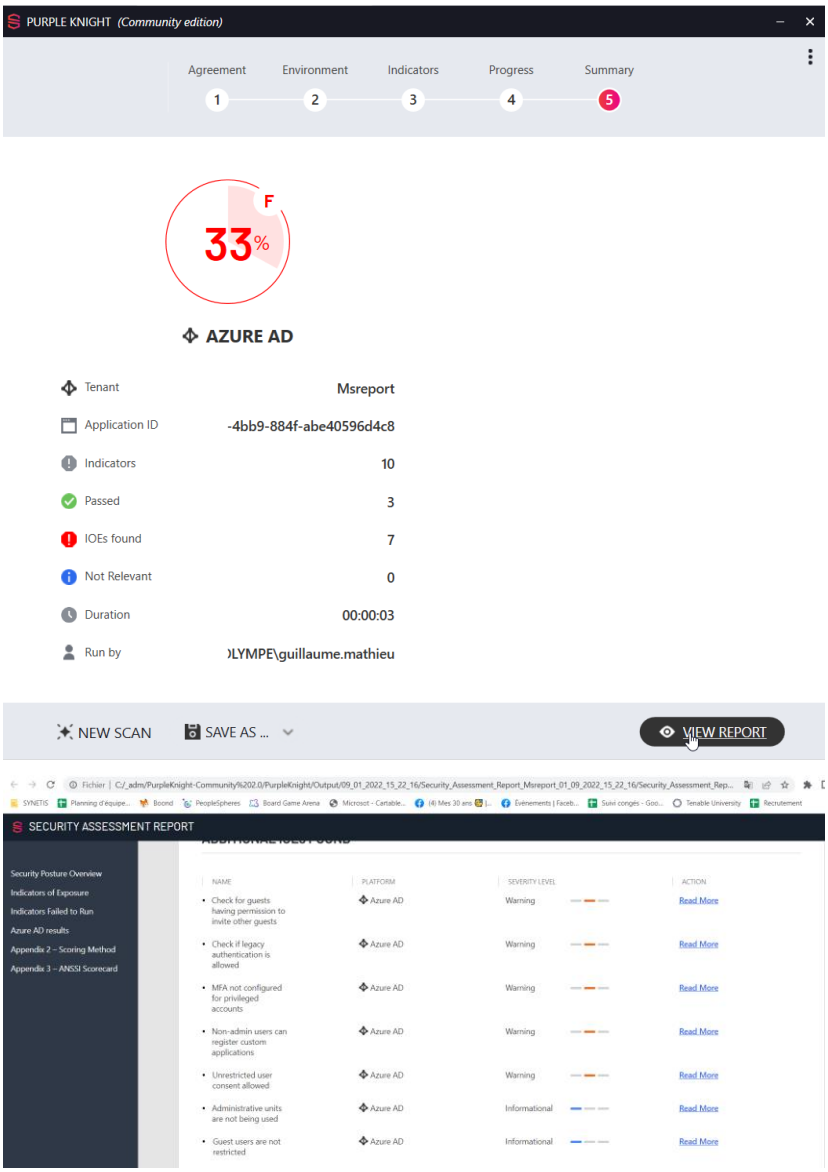
Copier ensuite les ID du tenant, de l'application et le Secret.

Cliquer sur le bouton *Test Connection*.



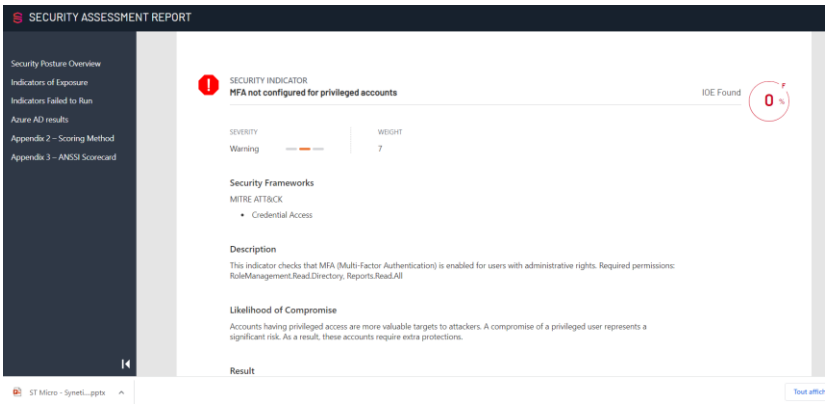
L’outil va analyser les éléments suivants :

- Les Administrative Unit non utilisées
- Les comptes invités qui ont des permissions sur d’autres comptes invités
- La possibilité d’utiliser des protocoles d’authentification Legacy (Authentification basique, …)
- Le fait que des comptes invités soit membres de rôles Azure AD à privilèges
- Le fait que le MFA n’est pas défini sur des comptes à forts privilèges
- Le fait de données des permissions API (Microsoft Graph) à risque.
- Le fait que le paramètre Security Defaults ne soit pas activé
- Le fait que les utilisateurs puissent ajouter des applications Azure
- Le fait que les utilisateurs puissent donner un consentement suite à l’ajout d’une application.



