



L'objet AdminSDHolder

Risques et contre-mesures

(environnement Active Directory)

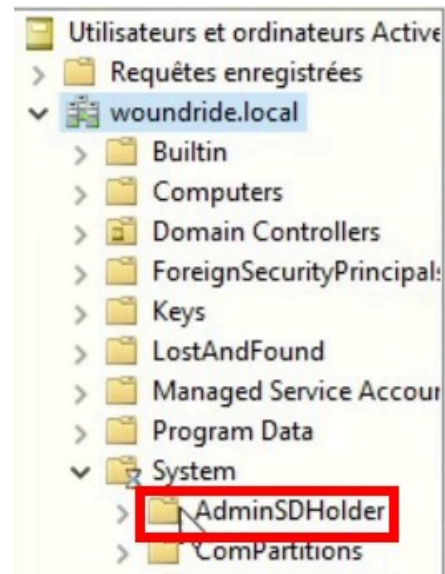




L'objet AdminSDHolder

Késako ?

- Un objet de type « conteneur » localisé dans le conteneur « System »
- Présent par défaut dans tout Active Directory depuis Windows Server 2003



Chemin : CN= AdminSDHolder, CN=System,<Domain DN>





L'objet AdminSDHolder

Objectif :

- Fournir un modèle d'autorisations aux groupes et comptes protégés du domaine
- Groupes et comptes protégés dans l'AD par système d'exploitation

| Windows Server 2003 R2 RTM | Windows Server 2003 SP1 | Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 | Windows Server 2016 |
|---------------------------------|---------------------------------|--|---|
| Opérateurs de compte | Opérateurs de compte | Opérateurs de compte | Opérateurs de compte |
| Administrateur | Administrateur | Administrateur | Administrateur |
| Administrateurs | Administrateurs | Administrateurs | Administrateurs |
| Opérateurs de sauvegarde | Opérateurs de sauvegarde | Opérateurs de sauvegarde | Opérateurs de sauvegarde |
| Éditeurs de certificats | | | |
| Administrateurs du domaine | Administrateurs du domaine | Administrateurs du domaine | Administrateurs du domaine |
| Contrôleurs de domaine | Contrôleurs de domaine | Contrôleurs de domaine | Contrôleurs de domaine |
| Administrateurs de l'entreprise | Administrateurs de l'entreprise | Administrateurs de l'entreprise | Administrateurs de l'entreprise |
| Krbtgt | Krbtgt | Krbtgt | Krbtgt |
| Opérateurs d'impression | Opérateurs d'impression | Opérateurs d'impression | Opérateurs d'impression |
| | | Contrôleurs de domaine en lecture seule | Contrôleurs de domaine en lecture seule |
| Duplicateur | Duplicateur | Duplicateur | Duplicateur |
| Administrateurs du schéma | Administrateurs du schéma | Administrateurs du schéma | Administrateurs du schéma |
| Opérateurs de serveur | Opérateurs de serveur | Opérateurs de serveur | Opérateurs de serveur |

Source : Microsoft





Le processus SDProp

Fonctionnement :

- Processus qui s'exécute toutes les 60 minutes par défaut
 - Délai modifiable : entre 60 secondes et 120 minutes
 - Diminuer le délai par défaut risque d'entraîner une surcharge de traitement du processus d'authentification LSASS
- Il s'exécute sur le contrôleur de domaine principal (portant le rôle de PDCE)
- Il compare les autorisations des comptes et groupes protégés avec celles présentes sur l'objet AdminSDHolder. En cas de différence(s), il écrase les autorisations pour appliquer celles de l'objet AdminSDHolder
- Il désactive l'héritage des autorisations
- Il « marque » chaque objet en définissant la valeur de l'attribut adminCount à 1



Que se passe-t-il lorsqu'un compte est ajouté dans un groupe protégé ?

