Sécurisation des environnements

Active Directory et Windows

avec

ISARS Pour Active Directory & Windows

La situation actuelle de la cybermenace

- ✓ Des compromissions de plus en plus nombreuses avec le contexte actuel
  L'ANSSI préconise à toutes les sociétés d'augmenter leur niveau de cybersécurité et de mettre en place les préconisation de cybersécurité de l'AD

- ✓ Une augmentation significative des attaques y compris dans le domaine de la santé
  D'après l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), le nombre de victimes de cyberattaques en France a été multiplié par 4.

- ✓ 95% des incidents de cybersécurité auraient pu être évités grâce à des approches simples et de bon sens pour améliorer la sécurité [1]

- ✓ Selon Microsoft : "Les mots de passe sont la cible dans près de 8 attaques sur 10" [2]

- ✓ Sécuriser uniquement les contrôleurs de domaine n'est pas suffisant, une approche globale de son environnement Active Directory et Windows est nécessaire

[1] https://www.internetsociety.org/news/press-releases/2019/internet-societys-online-trust-alliance-reports-cyber-incidents-cost-45b-in-2018/
[2] https://experiences.microsoft.fr/business/confiance-numerique-business/joy-chik-lingenieure-qui-voulait-eliminer-les-mots-de-passe/

ISARS

- ✓ Une société 100% française spécialisée dans la sécurité des environnements Active Directory et Windows proposant:
  - ✓ Une solution on-premise pour la sécurité Active Directory & Windows
  - ✓ Une solution Saas pour la sécurité Azure AD/M365/Azure

- ✓ ISARS Pour Active Directory & Windows, une solution on-premise
  - ✓ sans agent, facile à installer et déployer
  - ✓ dédiée à la sécurité des environnements Windows et Active Directory
  - ✓ intégrant l'ensemble des contrôles de l'ANSSI sur la sécurité de l'AD
  - ✓ installée sur un serveur Windows sur votre réseau interne et contenant vos données
  - ✓ disposant de tableaux de bord ANSSI et CxO pour gérer sa posture de sécurité
  - ✓ … et de rapport détaillés sur les points identifiés
  - ✓ accessible via une interface Web.