Nous obtenons alors un score de confidentialité.

Chaque point remonté peut être affiché en détails.



L'outil affiche les détails des préconisations.

3.10 Règles d'accès conditionnelles

Lister les règles d'accès conditionnelles en place (sur le portal Microsoft 365 Defender).

L'outil *Harden 365* propose la mise en place de règles d'accès conditionnelles pour :

- Bloquer l'utilisation des protocoles Legacy.
- Forcer l'utilisation du MFA pour les comptes standards.
- Forcer l'utilisation du MFA pour les comptes d'administration.

3.11 Stratégie de mots de passe

La solution *Azure AD Password Protection* permet de définir les mots de passe interdit pour l'annuaire Azure AD (et aussi pour l'annuaire Azure AD).

Déterminer les paramètres qui sont activés.

Voir document *Harden 365 - Azure AD Password Protection*.

3.12 Les comptes invités

Lister les comptes invités Azure invités.

http://www.wave16.com/2018/07/getting-azure-ad-guest-users-with-azure.html

Il est nécessaire de mettre en place un script qui désactive automatiquement les comptes invités qui ne servent plus.

4 Exchange Online

4.1 Lancer Microsoft Orca

Analyser les paramètres de sécurité de la messagerie Exchange Online en exécutant *Microsoft Orca*.

Ce dernier est inclus dans *Harden 365*.

Ce module PowerShell permet de faire un bilan de sécurité du tenant Microsoft 365 orienté sur la partie Microsoft Defender for Office 365 / Exchange Online Protection.

https://github.com/cammurray/orca

https://www.powershellgallery.com/packages/ORCA/1.10.6

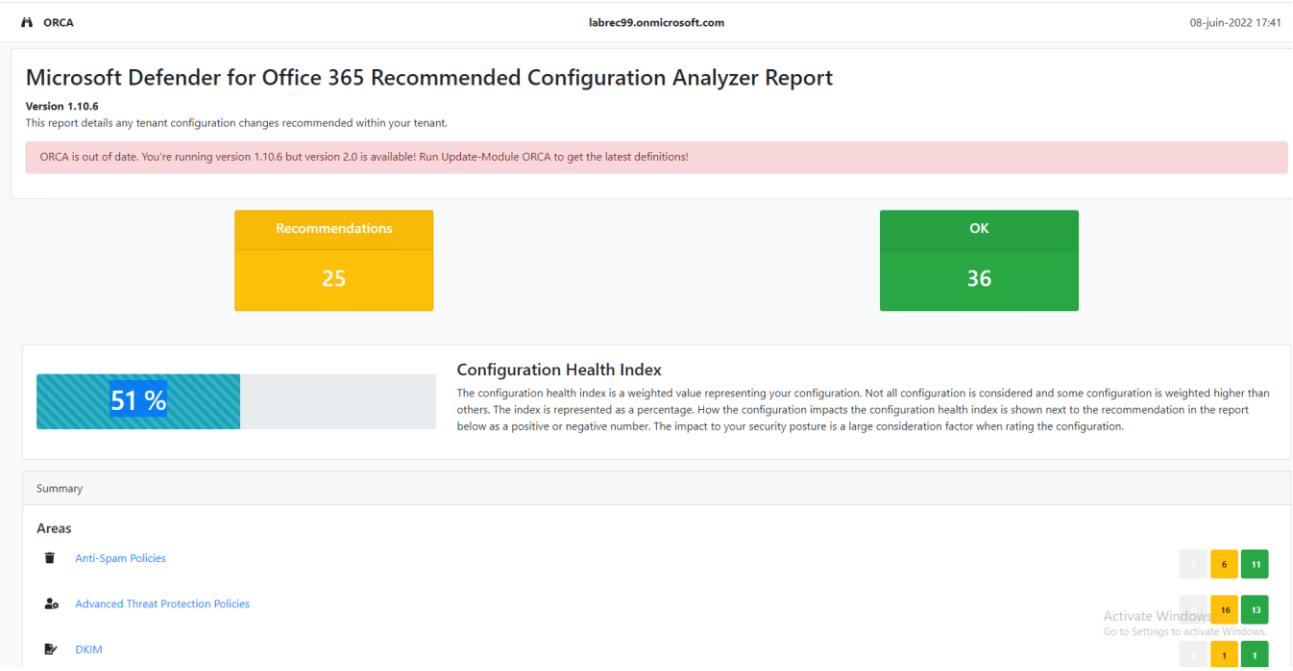
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365?view=o365-worldwide

Attention la version 2.0 d'Orca pose des problèmes.