Après exécution du processus SDProp :

- Application des autorisations de l'objet AdminSDHolder
- Désactivation de l'héritage
- Définition de l'attribut adminCount à 1

Propriétés de : Charles BLANC-ROLIN

| Environnement | | Sessions | | Contrôle à distance | | |
|---------------------------------------|---------|-----------------------------|--------|---------------------|--------------|---------------------|
| Général | Adresse | Compte | Profil | Téléphones | Organisation | Certificats publiés |
| Membre de | | Réplication de mot de passe | | Appel entrant | Objet | Sécurité |
| Profil des services Bureau à distance | | COM+ | | Éditeur d'attributs | | |

Attributs :

| Attribut | Valeur |
|--------------------|--------------|
| accountExpires | (jamais) |
| accountNameHistory | <non défini> |
| aCSPolicyName | <non défini> |
| adminCount | 1 |
| adminDescription | <non défini> |

Propriétés de : Charles BLANC-ROLIN

| Environnement | | Sessions | | Contrôle à distance | | |
|---------------------------------------|---------|-----------------------------|--------|---------------------|--------------|---------------------|
| Général | Adresse | Compte | Profil | Téléphones | Organisation | Certificats publiés |
| Membre de | | Réplication de mot de passe | | Appel entrant | Objet | Sécurité |
| Profil des services Bureau à distance | | COM+ | | Éditeur d'attributs | | |

Membre de :

| Nom | Dossier Services de domaine Active Directory |
|-----------------------|--|
| Admins du domaine | woundrde.local/Utilisateurs/Administrateurs/Admin de domaine |
| Utilisateurs du do... | woundrde.local/Users |

Paramètres de sécurité avancés pour Charles BLANC-ROLIN

Propriétaire : Admins du domaine (WOUNDRIDE\Admins du domaine) [Modifier](#)

Autorisations **Audit** Accès effectif

Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'autorisation. Pour modifier une entrée d'autorisation, sélectionnez l'entrée et cliquez sur Modifier (si disponible).

Entrées d'autorisations :

| Type | Principal | Accès | Hérité de | S'applique à |
|---------|-----------------------------------|-----------------------------|-----------|----------------------------------|
| Auto... | Éditeurs de certificats (WOU... | | Aucun | Cet objet uniquement |
| Auto... | Groupe d'accès d'autorisatio... | | Aucun | Cet objet uniquement |
| Auto... | Serveurs de licences des servi... | | Aucun | Cet objet uniquement |
| Auto... | Serveurs de licences des servi... | Lire/écrire Serveur de l... | Aucun | Cet objet uniquement |
| Auto... | Tout le monde | Modifier le mot de pas... | Aucun | Cet objet uniquement |
| Auto... | SELF | Modifier le mot de pas... | Aucun | Cet objet uniquement |
| Auto... | SELF | Spéciale | Aucun | cet objet et tous ceux descen... |
| Auto... | Admins du domaine (WOUN... | Spéciale | Aucun | Cet objet uniquement |
| Auto... | Administrateurs de l'entrepri... | Spéciale | Aucun | Cet objet uniquement |

[Ajouter](#) [Supprimer](#) [Afficher](#) [Paramètres par défaut](#)

Activer l'héritage

Que se passe-t-il lorsqu'un compte est retiré d'un groupe protégé ?

Après exécution du processus SDProp :

- Rien !!!
- L'attribut `adminCount` reste à 1
- L'héritage reste désactivé > risques : conserver des droits trop permissifs, ne pas obtenir de nouveaux droits ou restrictions des objets parents

Propriétés de : Charles BLANC-ROLIN

| Attribut | Valeur |
|--------------------|--------------|
| accountExpires | (jamais) |
| accountNameHistory | <non défini> |
| aCSPolicyName | <non défini> |
| adminCount | 1 |
| adminDescription | <non défini> |

Paramètres de sécurité avancés pour Charles BLANC-ROLIN

Propriétaire : Admins du domaine (WOUNDRIDE\Admins du domaine) [Modifier](#)

Autorisations **Audit** Accès effectif

Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'autorisation. Pour modifier une entrée d'autorisation, sélectionnez l'entrée et cliquez sur Modifier (si disponible).

