L'objet AdminSDHolder
Risques et contre-mesures

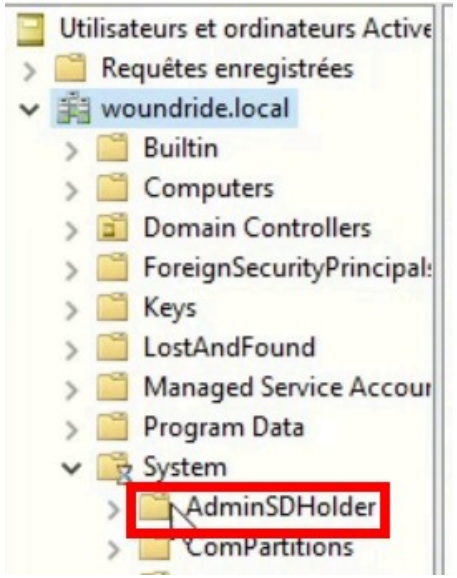
(environnement Active Directory)

Version 1.0 - 2025

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

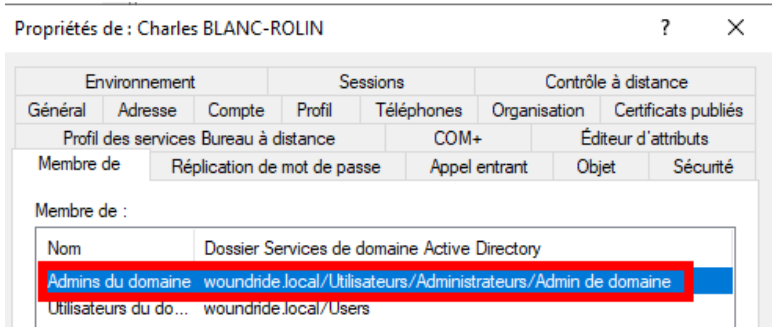
- Il désactive l'héritage des autorisations

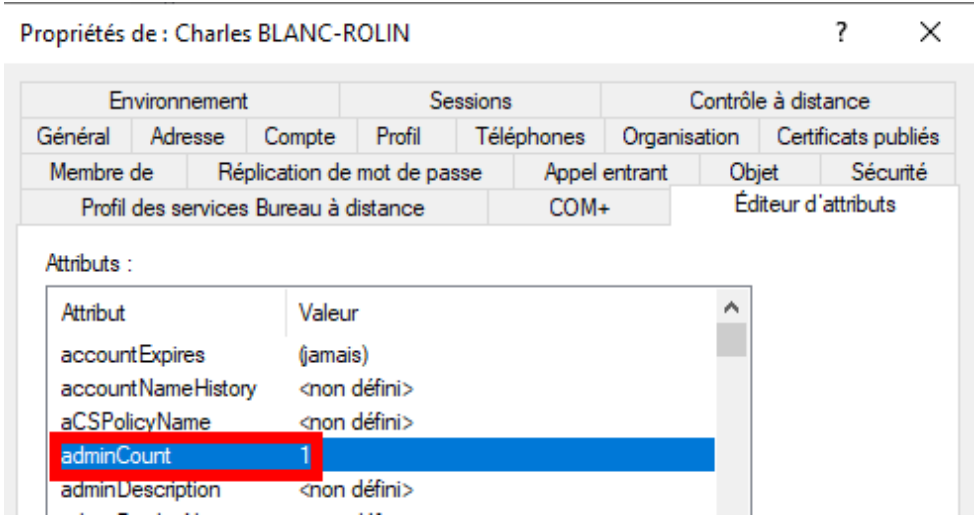
- Il « marque » chaque objet en définissant la valeur de l'attribut adminCount à 1

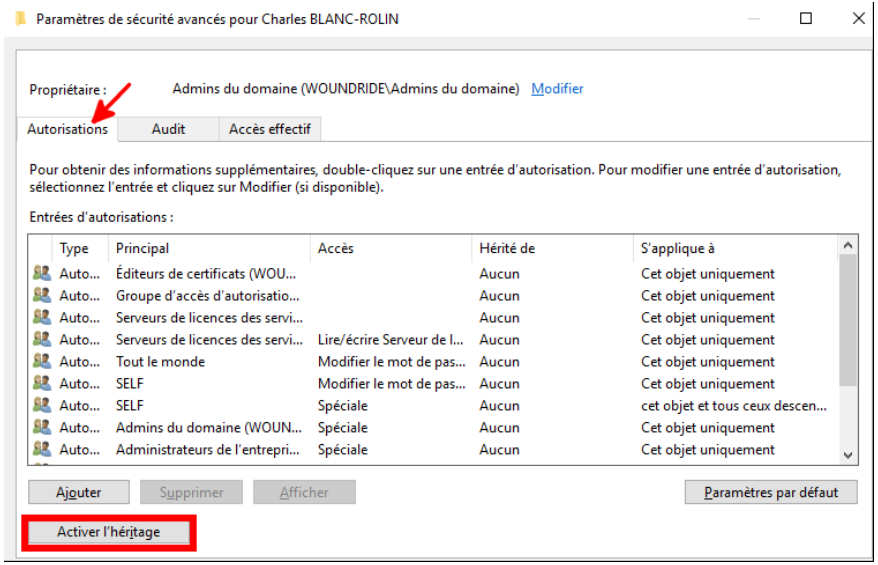
Que se passe-t-il lorsqu'un compte est ajouté dans un groupe protégé ?