La version 1.10.6 fonctionne sans problème.

Install-Module -Name ORCA -RequiredVersion 1.10.6

Get-ORCAReport



4.2 Boîtes aux lettres (permissions, transfert automatique)

Utiliser *Harden 365* pour lister les boîtes aux lettres avec du transfert automatique vers des boîtes aux lettres externes. Un attaquant peut mettre en place ce genre de transfert pour accéder aux contenus des boîtes aux lettres.

Exporter les délégations d'administration au niveau des boîtes aux lettres Exchange Online avec la solution *Harden 365*.

4.3 Paramètres de l'antispam

Déterminer la solution d'antispam utilisé pour sécuriser les services Microsoft 365.

Si Exchange Online Protection et Microsoft 365 Defender for Office 365 sont utilisés effectuer les actions suivantes :

- Exécuter Microsoft Orca pour voir les bonnes pratiques à implémenter.
- Lancer Harden 365 pour créer les règles de sécurité préconisées par Microsoft Orca.
- Prévoir des ateliers pour voir les exceptions à mettre en place pour éviter que ces outils bloquent les campagne emailing ou les envoies de courriels par les applications d'entreprise.

4.4 Mode hybride

Déterminer si l'organisation est configurée en mode hybride.

Si c'est le cas, le ou les serveurs *Exchange On-Premise* doivent être dans une unité d'organisation Tier 0 et sécuriser comme tel.

Une analyse de la configuration des serveurs *Exchange On-Premise* doit être réalisée.

Voir le standard AD (Harden AD).

5 OneDrive, SharePoint Online, et Teams :

5.1 Lancer Microsoft Orca

Analyser les paramètres de sécurité de *OneDrive*, *SharePoint Online*, *Teams* en exécutant *Microsoft Orca*.
Ce dernier est inclus dans *Harden 365*.
La procédure pour utiliser cet outil est présenter dans le chapitre sur Exchange Online.

5.2 Lister les liens anonymes et supprimer ceux qui ne sont plus utiles

Exporter tous les liens SharePoint Online et OneDrive. Indiquer en rouge dans le tableau de bord :

- Les liens accessibles par un utilisateur anonyme.
- Les liens accessibles par un utilisateur externe sans durée de vie.

6 Microsoft Azure AD Connect

6.1 Configuration de l'annuaire Active Directory

Lister les suffixes UPN de la forêt AD.

Chaque domaine DNS déclaré sur le Tenant Microsoft 365 doit être ajouté au niveau de la forêt AD dans lequel l'outil *Microsoft Azure AD Connect* est déployé.

Vérifier que tous les comptes synchronisés disposent d'un attribut *UserPrincipalName* avec un suffixe Dns publique. Dans le cas contraire, il faut utiliser la fonctionnalité *Alternate Login ID* (utilisation de l'attribut Mail pour générer l'attribut *UserPrincipalName* (Azure AD).

Etendre le schéma pour Exchange 2019 CU11.

Vérifier que le schéma n'est pas déjà étendu avec une ancienne version Exchange.

Voir le standard AD.

Installation sur un serveur d'administration les outils d'administration Exchange pour disposer des consoles Exchange

https://blog.expta.com/2022/10/how-to-setup-exchange-management-tools.html?m=1

6.2 Utiliser Azure AD Connect Configuration Documenter

Cet outil permet de documenter la configuration d'un serveur *Azure AD Connect*.

https://github.com/microsoft/AADConnectConfigDocumenter/releases

6.3 Vérifier que tous les comptes Azure avec des rôles sont des comptes InCloud

Les comptes d'administration Azure AD doivent être *InCloud*.

