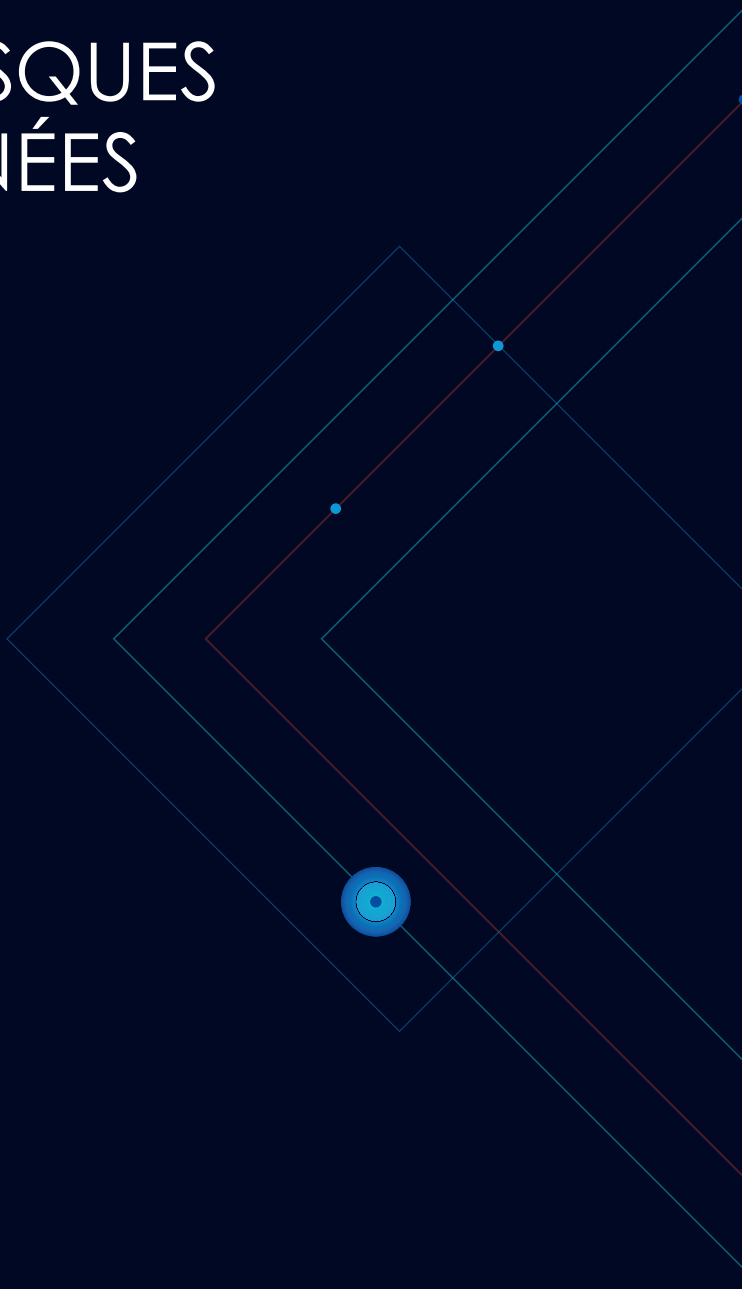
ÉVALUATION DES RISQUES RELATIFS AUX DONNÉES

RAPPORT TYPE: ACME

Vous voulez savoir où vos données sont le plus exposées aux menaces ?

