# Contexte

Si le filtrage des identificateurs de sécurité (SID Filtering) est inactif sur une relation d’approbation externe ou sur une relation d’approbation entre deux forêts, alors qu’aucune migration n’est en cours entre deux domaines de part et d’autre de la relation, alors celui-ci doit être activé. Si une migration est en cours, alors celui-ci doit être activé au plus vite après la fin de la migration, puis les historiques d’identificateurs de sécurité doivent être supprimés.

# Conséquences

Activer le filtrage des identificateurs de sécurité permet d’éviter les scénarios suivants :

* **Déplacement latéral** : Si un attaquant obtient l'accès à un compte utilisateur avec l'historique d’identificateurs de sécurité activé, il pourrait exploiter cette fonctionnalité pour se déplacer latéralement dans le réseau. En se faisant passer pour un utilisateur d'un autre domaine ou d'une autre forêt avec des privilèges élevés, l'attaquant pourrait accéder à des ressources dans d'autres domaines ou forêts où l'utilisateur compromis a des autorisations.
* **Élévation de privilèges** : Si un attaquant compromet un compte utilisateur avec l'historique d’identificateurs de sécurité activé et parvient à élever ses privilèges dans son propre domaine, il pourrait exploiter l'historique d’identificateurs de sécurité pour escalader davantage les privilèges dans d'autres domaines ou forêts où l'utilisateur compromis a des autorisations historiques. Cela pourrait conduire à l'obtention d'un accès administratif à des systèmes critiques ou à des données sensibles.
* **Persistance** : Un attaquant qui obtient l'accès à un environnement peut tenter d'établir une présence persistante en modifiant l'historique d’identificateurs de sécurité des comptes utilisateur compromis. En ajoutant leur propre identificateur de sécurité à l'historique d'un compte à privilèges élevés, l'attaquant pourrait maintenir l'accès aux ressources même si leur accès initial est détecté et corrigé.

## Chaine de cyberattaques

Activer le filtrage des identificateurs de sécurité permet d’éviter l’accomplissement des étapes suivantes d’une chaine de cyberattaques :

* **Reconnaissance** : L’activation du filtrage des identificateurs de sécurité rend plus difficile pour les attaquants de tirer parti des autorisations historiques lors des activités de reconnaissance.
* **Exploitation** : L’activation du filtrage des identificateurs de sécurité peut rendre plus difficile pour les attaquants d'exploiter les relations de confiance entre les domaines ou les forêts, limitant leur capacité à escalader les privilèges et à se déplacer latéralement dans le réseau.
* **Installation** : L’activation du filtrage des identificateurs de sécurité peut aider à empêcher les attaquants d'utiliser des identifiants compromis avec des autorisations historiques pour maintenir la persistance dans l'environnement.
* **Commande et contrôle** : L’activation du filtrage des identificateurs de sécurité peut perturber la capacité des attaquants à se faire passer pour des utilisateurs avec des autorisations historiques, rendant plus difficile pour eux d'éviter la détection et de contrôler les systèmes compromis.

# Détection

Les commandes PowerShell suivantes permettent de lister les relations d’approbation externes ou entre deux forêts qui n’ont pas de filtrage des identificateurs de sécurité :

#

# Installer le module PowerShell Active Directory

#

#Install-Module ActiveDirectory

#

# Importer le module PowerShell Active Directory

#

Import-Module ActiveDirectory

#

# Vérifier l'état du filtrage des identificateurs de sécurité dans les relations de confiance entre deux domaines

#

# Documentation : https://learn.microsoft.com/en-us/powershell/module/activedirectory/get-adtrust?view=windowsserver2022-ps

# -filter :

# - IntraForest -eq "False" : Sélectionner les relations d’approbation externes ou entre deux forêts  
# - Direction -eq "Bidirectional" : Sélectionner les relations d’approbation bidirectionnelles  
# - Direction -eq "Outbound" : Sélectionner les relations d’approbation sortantes (requêtes entrantes)  
# - SIDFilteringEnabled -eq "False" : Sélectionner les relations d’approbation sans filtrage des indicateurs de sécurité

#

Get-ADTrust -Filter {(IntraForest -eq "False") -and ((Direction -eq "Bidirectional") -or (Direction -eq "Outbound")) -and (SIDFilteringEnabled -eq "False")}

Le filtrage des identificateurs de sécurité doit être activé pour chaque relation d’approbation listée.