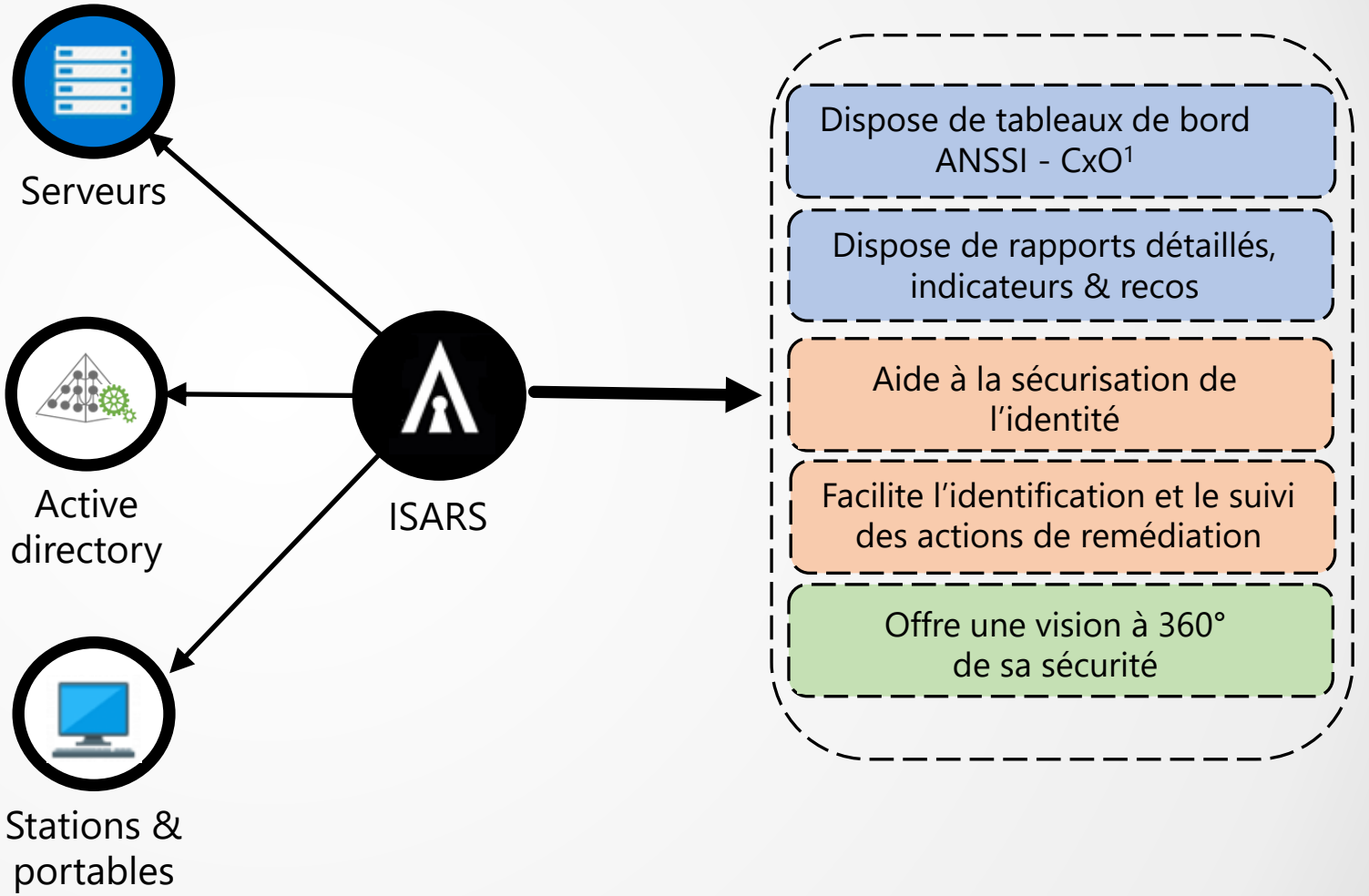
ISARS

- ✓ ISARS est membre éditeur du CIS Security (https://www.cisecurity.org/partner/isars)

- ✓ ISARS Cloud Pour Azure, une solution en SaaS
  - ➢ Dédiée à la sécurité de l'environnement Azure AD, M365 et Azure
  - ➢ Ne nécessitant qu'un compte avec des privilèges en lecture
  - ➢ Intégrant, de manière totalement automatisée les contrôles de cybersécurité
    - du CIS Benchmark M365
    - du CIS Benchmark Azure
  - ➢ Intégrant les recommandations Secure Score sur Azure AD et les abonnements
  - ➢ Disposant de fonctionnalités avancées pour mieux gérer sa sécurité (contrôles mensuels par rapports aux règles CIS, licences,..)

ISARS, une solution française de gestion de sa posture de sécurité dédiée à la sécurité Active Directory & Windows

ISARS est une **solution** centralisée on-premise et **sans agent** qui collecte des **élèments de configuration sur l'Active Directory et les équipements Windows** pour fournir automatiquement des tableaux de bord, indicateurs et rapports détaillés



[1]Active Directory – Gestion des comptes – Santé des machines Windows – Pratiques d'administration

ISARS vous aide à évaluer, renforcer et suivre le niveau de sécurité de vos environnements Active Directory & Windows

Evaluer

Évaluez votre posture de cybersécurité selon les contrôles de sécurité de l'ANSSI et les 4 piliers de la cybersécurité Microsoft :

- Active Directory
- Gestion des comptes
- Santé des appareils
- Pratiques d'adminisration

Remédier

Définissez votre plan de remédiation.

Lancez les actions de remédiation et suivez vos améliorations.

Assurez vous que les mesures ont été prises et que les corrections ont été correctement apportées.

Suivre

Assurez-vous que votre niveau de sécurité perdure dans le temps et que de nouveaux risques n'apparaissent pas.