Entrées d'autorisations :

| Type | Principal | Accès | Hérité de | S'applique à |
|---------|-----------------------------------|-----------------------------|-----------|----------------------------------|
| Auto... | Éditeurs de certificats (WOU... | | Aucun | Cet objet uniquement |
| Auto... | Groupe d'accès d'autorisatio... | | Aucun | Cet objet uniquement |
| Auto... | Serveurs de licences des servi... | | Aucun | Cet objet uniquement |
| Auto... | Serveurs de licences des servi... | Lire/écrire Serveur de l... | Aucun | Cet objet uniquement |
| Auto... | Tout le monde | Modifier le mot de pas... | Aucun | Cet objet uniquement |
| Auto... | SELF | Modifier le mot de pas... | Aucun | Cet objet uniquement |
| Auto... | SELF | Spéciale | Aucun | cet objet et tous ceux descen... |
| Auto... | Admins du domaine (WOUN... | Spéciale | Aucun | Cet objet uniquement |
| Auto... | Administrateurs de l'entrepri... | Spéciale | Aucun | Cet objet uniquement |

Ajouter Supprimer Afficher Paramètres par défaut

Activer l'héritage

Que faire pour se protéger dans ce cas ?

Identifier les comptes concernés :

- Identifier les comptes concernés (tous les comptes ayant la valeur 1 pour l'attribut adminCount et qui ne sont pas présents dans un groupe d'administration protégé)

Les outils pour vous aider : PingCastle, Purple Knight, PKE Meter

The screenshot displays a security tool interface with a terminal window on the left and a main dashboard on the right. The terminal window shows a list of user accounts extracted from a system, with a red arrow pointing to the 'AdminSDHolder' account. The main dashboard shows a 'SECURITY INDICATOR' for 'Unprivileged accounts with adminCount=1'. It includes a severity level of 'Informational', a weight of 3, and a description of the indicator. A table lists the detected accounts, with one account highlighted in red. Below the table, a 'Result' section shows the details of the selected account.

AdminSDHolder (detect temporary elevated accounts)

This control detects accounts which are former 'unofficial' admins. Indeed when an account belongs to a privileged group, the attribute admincount is set. If the attribute is set without being an official member, this is suspicious. To suppress this warning, the attribute admincount of these accounts should be removed after review.

Number of accounts to review: 1

[AdminSDHolder User List](#)

| Name | Creation | Last logon | Pwd Last Set | Event date | Distinguished name |
|---------------|----------------------|----------------------|--------------|----------------------|---|
| c.blanc-rolin | 2022-06-03 09:22:12Z | 2025-01-20 21:41:31Z | Never | 2025-01-23 22:12:29Z | CN=Charles BLANC-ROLIN,OU=Service 1,OU=T2_Utilisateurs,OU=T2,OU=_Utilisateurs,DC=woundride,DC=local |

Showing 1 to 1 of 1 rows

| DistinguishedName | Type | SamAccountName | EventTimestamp | Ignored |
|---|------|----------------|---------------------|---------|
| CN=Charles BLANC-ROLIN,OU=Service 1,OU=T2_Utilisateurs,OU=T2,OU=_Utilisateurs,DC=woundride,DC=local | user | cblanc-rolin | 23/01/2025 21:12:29 | False |

Found 1 AdminSDHolder account(s)

Exported file : C:\Users\admin_t0_cbr\Desktop\adminsdholder.txt

Que faire pour se protéger dans ce cas ?

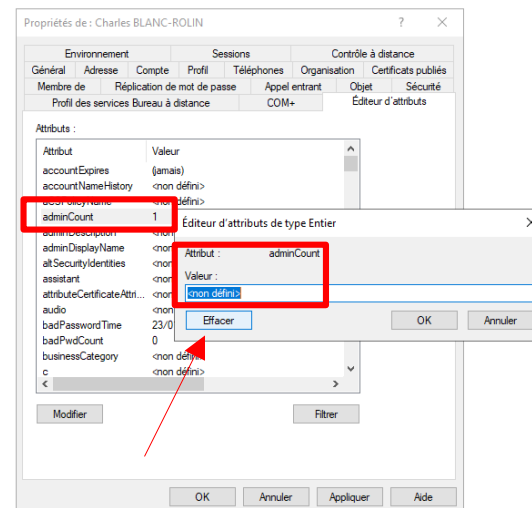
Agir sur les comptes concernés :

- L'ANSSI recommande la désactivation des comptes concernés

R40 - Priorité 1

L'attribut `adminCount` doit être positionné à `1` uniquement sur les comptes membres d'un groupe d'administration protégé. Il est impératif de désactiver un compte lorsqu'il est retiré de la liste des membres d'un groupe d'administration protégé.