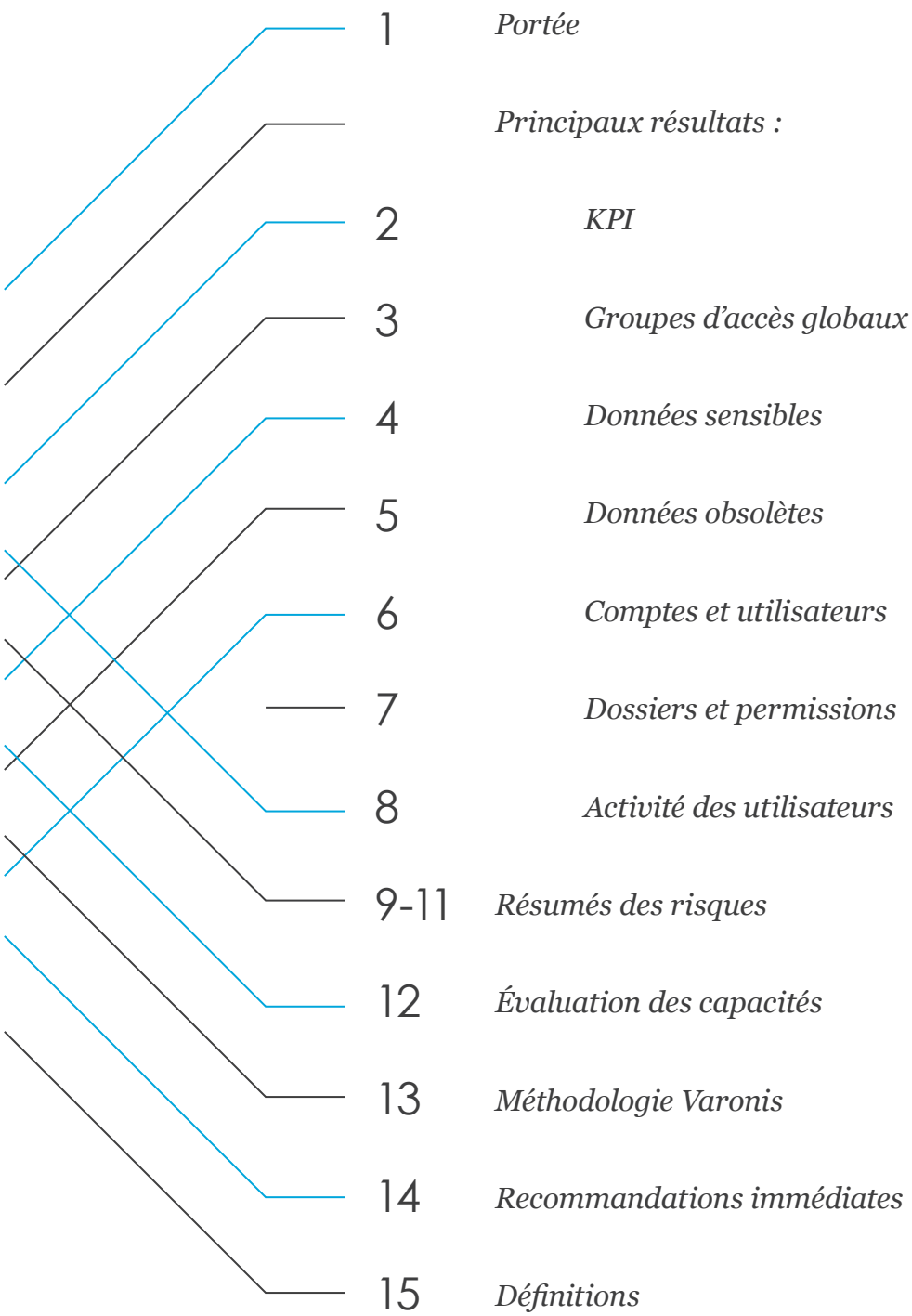
Nous allons vous le montrer.

L'Évaluation des risques relatifs aux données Varonis est un rapport détaillé basé sur les données de votre entreprise :
Analysez les risques, identifiez les atouts et faiblesses, faites la synthèse des principaux résultats, mettez en évidence les vulnérabilités de sécurité et obtenez des conseils de remédiation classés en fonction de leur priorité.



VARONIS

SOUS LE CAPOT



PORTÉE DE L'ÉVALUATION DES RISQUES RELATIFS AUX DONNÉES

Un échantillon de la portée des dépôts de données surveillés dans le cadre de ce rapport : il comprend données, dossiers, fichiers et droits, utilisateurs et comptes de groupes. Parmi les domaines à risque mis en évidence figurent les données sensibles surexposées, les problèmes de contrôle d'accès, etc.