Contrôlez périodiquement votre niveau de cybersécurité et prenez les mesures nécessaires pour renforcer votre sécurité.

Les forces d'ISARS Pour Active Directory & Windows

- ✓ ISARS Pour Active Directory & Windows est sans agent, rapide et a une approche audit avec planification des collectes de données

- ✓ ISARS Pour Active Directory & Windows couvre sur l'ensemble de l'environnement Microsoft (AD, Serveurs, postes de travail). Indépendant du nombre de domaines ou forêts.

- ✓ ISARS Pour Active Directory & Windows permet la génération automatique de rapports CxO & ANSSI et de rapports détaillés permettant aux clients de connaitre précisément les dysfonctionnements et actions à effectuer.

- ✓ Le périmètre couvert est exhaustif : comptes, gpo, groupes, partages réseaux, services, taches planifiées, mots de passe, antivirus, …
  - Possibilité par exemple de voir pour un compte les groupes auxquels il appartient ainsi que les services et taches planifiées qui tournent avec ce compte sur vos différentes machines

Les forces d'ISARS Pour Active Directory & Windows

- ✓ L'approche ISARS est dynamique dans le sens où ISARS permet de suivre dans le temps son niveau de sécurité et de savoir les actions à engager avec un historique des états.
- ✓ ISARS facilite le travail des opérationnels dans les actions de nettoyage, remédiation et suivi de la sécurité et permet un gain de temps très important.
- ✓ ISARS vous aide à contrôler votre niveau de sécurité facilement et régulièrement
- ✓ ISARS intégre l'ensemble des points de contrôles Active Directory préconisés par l'ANSSI

Les clients

« *ISARS nous permet de recenser facilement l'état de la sécurité Active Directory & Windows et de suivre les actions de remédiation. Sa simplicité d'utilisation en fait un outil à la portée de toute DSI. Il est devenu incontournable au quotidien dans notre arsenal de sécurité* » :
S. Borsari, DSI, Compagnie Monégasque de Banque

ISARS est utilisé par des d'entreprises toute taille et de différents secteurs d'activité :

- ✓ Banques
- ✓ Instituts hospitaliers
- ✓ Secteur Public
- ✓ BTP
- ✓ Organisme de sécurité
- ✓ Consulting
- ✓ …