Dans le cas contraire, un attaquant disposant des accès Tier 0 dans l'annuaire AD pourrait prendre le contrôle d'un Tenant Microsoft 365

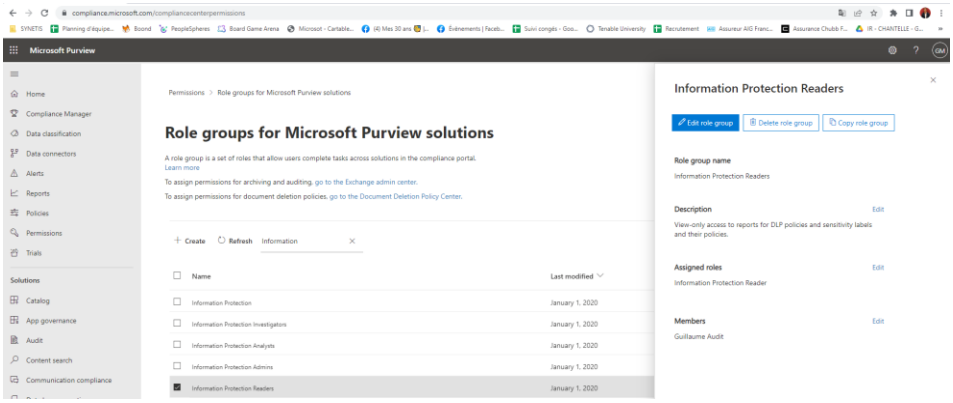
Il existe depuis 2019 un mécanisme de sécurité qui empêche un compte AD de se resynchroniser (soft matching) avec un compte Azure AD avec un rôle d'administration (pour éviter les attaques AD -> Azure AD).

7 Analyse des paramètres Microsoft Purview Information Protection et Microsoft DLP

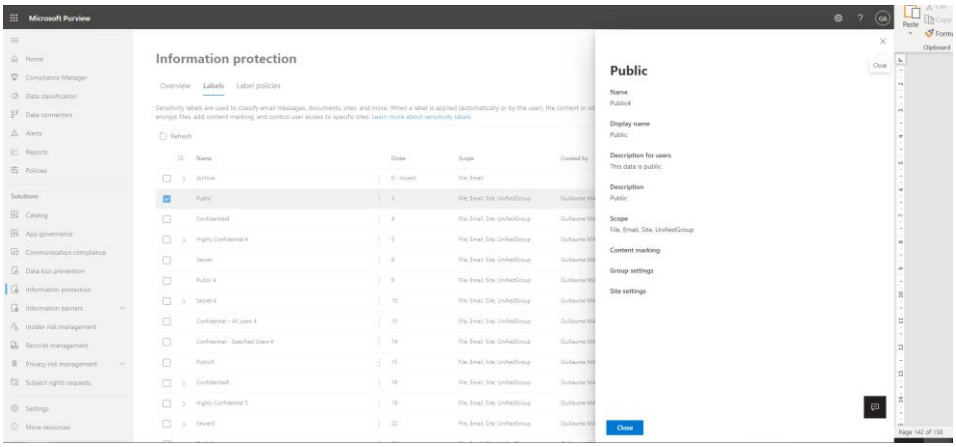
7.1 Script d'audit

Le script ci-dessous permet d'afficher la configuration des étiquettes de confidentialités et des politiques d'étiquettes de confidentialité.

Pour exécuter ce script, il est nécessaire de disposer d'au moins un compte Azure AD sans licence avec les rôles *Global reader* et *Protection Reader* (configuration depuis le portail Azure AD).



Le compte alors accès aux informations depuis le portail *Microsoft Purview*.



Le script est disponible ci-dessous (à renommer en *.PS1*).

Audit-MIPV2.txt

7.2 Utilisation du module PowerShell CAMP

Il est possible d'utiliser le module CAMP.

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-mcca?WT.mc_id=365AdminCSH_AdminPortalGlobalSearch%3FWT.mc_id%3D365AdminCSH_globalsearch&view=o365-worldwide

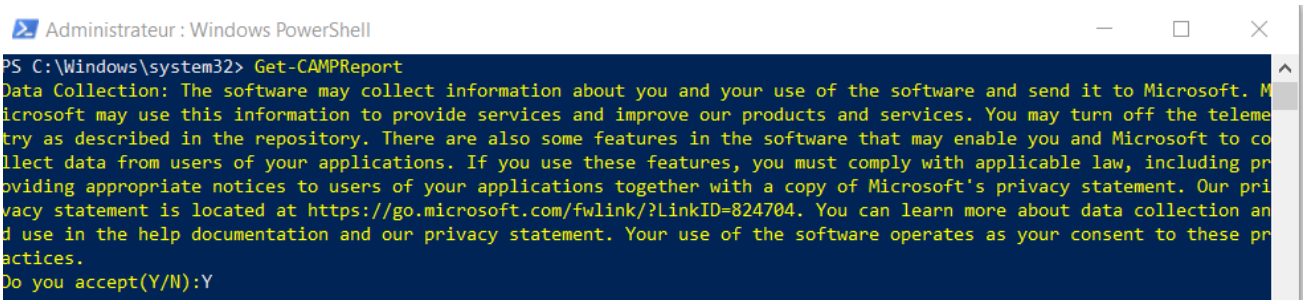
Taper les commandes suivantes :