- Solution de contournement :
 - Effacer la valeur à 1 pour l'attribut `adminCount`
 - Réactiver l'héritage
 - Réappliquer les droits par défaut sur l'objet



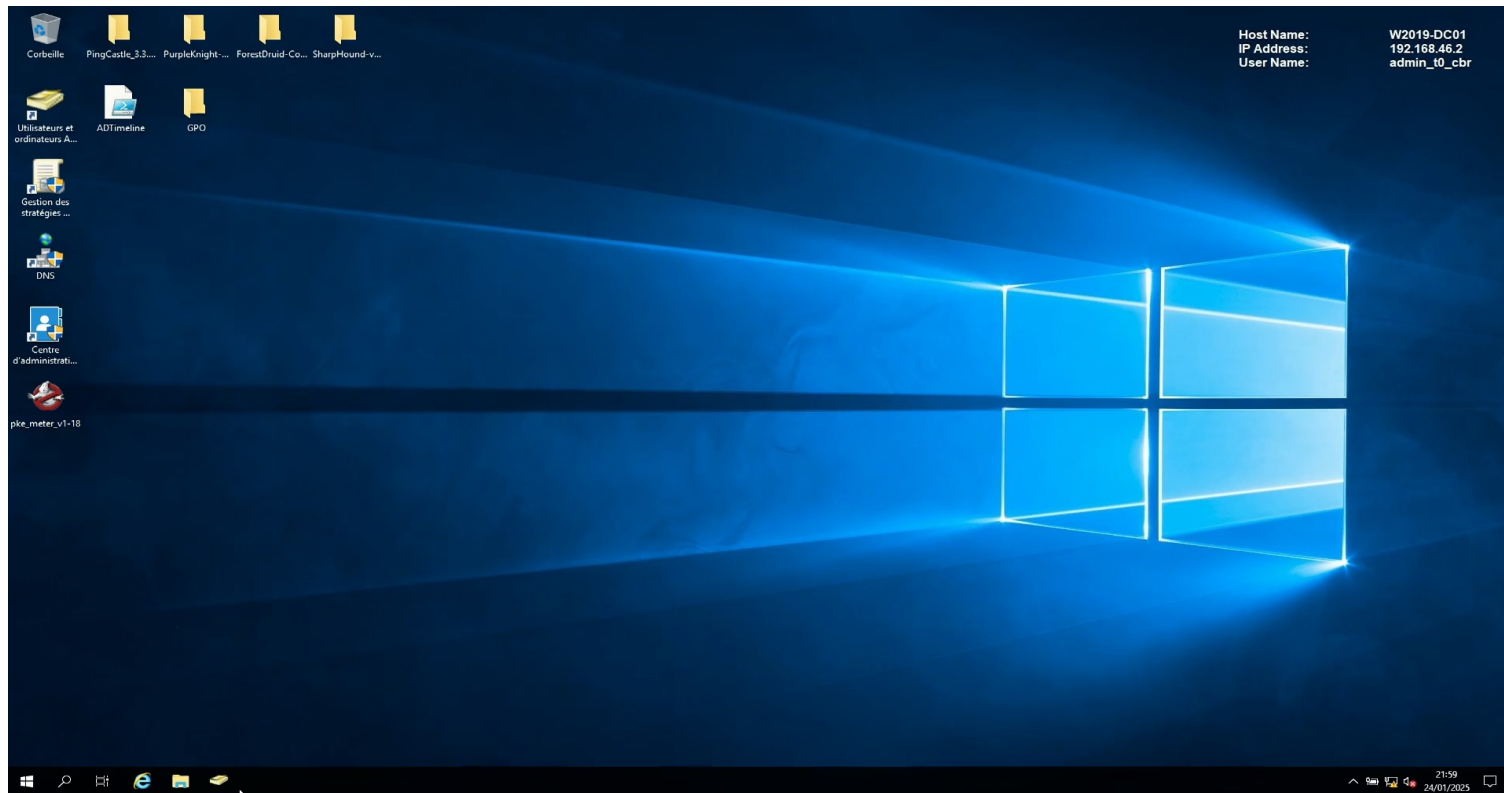
```
Administrateur: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

PS C:\Windows\system32> dsacl.exe "CN=Charles BLANC-ROLIN,OU=Service 1,OU=T2_Utilisateurs,OU=T2,OU=_Utilisateurs,DC=woundride,DC=local" /S /T
Entrée traitée CN=Charles BLANC-ROLIN,OU=Service 1,OU=T2_Utilisateurs,OU=T2,OU=_Utilisateurs,DC=woundride,DC=local
Paramètre incorrect.

La commande n'a pas pu terminer correctement.
PS C:\Windows\system32>
```