Des tableaux de bord ANSSI & CxO

Niveau de sécurité ANSSI - Points de contrôles Active Directory

1 2 3 4 5

Points importants	1
Points validés	32

Progression dans le niveau

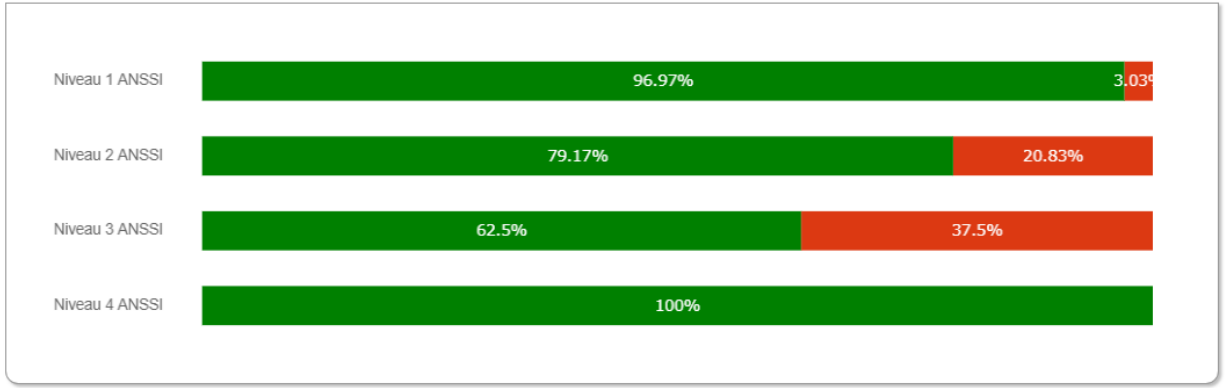
3200 / 3300

Progression globale

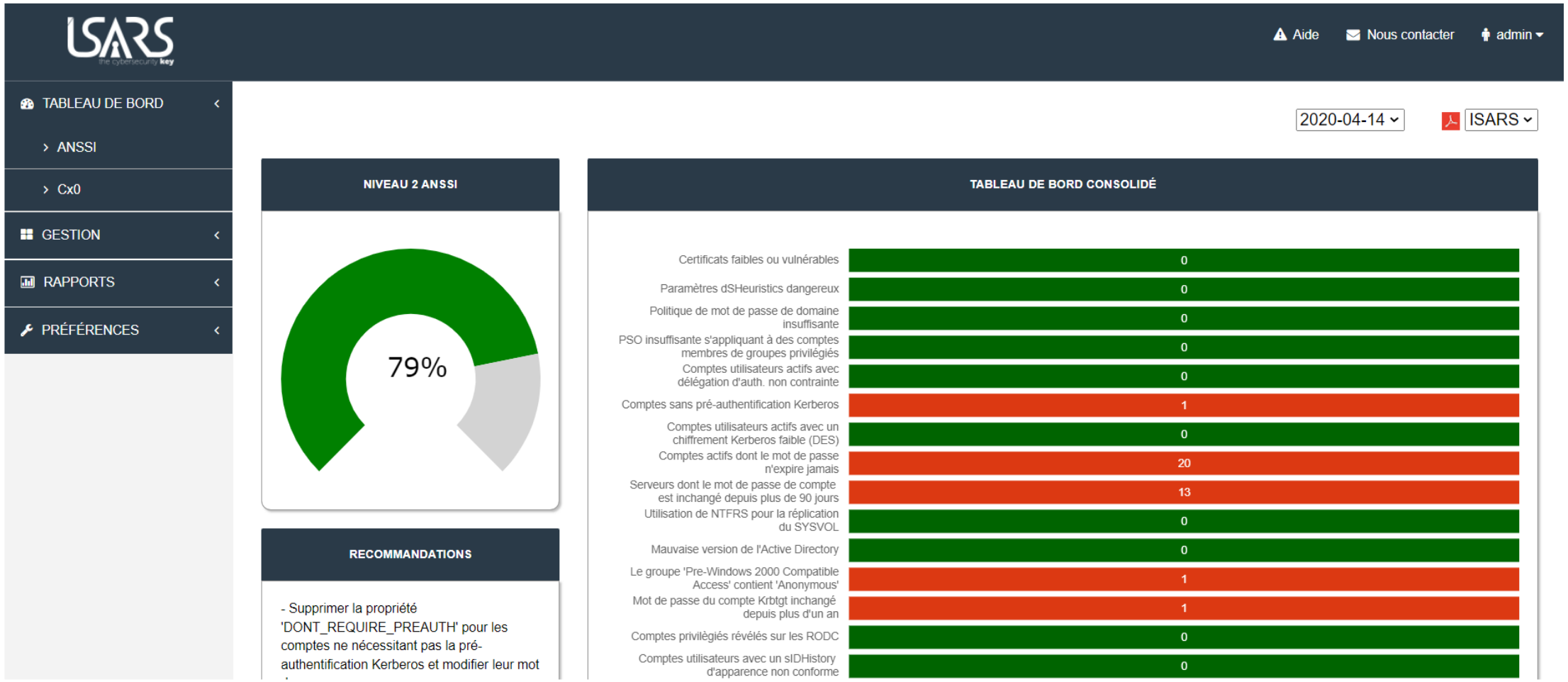
6500 / 7700

Pour plus de détails : liste de contrôles ANSSI sur l'AD.