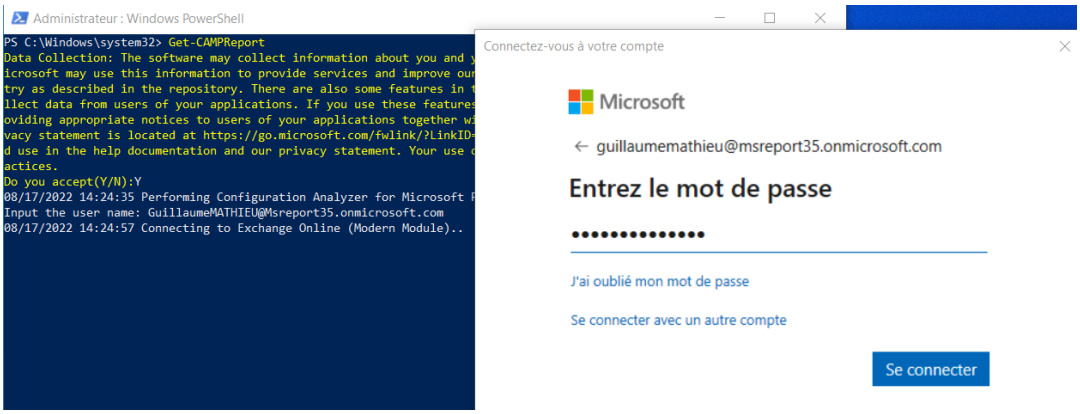
Uninstall-Module ExchangeOnlineManagement -Force

Install-Module -Name ExchangeOnlineManagement

Install-Module -Name CAMP

Get-CAMPReport

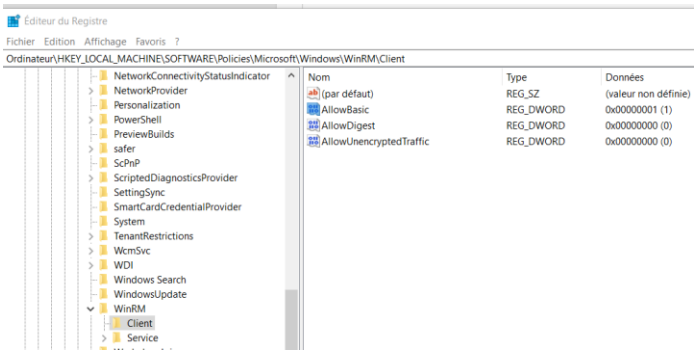


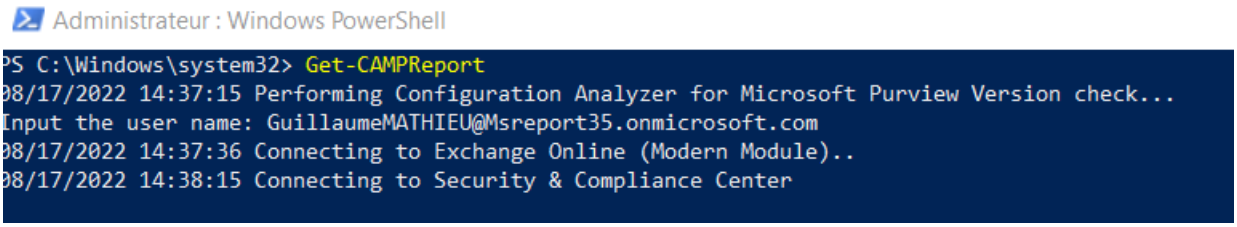


L'erreur suivante apparaît si vous disposez d'une ancienne version d'Exchange Online Management Shell.

Il faut aussi activer l'authentification basique pour *WinRM*.

http://www.mistercloudtech.com/2022/02/28/how-to-fix-create-powershell-session-is-failed-using-oauth-exo-v2-powershell-error/





Fichiers résultats.

CAMP.zip

Pour chaque point, l’outil présente ses préconisations.