Documentation :

* <https://learn.microsoft.com/en-us/powershell/module/activedirectory/get-adtrust?view=windowsserver2022-ps>

# Correction

## Prérequis

Afin de corriger l’anomalie, il faut d’abord s’assurer que les relations de confiance ne sont pas entre domaines d’une même forêt. Car le filtrage des identificateurs de sécurité dans une relation d’approbation entre domaines d’une même forêt n’est pas une configuration supportée et peut provoquer des erreurs. Si un domaine au sein d’une forêt n’est pas digne de confiance, alors il faut d’abord séparer les domaines de confiance et les autres domaines dans des forêts différentes. Ainsi, le filtrage des identificateurs de sécurité pourra être appliqué entre les forêts.

Ensuite, il faut s’assurer qu’aucune migration de domaine légitime ne soit en cours, car l’activation du filtrage des identificateurs de sécurité sur un domaine qui est en cours de migration pourrait compromettre le bon fonctionnement des comptes dont l’ancien identificateur de sécurité est encore utilisé dans des listes de contrôle d’accès (ACL) sur le nouveau domaine. Si une migration est en cours, celle-ci doit être terminée au plus vite et les anciens identificateurs de sécurité ne doivent plus être utilisés.

Pour pouvoir exécuter les commandes suivantes, l’utilisateur doit faire partie du groupe d’administrateurs du domaine, *domain administrators* en anglais, ou d’administrateurs de l’entreprise, *enterprise administrators* en anglais, et le système d’exploitation doit faire partie de la liste suivante :

* Windows 8
* Windows Server 2008
* Windows Server 2008 R2
* Windows Server 2012

Documentation :

* <https://attack.mitre.org/techniques/T1134/005/>
* <https://learn.microsoft.com/fr-fr/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc835085(v=ws.11)>

## Procédure

Pour commencer, il est recommandé de désactiver l’utilisation de l’historique d’identificateurs de sécurité (SID History) pour les relations d’approbation (Trust) entre forêts.

La commande Netdom suivante permet de désactiver l’historique d’identificateurs de sécurité au niveau de la relation d’approbation entre deux forêts. L’historique d’identificateurs de sécurité ne peut être désactivé que depuis le domaine confiant :

#

# Désactiver l’historique d’identificateurs de sécurité sur une relation d’approbation entre forêts :

# Forêt confiante : La forêt ne transmettra plus l’historique d’identificateurs de sécurité lors de l’envoi de requêtes vers une autre forêt.  
# Forêt de confiance : La forêt ne s’attendra plus à recevoir d’historique d’identificateurs de sécurité lors de la réception de requêtes depuis une autre forêt.

#

netdom trust <forêt confiante> /domain:<forêt de confiance> /EnableSIDHistory:no

Ensuite, il est recommandé d’activer le filtrage des identificateurs de sécurité pour les relations d’approbation entre domaines.

La commande Netdom suivante permet d’activer le filtrage des identificateurs de sécurité au niveau de la relation d’approbation entre deux domaines. Il ne faut pas utiliser cette commande pour des relations d’approbation entre forêts, car la transitivité de la relation serait brisée. Le filtrage des identificateurs de sécurité ne peut être activé que depuis le domaine confiant :

#

# Activer la fonctionnalité de filtrage des identificateurs de sécurité (SID Filtering) :

#

netdom trust <domaine confiant> /domain:<domaine de confiance> /quarantine:yes

Documentation :

* <https://learn.microsoft.com/fr-fr/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc835085(v=ws.11)>
* <https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html>
* <https://cyber.gouv.fr/sites/default/files/IMG/pdf/NP_ActiveDirectory_NoteTech.pdf#paragraph.3.3.1.6>
* <https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html>

# Vérification

Pour vérifier la bonne correction de l’anomalie, il est possible de d’exécuter à nouveau la partie "Détection" et de constater qu’aucune relation de confiance sans filtrage des identificateurs de sécurité n’est listée.