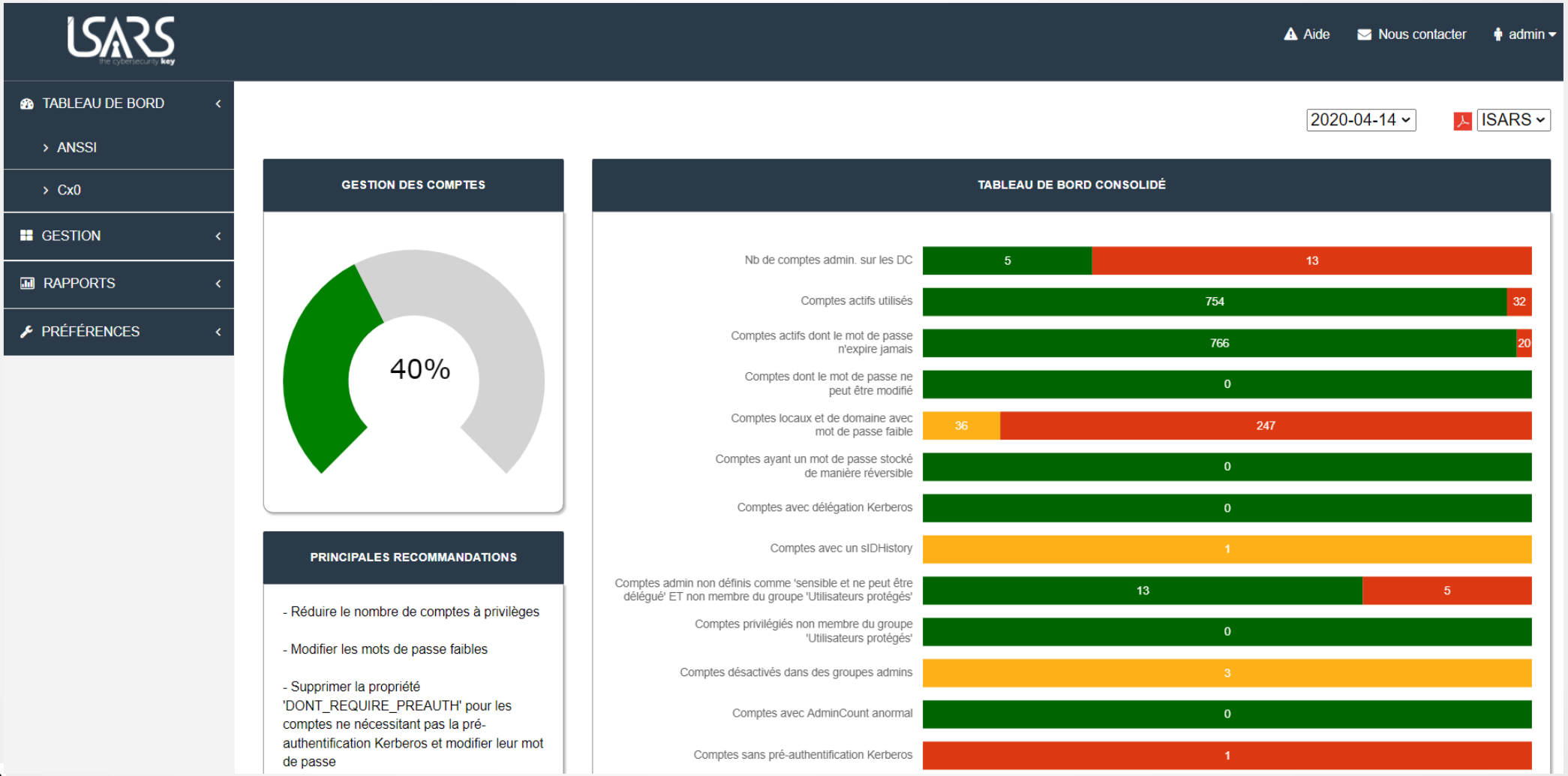
Niveau fonctionel de la forêt	Windows 2016 / 2019
Date de redémarage des DC	2021-08-29 08:28:36
Poubelle activée	Non