SERVEURS DE FICHIERS ET SOURCES DE DONNÉES CONTRÔLÉS

- CIFS_FS_1
- CIFS_FS_2
- CIFS_FS_3
- CIFS_FS_4
- CIFS_FS_5
- NS_FS_1
- EXCH_1
- SP_1

SOMMAIRE

- 331,237 GB de données
- 90,348,156 dossiers
- 1,617,176,767 fichiers
- 701,387,576 entrées d'autorisation

ACTIVE DIRECTORY

- 8,580 comptes utilisateur
- 14,427 groupes
- 9,268 comptes d'ordinateur
- 420 utilisateurs désactivés

Un échantillon des données d'ACME a été analysé ; les risques ont été évalués dans les domaines suivants:

- Données sensibles et classées qui sont surexposées et courent un risque
- Processus de contrôle d'accès et d'autorisation
- Surveillance des accès privilégiés et d'utilisateurs finaux
- Structure d'Active Directory
- Structure de NTFS et des autorisations d'accès
- Performances de la rétention de données
- Conformité aux réglementations en vigueur

Nombre de dossiers dotés d'un accès de groupe global

66,502,975 dotés d'un accès de groupe global

Fichiers sensibles avec accès de groupe global

339,213,456 Fichiers sensibles avec accès de groupe global

Nombre de dossiers contenant des données obsolètes

85,377,723 dossiers contenant des données obsolètes

Fichiers contenant des données sensibles

950,534,645 Fichiers contenant des données sensibles

Nombre de dossiers comportant des SID non-résolus.

58,419

dossiers comportent des SID non-résolus.

Comptes utilisateurs avec mots de passe sans date d'expiration.

1,182

Comptes utilisateurs avec mots de passe sans date d'expiration.

GROUPES D'ACCÈS GLOBAUX:

Les groupes d'accès globaux permettent à tous les membres d'une organisation d'accéder à ces dossiers. Les groupes d'accès globaux sont des groupes tels que Tous, Utilisateurs du domaine et Utilisateurs authentifiés.

La surexposition des données est une vulnérabilité courante. Les professionnels de l'informatique estiment qu'il faut environ 6 à 8 heures par dossier pour localiser et supprimer manuellement des groupes d'accès globaux. Ils doivent identifier les utilisateurs qui ont besoin de disposer d'un accès, créer et appliquer les nouveaux groupes et les remplir avec les utilisateurs autorisés.

RÉSUMÉ DES RISQUES:

Bas Moyen Haut

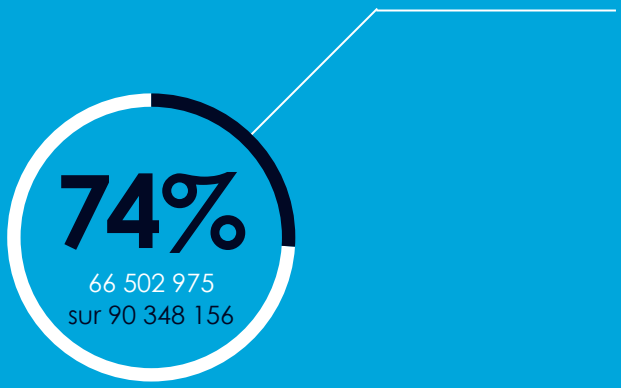
- L'accès excessif est une des principales causes de piratage de données.
- La surexposition des données sensibles et critiques constitue un risque important
- Les droits utilisateurs obsolètes sont exploités et utilisés à des fins malveillantes

ACTIONS RECOMMANDÉES:

- Retirez les droits de groupes d'accès globaux pour identifier les dossiers accessibles aux groupes d'accès globaux
- Placez les utilisateurs actifs dans un nouveau groupe
- Remplacez le groupe d'accès global par le nouveau groupe dans la LCA

66,5 millions de dossiers

dotés d'un accès de groupe global



RÉPARTITION DES ACCÈS DE GROUPE GLOBAL

- CIFS_FS_2 11%
- CIFS_FS_3 7%
- CIFS_FS_4 20%
- SP_FS_1 44%
- EXCH_FS_1 18%

FICHIERS SENSIBLES AVEC ACCÈS DE GROUPE GLOBAL

- CIFS_FS_2 2%
- CIFS_FS_3 1%
- CIFS_FS_4 2%
- SP_FS_1 82%
- EXCH_FS_1 13%

DONNÉES SENSIBLES:

De nombreux fichiers contiennent des informations critiques sur les employés, les clients, les projets, les clients finaux ainsi que d'autres contenus importants pour l'entreprise. Bien souvent, ces données sont soumises à des normes, telles que SOX, HIPAA, PCI, le GDPR de l'UE, GLBA, etc.