Démonstration

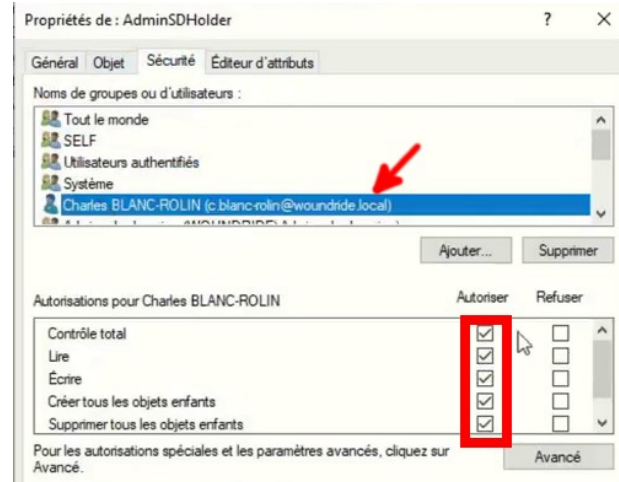




« AdminSDHolder Backdooring »

Comment un attaquant peut tirer parti de l'objet AdminSDHolder ?

- S'il dispose temporairement de privilèges Administrateur sur le domaine (compromission, collaborateur malveillant)
- Il lui suffit de donner le contrôle total à un « simple » compte utilisateur pour en faire un compte « administrateur » dormant et très difficile à détecter (permet d'avoir une persistance sur le SI)
- Ce « simple » compte utilisateurs peut à tout moment :
 - S'octroyer les droits d'administration du domaine
 - Et se les retirer pour redevenir « invisible »





« AdminSDHolder Backdooring » : Démonstration



Quelques pistes pour repérer cette persistance

Check last modification date of AdminSDHolder object

Creation date : @{WhenCreated=03/06/2022 10:57:59}

Last modification : @{Modified=22/11/2023 16:34:05}



```
AObjects_woundride.local.xml X
home > charles > Téléchargements > AObjects_woundride.local.xml
2502      </Obj>
2503      <I32 N="instanceType">4</I32>
2504      <B N="isCriticalSystemObject">>true</B>
2505      <Nil N="isDeleted" />
2506      <Nil N="LastKnownParent" />
2507      <DT N="Modified">2023-11-27T15:50:40+01:00</DT>
2508      <DT N="modifyTimeStamp">2023-11-27T15:50:40+01:00</DT>
2509      <S N="Name">AdminSDHolder</S>
2510      <Obj N="nTSecurityDescriptor" RefId="144">
2511      <TNRef RefId="2" />
```