Un tableau de bord ANSSI pour chaque niveau de sécurité de l'AD

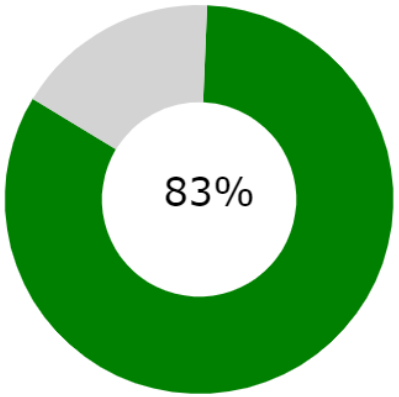


Un tableau de bord pour chacun des 4 pilliers de la cybersécurité



Des recommandations pour améliorer sa sécurité

SÉCURITÉ DE L'ACTIVE DIRECTORY

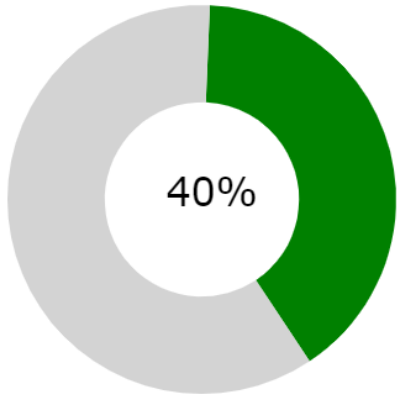


PRINCIPALES RECOMMANDATIONS

- Revoir les permissions et délégations sur les objets de l'Active Directory

- Modifier le propriétaire des objets de l'Active Directory détenus par des utilisateurs

GESTION DES COMPTES



PRINCIPALES RECOMMANDATIONS

- Réduire le nombre de comptes à privilèges

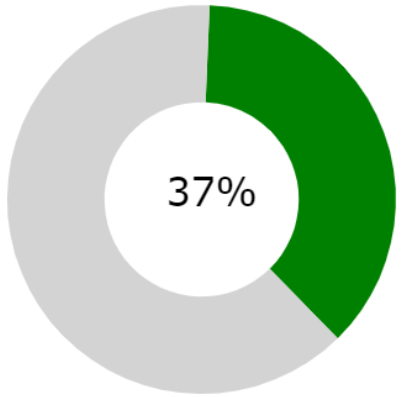
- Modifier les mots de passe faibles

- Supprimer la propriété 'DONT_REQUIRE_PREAUTH' pour les comptes ne nécessitant pas la pré-authentification Kerberos et modifier leur mot de passe

- Désactiver ou supprimer les comptes non utilisés

- Réduire le nombre de comptes dont le mot de passe n'expire jamais

SANTÉ DES MACHINES WINDOWS



PRINCIPALES RECOMMANDATIONS

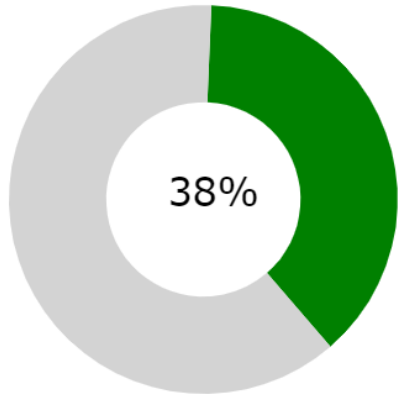
- Lancer une investigation de sécurité et réinstaller les machines compromises

- Déployer, activer et mettre à jour les antivirus sur tous les ordinateurs

- Retirer, à défaut isoler, les machines Windows avec des OS qui ne sont plus pris en charge et qui ne peuvent pas être corrigés

- Utiliser des comptes de services managés; à défaut réduire les privilèges des comptes de services

PRATIQUES D'ADMINISTRATION



PRINCIPALES RECOMMANDATIONS

- Réduire les privilèges attribués aux utilisateurs et groupes

- Modifier le mot de passe du compte krbtgt

- Déployer LAPS sur tous les postes de travail

- Définir des stations d'administration dédiées pour chaque compte d'administration

- Supprimer les comptes non admin du groupe 'opérateurs de serveur'