Les données sensibles ouvertes aux groupes d'accès globaux constituent un risque important pour l'entreprise et doivent être identifiées et corrigées afin que seuls les utilisateurs adéquats puissent y accéder.

RÉSUMÉ DES RISQUES:

Bas — Moyen — Haut

- Parmi les données sensibles figurent souvent les informations les plus confidentielles et les plus recherchées : données à caractère personnel, informations de carte de crédit, propriété intellectuelle, e-mails, etc.
- L'accès excessif est une des principales causes de piratage de données
- La surexposition des données sensibles et critiques constitue un risque important

ACTIONS RECOMMANDÉES:

- Analysez, classifiez et surveillez les données sensibles (où elles se trouvent, qui y a accès et qui y accède réellement)
- Mettez en place et appliquez un modèle de moindre privilège
- Appliquez une politique de sécurité centrée sur les données pour respecter les réglementations qui régissent les données sensibles

+950 millions

de fichiers contiennent des données sensibles (950 534 645)

+339 millions

(339,213,456) de fichiers sensibles sont ouverts aux groupes d'accès globaux

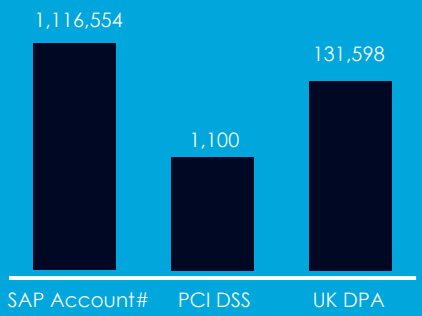
Plus de la moitié des informations sensibles résident sur un serveur de fichiers : SP_FS_1

RÉPARTITION DES FICHIERS SENSIBLES

- CIFS_FS_2 13%
- CIFS_FS_3 12%
- CIFS_FS_4 8%
- SP_FS_1 54%
- EXCH_FS_1 13%

NOMBRE TOTAL D'OCCURRENCES PAR TYPE

- SAP Acc# 1,116,554
- PCI DDS 1,100
- UK DPA 131,598



DONNÉES OBSOLÈTES:

Les données obsolètes (conservées au-delà d'une période prédéterminée ou qui n'ont pas été utilisées pendant longtemps) peuvent occasionner des frais de stockage et de gestion importants, et accroissent les risques de sécurité(inutilement).

RÉSUMÉ DES RISQUES:

Bas — Moyen — Haut

- Rapidement, les données obsolètes entraînent des problèmes de sécurité et des frais de stockage inutiles
- Les données obsolètes génèrent un risque inutile et laissent la porte ouverte au vol et à la mise en danger de ces données

ACTIONS RECOMMANDÉES:

- Identifiez les données obsolètes et déterminez lesquelles peuvent être déplacées, archivées ou supprimées
- Créez et appliquez une politique cohérente pour la gestion des données obsolètes

253 168 Go

de données obsolètes

+85 millions

(85,377,723)

de dossiers contiennent des données obsolètes

Plus de 75 % des données évaluées dans le cadre de ce scénario sont obsolètes.

QUANTITÉ DE DONNÉES OBSOLÈTES

- CIFS_FS_2 25%
- CIFS_FS_3 22%
- CIFS_FS_4 8%
- SP_FS_1 29%
- EXCH_FS_1 16%

DONNÉES OBSOLÈTES CONTENANT DES INFORMATIONS SENSIBLES

- CIFS_FS_2 14%
- CIFS_FS_3 11%
- CIFS_FS_4 9%
- SP_FS_1 53%
- EXCH_FS_1 13%

COMPTES UTILISATEURS

- **1 182** comptes utilisateurs disposent de mots de passe sans date d'expiration.
- **2 555** comptes utilisateurs sont périmés mais toujours activés.
- **46%** (4 635) des comptes utilisateurs comportent des recommandations de suppression.

GROUPES

- **14%** des groupes de sécurité ne comportent aucun utilisateur (2034)
- **26%** des groupes de domaines sont vides

1 182

comptes utilisateurs disposent de mots de passe sans date d'expiration.

COMPTES ET UTILISATEURS :

Utilisateurs dont les mots de passe n'expirent jamais

Les comptes dont les mots de passe n'expirent jamais peuvent rester exposés au piratage indéfiniment.