timeline_woundride.local.csv - LibreOffice Calc

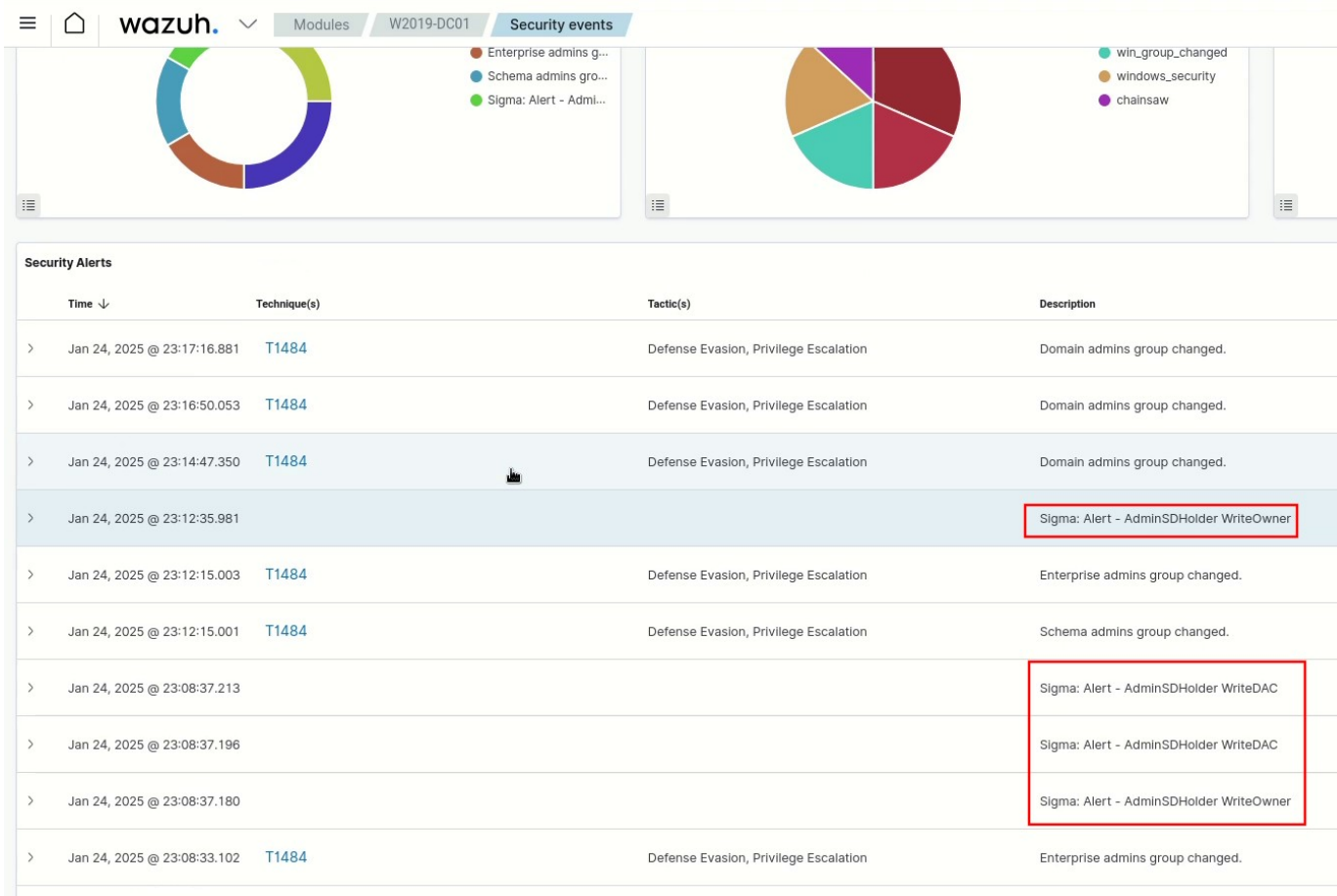
Eichier Édition Affichage Insertion Format Styles Feuille Données Outils Fenêtre Aide