Vue détaillée d'un compte utilisateur

Rechercher un compte / groupe

Informations sur le compte ISARS\services

Domaine	Compte	Nom complet	Nom	Prénom	Commentaire	Privilège
ISARS	services	services				Administrateur

Désactivé?	Bloqué?	Date d'expiration	Dernière connexion	Dernière connexion 2	Entreprise	Titre	Département	Bureau
Non	Non		2019-09-25 00:00:00	Jamais				

Dernier chgt de mot de passe	Le mot de passe n'expire jamais	Mot de passe réversible?	Essais infructueux	Créé le	Modifié le	Carte à puce requise?
2016-03-02 10:11:05	Oui	Non	0	2015-01-25 17:02:15	2016-03-02 10:11:05	Non

Liste des groupes dont ce compte est membre (25)

Information sur le mot de passe du compte (0)

Liste des services tournant avec ce compte (47)

Liste des tâches planifiées tournant avec ce compte (19)

Afficher 10 lignes

Rechercher:

Domaine	Ordinateur	Tâche planifiée	Chemin	Activée ?	Mot de passe stocké?
ISARS	isacft1.isars.dom	Changement Date Exploitation	C:\proc\creationdateexploitation.vbs	Oui	Oui
ISARS	isacft1.isars.dom	Scan_envoi_sepa	C:\Axway\Transfer_CFT\runtime\exec\scan_envoi_sepa.bat	Oui	Oui
ISARS	isafile1.isars.dom	Suivi Replication	C:\isars\proc\Rapport_batch.bat	Oui	Oui
ISARS	isarfdb.isars.dom	Sauvegarde Oracle	D:\Install\isars\Database\DB\TOOLS\IMPORT_EXPORT\Sauvegarde.bat	Oui	Oui

Vue détaillée des partages réseaux accessibles en lecture pour tout le monde

Rapport sur les partages en lecture

Filtrer les résultats

62 résultats pour le groupe ISARS (2020-03-24 16:38:37)

Tous les domaines | ISARS

Afficher 25 lignes

Rechercher:

Domaine	Ordinateur	Partage réseau	Chemin	Commentaire	Propriétaire	Utilisateurs autorisés
ISARS	cis-001.isars.dom	E	E:\		BUILTIN\Administrateurs	
ISARS	cis-001.isars.dom	passport	G:\		BUILTIN\Administrateurs	Tout le monde
ISARS	cis-001.isars.dom	scan	D:\base_clients		ISARS\ellocos	Tout le monde
ISARS	cis-018.isars.dom	scan	D:\base_clients		ISARS\Administrateur	Tout le monde
ISARS	isaav1.isars.dom	AVCLIENTS	D:\AVCLIENTS		BUILTIN\Administrators	Tout le monde
ISARS	isaav1.isars.dom	jdb	D:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\inbox\content\incoming		BUILTIN\Administrators	Tout le monde
ISARS	isabkp1.isars.dom	Backup_Exec_2012_14.0.1798	C:\Install\Backup_Exec_2012_14.0.1798		BVSBKP1\svc_veeam	Tout le monde
ISARS	isabkp1.isars.dom	BE	C:\Install\Backup_Exec_2012_14.0.1798		BUILTIN\Administrators	Tout le monde
ISARS	isacft1.isars.dom	CFT$	D:\CFT		BUILTIN\Administrateurs	Tout le monde
ISARS	isadc1.isars.dom	CertEnroll	C:\Windows\system32\CertSrv\CertEnroll	Partage de services de certificats Active Directory	BUILTIN\Administrateurs	Tout le monde
ISARS	isadc1.isars.dom	files$	C:\DFSRoots\files$		BUILTIN\Administrateurs	Tout le monde
ISARS	isafile1.isars.dom	DAG.isars.dom	D:\quorummns	File share witness created for microsoft exchange database availability group DAG.	BUILTIN\Administrateurs	Tout le monde
ISARS	isafile1.isars.dom	Partage_fic	D:\Partage_fic		BUILTIN\Administrateurs	Tout le monde

Merci

sales@isars.company