Utilisateurs obsolètes actifs

Les comptes obsolètes actifs conservent les droits d'accès qui étaient les leurs lorsqu'ils étaient en activité et sont la cible de tentatives de piratage et d'utilisation malveillante.

Groupes de sécurité vides

Bien souvent, les groupes de sécurité vides ne sont plus nécessaires et peuvent être exploités pour accéder à des données et à des ressources.

RÉSUMÉ DES RISQUES:

Bas | Moyen | Haut

- Les droits utilisateur périmés et comptes obsolètes sont exploités et utilisés à des fins malveillantes
- Les utilisateurs qui ont accès à des données sensibles alors qu'ils n'en ont pas besoin présentent un risque important pour l'entreprise
- Les comptes obsolètes mais actifs présentent un risque inutile

ACTIONS RECOMMANDÉES:

- Examinez les comptes obsolètes actifs pour déterminer s'ils ont une utilité
- Supprimez ou désactivez les comptes selon les besoins
- Actualisez les comptes pour appliquer une politique de mot de passe fort, consistant notamment à changer régulièrement de mot de passe.

DOSSIERS

- **277 027** dossiers comportent des SID non-résolus.
- **58 419** dossiers présentent des autorisations incohérentes.
- **1 040 040** dossiers sont dotés d'autorisations uniques

PERMISSIONS

- **423 872** dossiers comportant des ACE utilisateurs directes ont été détectés.
- **25 551** dossiers protégés
- **90 348 156** dossiers sans propriétaire de données

277 027

SID non résolus

DOSSIERS & PERMISSIONS:

Identifiants sécurisés non résolus

On est en présence d'Identifiants sécurisés non résolus (SID) lorsqu'un compte figurant dans une liste de contrôle d'accès est supprimé d'AD. Les SID non résolus ne font que compliquer la situation et peuvent être exploités à des fins malveillantes.

Incohérence au niveau des droits

Les droits deviennent incohérents lorsque les dossiers ou fichiers héritent d'entrées de contrôle d'accès supplémentaires de leurs parents ou, au contraire, n'en héritent pas. Des droits d'accès peuvent être accordés ou retirés par erreur.

RÉSUMÉ DES RISQUES:

Bas | Moyen | Haut

- Les héritages incohérents ont pour conséquence d'exposer certains utilisateurs à des données auxquelles ils ne devraient pas avoir accès, ou de priver des utilisateurs de droits d'accès légitimes
- Les problèmes non résolus de SID ou d'incohérence des droits présentent un risque inutile
- Les problèmes non résolus de SID ou d'incohérence des droits présentent un risque inutile

ACTIONS RECOMMANDÉES:

- Examinez la structure des droits pour déterminer si l'unicité des dossiers est nécessaire. Si ce n'est pas le cas, autorisez les dossiers à hériter des droits de leurs parents, pour remplacer les entrées de contrôle d'accès uniques
- Identifiez les dossiers présentant des Identifiants sécurisés non résolus et retirez-les des LCA
- Identifiez les dossiers présentant des droits utilisateurs directs, placez les utilisateurs dans les groupes requis et retirez l'entrée de contrôle d'accès de l'utilisateur de la LCA

PRINCIPALES CATÉGORIES D'ALERTES DÉCLENCHÉES

- Intrusion 5
- Droit 9
- Exfiltration 2

RÉPARTITION DES FICHIERS SENSIBLES

- CIFS_FS_2 13%
- CIFS_FS_3 12%
- CIFS_FS_4 8%
- SP_FS_1 54%
- EXCH_FS_1 13%

ACTIVITÉ UTILISATEUR

- **423 110** ouvertures de fichiers
- **182 335** modifications de fichiers
- **65 120** suppressions de fichiers
- **22 965** modifications de droits

+750 000

événements d'audit, dont 950 concernant des données sensibles

ACTIVITÉ DE L'UTILISATEUR :

Activité et comportement de l'utilisateur

L'activité de l'utilisateur correspond aux activités effectuées au niveau des droits et des fichiers par les utilisateurs de l'organisation : activité sur les fichiers et droits, sur la messagerie et SharePoint, et modifications apportées aux utilisateurs et groupes de l'organisation.