Après exécution du processus SDProp :

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



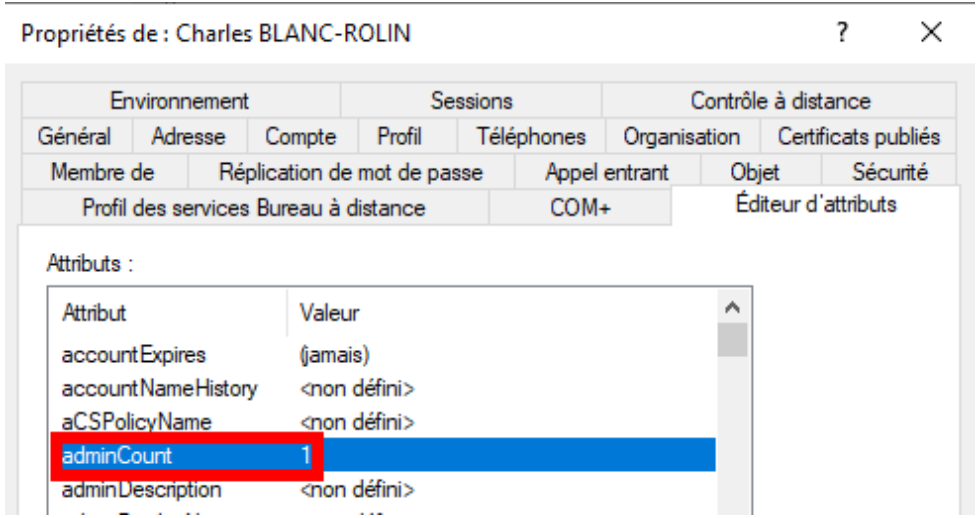


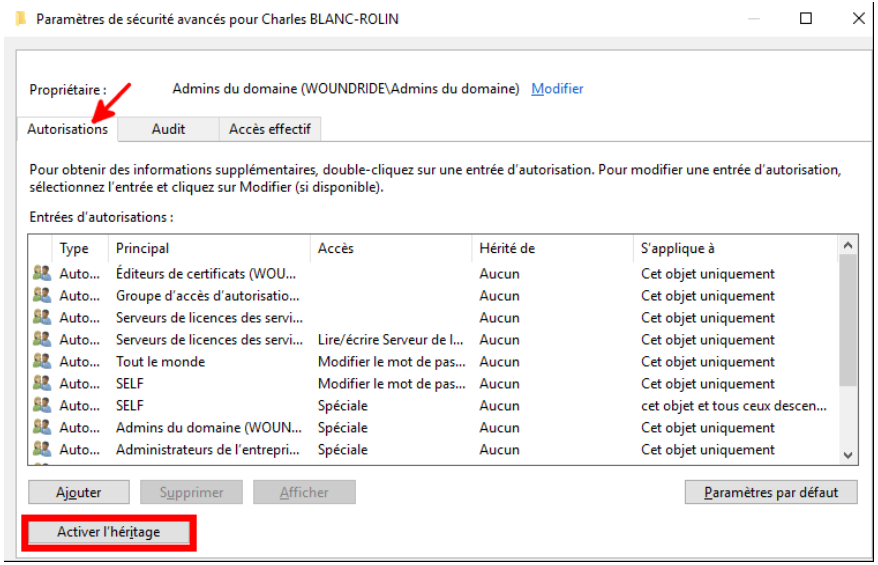


Que se passe-t-il lorsqu'un compte est retiré d'un groupe protégé ?

