Restitution Projets

Sécurité Active directory
Fonctionnalité Réinitialisation mot de passe en libre - service

Sommaire

01

Rappel contexte

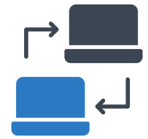
Rappel contexte

Remédiation Post Analyse

- Mise en conformité post analyse Sécurité AD

Self – service password reset

- Apporter une totale autonomie pour les utilisateurs concernant le changement de mot de passe
- Soulager le support des appels de réinitialisation mot de passe utilisateur



Connexion VPN avec les identifiants LDAP AD

- Etablir une relation entre le VPN du Fortigate avec l'annuaire active directory via le protocole LDAP pour que les utilisateurs puissent se connecter avec leurs identifiants AD.

02

LOT 1 : Sécurité Active Directory

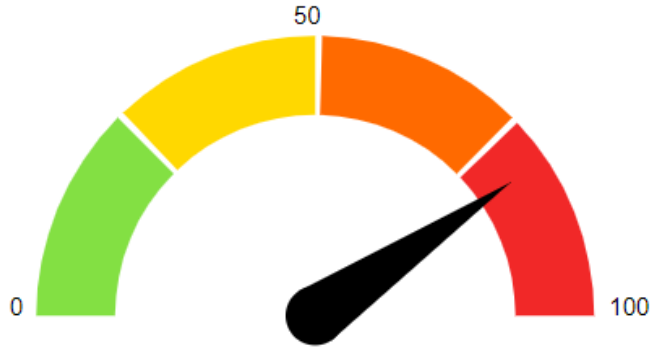
LOT 1 – Sécurité Active Directory

En date du 29 Novembre 2023

- Healthcheck analysis

Date: 2023-11-29 - Engine version: 3.1.0.1

Indicators



Domain Risk Level: 81 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

02 LOT 1 – Sécurité Active Directory

Corrections apportées :

- ✓ Remédiation des comptes dont le mot de passe n'expire jamais
- ✓ Comptes administrateurs / utilisateurs sensibles
- ✓ Compte Administrateur de clé contrôle total sur le domaine sedif.local
- ✓ Mot de passe Objet AzureADSSOACC
- ✓ Forcer la réinitialisation des comptes Admin
- ✓ Retirer du groupe Administrateurs les comptes non approuvés.

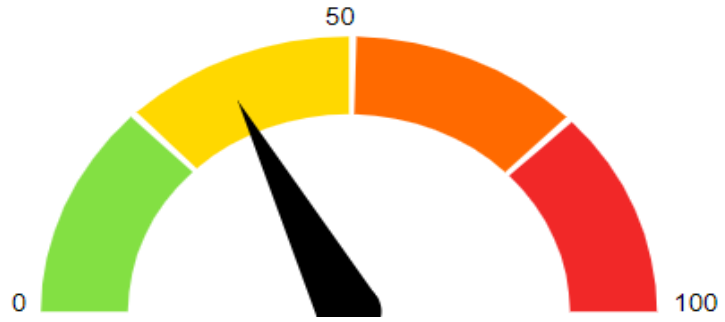
LOT 1 – Sécurité Active Directory

En date du 08 mars 2024

- Healthcheck analysis

Date: 2024-03-08 - Engine version: 3.1.0.1

Indicators



Domain Risk Level: 36 / 100

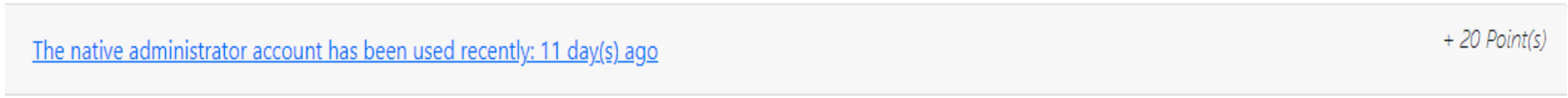
It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