Varonis surveille et analyse le comportement habituel des utilisateurs et des entités afin de vous apporter des connaissances sur tout comportement potentiellement suspect ou toute activité inhabituelle.

Nous utilisons cette analyse pour détecter et signaler les écarts de comportement, mettre les risques en évidence, découvrir les menaces internes, le ransomware, etc…

RÉSUMÉ DES RISQUES:

- Les tentatives non autorisées d'accès ou de modification de données trahissent souvent un malware, une menace interne ou une cyberattaque.
- Le comportement inhabituel d'un utilisateur (par rapport à son comportement de référence) peut être révélateur d'un détournement de compte, d'une exfiltration de données et de tentatives d'atteinte aux données
- Un accès inhabituel à des données sensibles suggère que les données sont exposées à un risque et sont susceptibles de déboucher sur un incident de sécurité

ACTIONS RECOMMANDÉES:

- Surveillez le comportement des utilisateurs et l'activité effectuée sur les fichiers
- Détectez et signalez les violations de sécurité, les comportements suspects et les activités inhabituelles
- Mettez en place des plans de réponse et des processus d'enquête pour engager une action en cas de violations potentielles de la sécurité

RISQUE FAIBLE

Plus la structure d'un système de fichiers est complexe, plus le risque de surexposition et de vulnérabilité est élevé. Des procédures et normes de gestion des accès plus simples aident à éviter que les données sensibles ne soient exposées aux menaces internes.

1 040 040 DOSSIERS SONT DOTÉS D'AUTORISATIONS UNIQUES

Recommandation:
réviser la structure des permissions afin de décider de la nécessité ou non de l'unicité d'un dossier. Si cela n'est pas nécessaire, laisser le dossier hériter de permissions parentes remplaçant les ACE uniques.

277 027 DOSSIERS COMPORTENT DES SID NON RÉSOLUS

Recommandation:
identifier les dossiers présentant des SID non résolus et les retirer des ACL.

423 872 DOSSIERS AVEC DES ACE UTILISATEURS DIRECTES

Recommandation:
identifier les dossiers dotés d'autorisations utilisateurs directes, placer les utilisateurs dans le groupe adéquat et retirer les ACE utilisateurs de l'ACL.

RISQUE MOYEN

Les données obsolètes, qu'il s'agisse de fichiers, d'utilisateurs ou de groupes, deviennent rapidement une responsabilité en termes de sécurité et une dépense de stockage inutile. Une maintenance continue et automatisée permet de garantir la sécurité de l'environnement, une utilisation efficace des ressources et des boucles de sécurité fermées, qui sont ainsi protégées de toute exploitation ou attaque par force brute.

DONNÉES PÉRIMÉES: 85 377 723 DOSSIERS CONTENANT DES DONNÉES PÉRIMÉES ; 4 381 574 FICHIERS SENSIBLES PÉRIMÉS

Recommandation:
identifier les données périmées et déterminer si elles peuvent être déplacées, archivées ou supprimées. Élaborer et mettre en œuvre une politique de gestion des données périmées cohérente.

1 182 UTILISATEURS POSSÉDANT DES MOTS DE PASSE SANS DATE D'EXPIRATION

Recommandation:
mettre les comptes à jour afin d'adopter une politique rigoureuse en matière de mots de passe, comprenant notamment le renouvellement régulier des mots de passe. Un nombre minimal de comptes de service dotés de mots de passe sans échéance doivent être conservés.

455 GROUPES IMBRIQUÉS EN BOUCLE

Recommandation:
les groupes imbriqués en boucle peuvent provoquer le plantage d'applications, consommer des ressources de processeur excessives et entraîner un comportement inattendu, car bon nombre d'applications et de scripts énumèrent l'appartenance à un groupe de manière récursive. Pour corriger le problème, identifier les groupes imbriqués en boucle et supprimer la condition circulaire.

RISQUE ÉLEVÉ

Les accès excessifs sont l'une des principales causes d'atteinte à la sécurité des données: les données sensibles et critiques surexposées représentent un risque de sécurité débilitant et les autorisations d'utilisateurs obsolètes constituent une cible d'exploitation et d'utilisation malveillante. Pour parvenir à un modèle d'accès présentant des privilèges moindres, il est indispensable de limiter l'accès uniquement à ceux qui en ont besoin: gérer les utilisateurs, éliminer les héritages rompus et les incohérences d'autorisations, mais aussi verrouiller les données sensibles.