Liberation Sans 10 pt

C8793 f_x Σ = "nTSecurityDescriptor"

| | A | B | C | D | |
|------|------------------------|--|------------------------|-------------|------------------|
| 8789 | "2023-11-05T17:29:26Z" | "Charles BLANC-ROLIN" | "nTSecurityDescriptor" | "user" | "CN=Charles BLA |
| 8790 | "2023-11-22T14:10:27Z" | "W2019-DC01" | "lastLogonTimestamp" | "computer" | "CN=W2019-DC0 |
| 8791 | "2023-11-22T14:17:30Z" | "[Admin de domaine] Charles BLANC-ROLIN" | "lastLogonTimestamp" | "user" | "CN=[Admin de di |
| 8792 | "2023-11-22T14:18:43Z" | "Charles BLANC-ROLIN" | "lastLogonTimestamp" | "user" | "CN=Charles BLA |
| 8793 | "2023-11-27T14:50:40Z" | "AdminSDHolder" | "nTSecurityDescriptor" | "container" | "CN=AdminSDHo |
| 8794 | "9999-12-29T23:59:59Z" | "Deleted Objects" | "Deleted Objects" | "container" | "CN=Deleted Obj |

Détection via les journaux de sécurité



Détection via les chemins de contrôle (Forest Druid)

Export Forest Druid

forest druid powered by **semperis** DEFENSE PERIMETER ATTACK PATHS

Unclassified privilege escalation relationships: 34

↑ Source Name ▾ No filters CLASSIFY MULTIPLE

| Source | Relationship | Target |
|---|--|--|
| Charles BLANC-ROLIN [AD] User woundride.local | Unclassified Generic All Cost: 2 | Opérateurs de compte [AD] Group woundride.local |
| Charles BLANC-ROLIN [AD] User woundride.local | Unclassified Generic All Cost: 2 | AdminSDHolder [AD] Container woundride.local |
| Charles BLANC-ROLIN [AD] User woundride.local | Unclassified Generic All Cost: 2 | Contrôleurs de domaine [AD] Group woundride.local |
| Charles BLANC-ROLIN [AD] User woundride.local | Unclassified Generic All Cost: 2 | Administrateurs clés [AD] Group woundride.local |
| Charles BLANC-ROLIN [AD] User woundride.local | Unclassified Generic All Cost: 2 | Opérateurs d'impression [AD] Group woundride.local |
| Charles BLANC-ROLIN [AD] User woundride.local | Unclassified Generic All Cost: 2 | krbtgt [AD] User woundride.local |
| Charles BLANC-ROLIN [AD] User woundride.local | Unclassified Generic All Cost: 2 | Opérateurs de serveur [AD] Group woundride.local |
| Charles BLANC-ROLIN [AD] User woundride.local | Unclassified Generic All Cost: 2 | Administrateur [AD] User woundride.local |
| Charles BLANC-ROLIN [AD] User woundride.local | Unclassified Generic All Cost: 2 | Administrateurs clés Enterprise [AD] Group woundride.local |
| Charles BLANC-ROLIN [AD] User woundride.local | Unclassified Generic All Cost: 2 | Opérateurs de sauvegarde [AD] Group woundride.local |
| Charles BLANC-ROLIN [AD] User woundride.local | Unclassified Generic All Cost: 2 | Contrôleurs de domaine en lectur... [AD] Group woundride.local |



Ressources et outils utilisés

- Comptes et groupes protégés (Microsoft) :
<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups>
<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-c-protected-accounts-and-groups-in-active-directory>
- Désactivation des comptes ayant été privilégiés (ANSSI) :
https://cyber.gouv.fr/sites/default/files/IMG/pdf/NP_ActiveDirectory_NoteTech.pdf#paragraph.3.6.3.1
- PingCastle (Vicent LE TOUX) :
<https://www.pingcastle.com/>
- Purple Knight (Semperis) :
<https://semperis.com/downloads/tools/pk/PurpleKnight-Community.zip>
- PowerSploit (PowerShellMafia) :
<https://github.com/PowerShellMafia/PowerSploit>
- BloodHound (Specterops) :
<https://specterops.io/bloodhound-community-edition/>
- Forest Druid (Semperis) :
<https://semperis.com/downloads/tools/fd/ForestDruid-Community.zip>
- PKE Meter (Charles BLANC-ROLIN):
https://github.com/woundride/PKE_Meter