LOT 1 – Sécurité Active Directory

Quelques points à améliorer

- ✓ Protocole NTLM et SMBv1 à désactiver après avoir mis à jour la GED

- ✓ Auditer le compte administrateur afin de ne plus l'utiliser en production

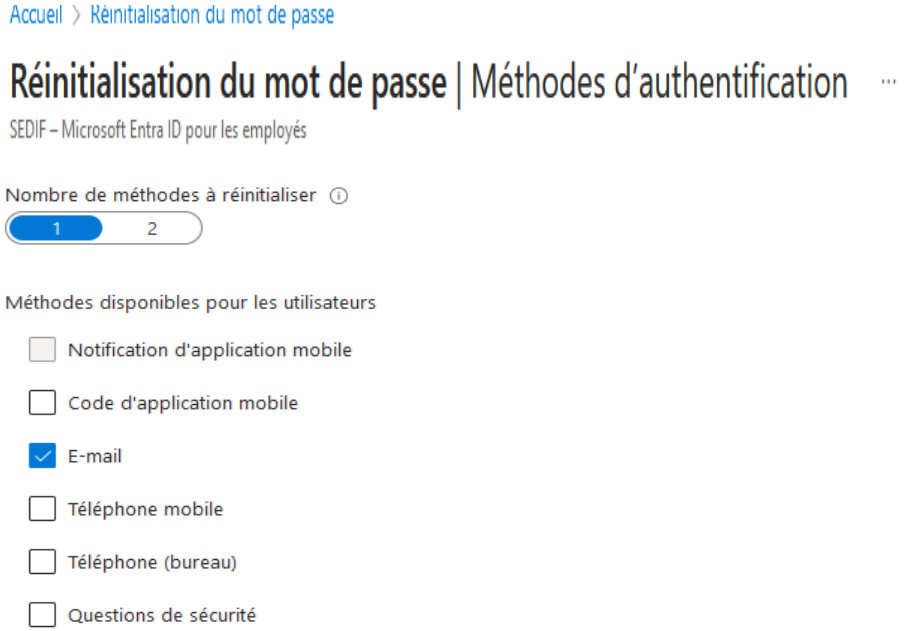


- ✓ Appliquer la stratégie de mot de passe au niveau domaine. **EDIT : planification le 13 mars au matin**

LOT 2 – Portail réinitialisation mot de passe en libre – service

LOT 2 – Portail réinitialisation mot de passe en libre – service

Paramétrage SSPR



LOT 2 – Portail réinitialisation mot de passe en libre – service

Fonctionnalité SSPR

Vue d'ensemble | Supervision | Propriétés | Recommandations | Tutoriels

Rechercher dans votre locataire

Informations de base

Nom

ID du client

Domaine principal

Licence Microsoft Entra ID P1

Réinitialisation du mot de passe | Intégration locale

Microsoft Entra ID pour les employés

Agent de synchronisation Microsoft Entra Connect

État : Configuration terminée

Voir les détails

Gérer les paramètres

Activer la réécriture du mot de passe pour les utilisateurs synchronisés

GRP_Licence_F1 | Règles d'appartenance dynamique

Groupe

Configurer les règles | Valider les règles (préversion)

Vous pouvez utiliser le générateur de règles ou la zone de texte de syntaxe de la règle pour créer ou modifier une règle d'appartenance dynamique. En s