66 502 975 DOSSIERS AVEC GROUPES D'ACCÈS GLOBAUX

Recommandation:
supprimer les autorisations de groupe d'accès global afin d'identifier les dossiers ouverts à l'accès de groupe global et leurs utilisateurs actifs: placer les utilisateurs actifs dans un nouveau groupe et remplacer le groupe d'accès global par le nouveau groupe sur l'ACL.

9 213 456 FICHIERS SENSIBLES SONT OUVERTS À L'ACCÈS DE GROUPE GLOBAL

Recommandation:
les données sensibles doivent être scannées, classées et surveillées afin d'être en sécurité sur tous les réseaux.

423 872 DOSSIERS AVEC ENTRÉES DIRECTES DE CONTRÔLE D'ACCÈS UTILISATEUR

Recommandation :
La meilleure pratique est que les groupes s'appliquent aux LCA et que les utilisateurs soient ajoutés aux groupes.
Les ECA individuels sont difficiles à gérer et à suivre. La modification des entrées de contrôle d'accès nécessite la réécriture de chaque LCA sur tous les objets hérités, et comme les exigences d'accès des utilisateurs changent fréquemment, il en résulterait des milliers d'opérations d'écriture de disques inutiles et intensifs.

2 555 UTILISATEURS OBSOLÈTES MAIS ACTIVÉS

Recommandation:
revoir les comptes obsolètes activés pour définir leur utilité. Supprimer ou désactiver les comptes selon les besoins.

NIVEAU	CAPACITÉS
COMPLET	• Suivi et état des modifications apportées à Active Directory (appartenance aux groupes, GPO, etc.)
PARTIEL	• Suivi et état des modifications apportées à la liste de contrôle d'accès • Analyse de l'accès potentiel aux objets supports de fichiers • Analyse de l'accès potentiel aux objets supports d'e-mails • Identification du contenu sensible ou réglementé • Identification du contenu périmé, non utilisé
NUL	• Suivi et état de l'utilisation des fichiers (créations, modifications, suppressions, etc.) • Suivi et état de l'utilisation des e-mails (envoi, réception, envoi comme, etc.) • Détection des activités inhabituelles sur les fichiers et les e-mails • Analyse de l'accès potentiel d'un utilisateur ou d'un groupe à plusieurs conteneurs de fichiers • Analyse de l'accès potentiel d'un utilisateur ou d'un groupe à plusieurs dépôts de courrier électronique • Déléguer le processus d'approbation des demandes d'accès aux propriétaires de données

PARCOURS OPÉRATIONNEL

Au fil de ses milliers d'interventions auprès de ses clients, Varonis a développé une méthodologie éprouvée et efficace pour permettre aux entreprises de surveiller, protéger et gérer leurs données. Notre approche centrée sur les données réduit les risques, améliore l'efficacité et aide à devenir conforme aux réglementations de type PCI, HIPAA et GDPR.

DÉTECTER : 1. PRÉPARER

- Déployer Varonis
- Déployer Varonis

Ce rapport préliminaire donne un aperçu de la première étape du Voyage opérationnel de Varonis.

DÉTECTER : 2. RENDRE OPÉRATIONNEL

- Créer un plan de réponse aux incidents en fonction des alertes, avec automatisation
- Former le personnel aux compétences de base - gestion des droits et recherche des fichiers perdus

PRÉVENIR : 3. CORRIGER

- Corriger les listes de contrôle d'accès endommagées
- Éliminer l'accès global aux données sensibles
- Éliminer les groupes d'accès globaux restants
- Éliminer les artefacts AD inutiles (groupes de sécurité inutilisés, mots de passe sans date d'expiration)
- Mettre en quarantaine/archiver/ supprimer les données obsolètes

PRÉVENIR : 4. TRANSFORMER

- Identifier les dossiers devant être attribués à des propriétaires
- Identifier les propriétaires de données
- Simplifier la structure des droits
- Fournir aux propriétaires des rapports sur leurs données

MAINTENIR : 5. AUTOMATISER

- Automatiser un workflow d'autorisation par le biais des propriétaires de données
- Automatiser les vérifications périodiques des habilitations
- Automatiser la mise au rebut, la mise en quarantaine, la mise en application de la politique

MAINTENIR : 6. AMÉLIORER

- Examiner régulièrement les risques, les alertes et les procédures pour veiller à l'amélioration continue

ÉTAPE 1

- Identifier et corriger les domaines présentant un risque élevé. Former le personnel à l'utilisation des fonctions de modélisation et de validation de DatAdvantage.
- Résoudre les problèmes de performances grâce à l'interface utilisateur de DatAdvantage.
- Créer un rapport complet basé sur les demandes d'ACME (inventaire complet sur la portée définie).
- Mettre en place un tableau de bord pour procéder au suivi des efforts de remédiation.

ÉTAPE 2

- Supprimer le groupe « Tous » et mettre en œuvre un modèle de moindre privilège dans tout l'environnement de partage Windows.
- Appliquer des groupes à vocation unique aux dossiers et partages de base. Éliminer les groupes qui donnent accès à d'autres partages ou applications.
- Identifier et désigner les divisions responsables et les propriétaires des ensembles de données d'ACME.

ÉTAPE 3

- Paramétrer l'émission d'alertes en cas d'écart dans les ressources corrigées.
- Automatiser la conservation et la migration des données en recourant à des règles, à la portée et au stockage en couches dans Data Transport Engine.
- Automatiser le processus de fourniture d'accès au partage de fichiers et procéder régulièrement à l'audit et à la rectification des droits des ensembles de données avec DataPrivilege.

DÉFINITIONS

Données inactives/périmées:

Données pour lesquelles aucun événement n'a été enregistré sur le système de fichiers depuis 180 jours.

Accès ouvert/global:

Cas dans le(s)quel(s) l'accès à une entité est ouvert à des groupes qui donnent accès à un ensemble d'utilisateurs important ou indéfini.
Un accès défini n'indique pas nécessairement qu'une entité est protégée ou sûre.

Données sensibles:

Les fichiers sensibles peuvent inclure des données réglementées (PCI, PII, HIPAA, etc.), soumises à la propriété intellectuelle et des fichiers confidentiels.

Utilisateurs activés obsolètes:

Les comptes utilisateurs qui ne sont pas désactivés mais n'ont pas été utilisés pour se connecter au domaine.

Utilisateurs dont la suppression a été recommandée:

Utilisateurs qui conservent des privilèges sur des données dont ils avaient besoin dans leurs rôles précédents, mais auxquelles ils n'ont plus besoin d'accéder.

Groupes de sécurité vides:

Groupes Active Directory ne contenant aucun utilisateur.

SID non résolus:

Les identificateurs de sécurité sont non-résolus lorsque l'on attribue les permissions de l'ACE d'un groupe ou d'un utilisateur directement au dossier et que le compte Active Directory associé de ce groupe ou cet utilisateur a été supprimé.

Dossier avec permission unique:

Dossier qui hérite son ACL d'un dossier parent et auquel s'appliquent des ACE supplémentaires.

Dossiers protégés:

Dossiers du NTFS qui contiennent une ACL définie de manière explicite et qui n'héritent d'aucune ACE de leurs dossiers parents.

A PROPOS DE VARONIS

Varonis est un pionnier en sécurité et analyse des données, spécialisé dans les logiciels de sécurité, gouvernance, conformité, et classification des données et analyse des menaces. Varonis détecte les menaces internes et cyberattaques, analyse l'activité des fichiers et comportements des utilisateurs, verrouille les données sensibles et maintient la sécurité par automatisation.

DÉMO EN DIRECT

Installez Varonis dans votre propre environnement. Rapide et simple.

https://info.varonis.com/trial-fr

ÉVALUATION DES RISQUES RELATIFS AUX DONNÉES

Obtenez une évaluation personnalisée des risques, réduisez votre profil de risque et corrigez vos problèmes de sécurité.

https://info.varonis.com/express-assessment-fr

CONTACT

Vous avez des questions ? Contactez-nous.
tel:+33-186-26-78-00

https://sites.varonis.com/fr/entreprise/contact/

NASA ING Nasdaq CHAMPAGNE BOLLINGER MAISON FONDÉE EN 1829 DELL EMC

TOYOTA LUXEMBOURG INSTITUTE OF HEALTH RESEARCH DEDICATED TO LIFE L'ORÉAL

VARONIS