et/Ou	Propriété	Opérateur	Valeur
	extensionAttribute2	Match	F1

+ Ajouter une expression + Obtenir des propriétés d'extension personnalisée

Syntaxe de la règle

```
(user.extensionAttribute2 -match "F1")
```

Produits	État	Services activés
Microsoft 365 F1	Actif	5/18

Microsoft Entra ID P1

LOT 2 – Portail réinitialisation mot de passe en libre – service

1. Lien pour enregistrement

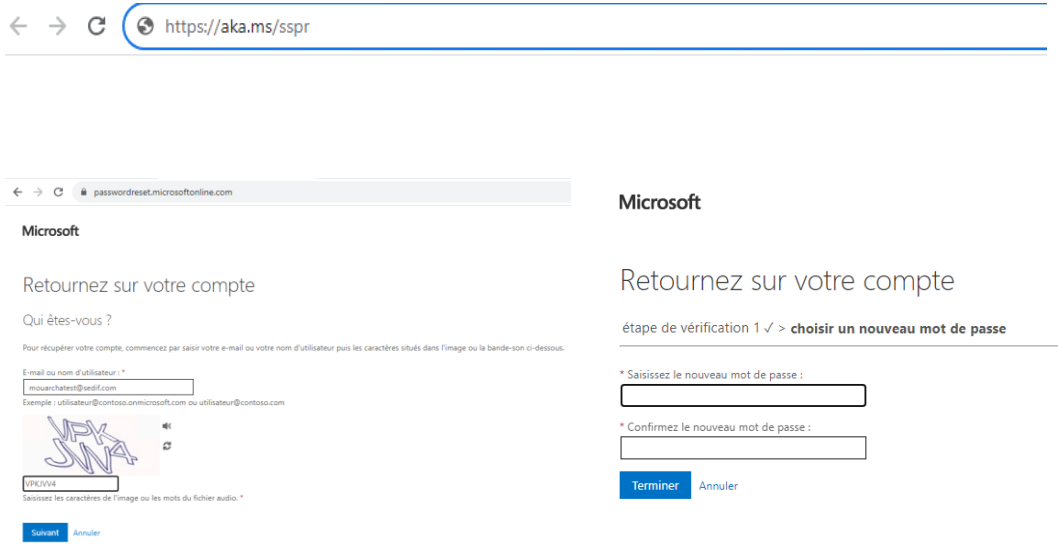
https://aka.ms/ssprsetup

Ce lien permet d'ajouter un mode de vérification pour la première configuration SSPR

2. Lien pour modifier son mot de passe

https://aka.ms/sspr

Ce lien permet, une fois la méthode réalisée, de modifier son mot de passe et d'être réécrit dans l'AD local.



LOT 2 – Portail réinitialisation mot de passe en libre – service

1. En Résumé

- ✓ Choisir des personnes qui pourront bénéficier de cette fonctionnalité
- ✓ Ajouter la valeur EXT dans ‘ExtensionAttibute1’ pour être membre du groupe GRP_SSPR
- ✓ Ajouter la valeur F1 dans ‘ExtensionAttibute2’ pour être membre du groupe GRP_Licence
- ✓ Ajouter le compte dans le groupe LOCAL GS_AZUREAD_SYNC

Nom	Type	Description
GS_AZUREAD_SYNC	Groupe de sécurité - Global	Compte pour ajouter les utilisateurs dans le synchronisation AD connect

- ✓ Suivre les 2 étapes d’enrollment pour modifier son mot de passe.
  - ➢ Lien pour enregistrement
  - ➢ Lien pour réinitialiser son mot de passe

04

LOT 3 – Accès VPN aux comptes externe

04 LOT 3 – Accès VPN aux comptes externe

1- Technique

- ✓ Le socle technique est mis en place
- ✓ Les groupes dans l'Active directory sont créés

2- Organisationnel

➔ Identifier tous les comptes externes et indiqué le nom de l'entreprise

➔ Les utilisateurs auront dans la phase de changement, la possibilité de se connecter avec leurs comptes AD mais aussi leurs comptes VPN.

05

Conclusion

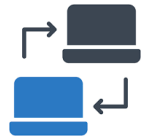
05 Conclusion

LOT 1 – Sécurité Active directory

- Point sur la GED à faire évoluer

LOT 2 – Fonctionnalité SSPR

- Qui doit en bénéficier ?



LOT 3 – Connexion VPN avec les identifiants LDAP AD

- Réorganiser l'OU Compte Externe

Je vous remercie pour votre attention.