Après exécution du processus SDProp :

- Rien !!!
- L'attribut reste 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

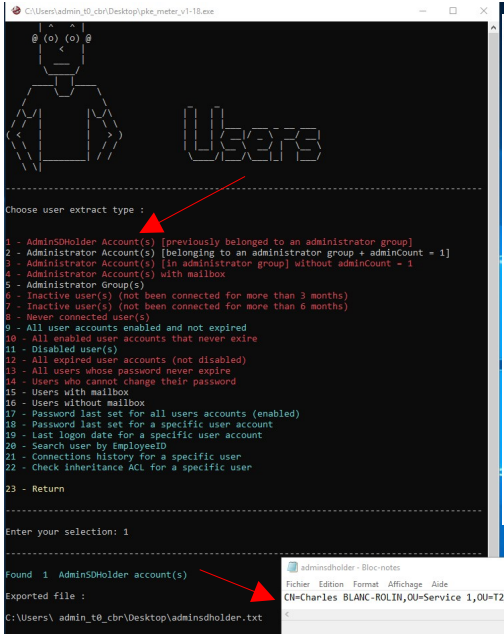


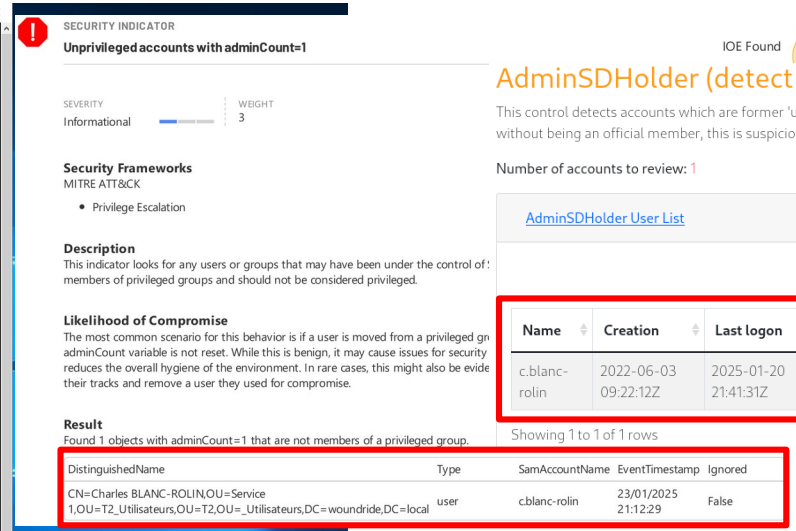


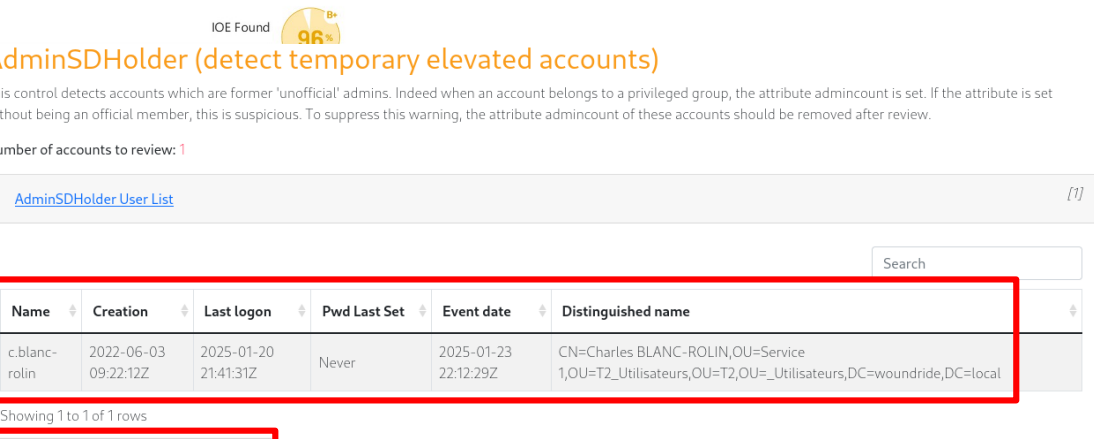
Que faire pour se protéger dans ce cas ?

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





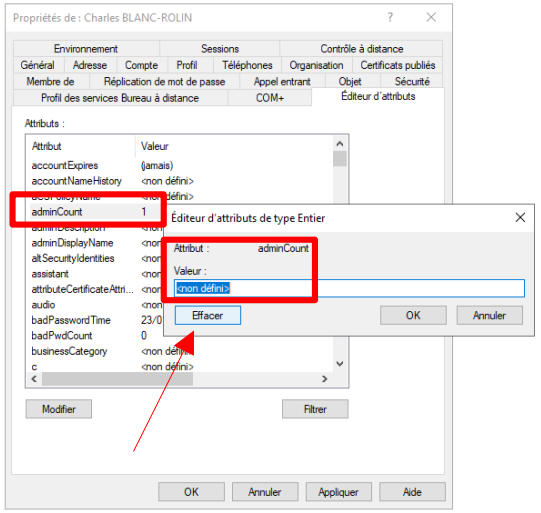


Que faire pour se protéger dans ce cas ?

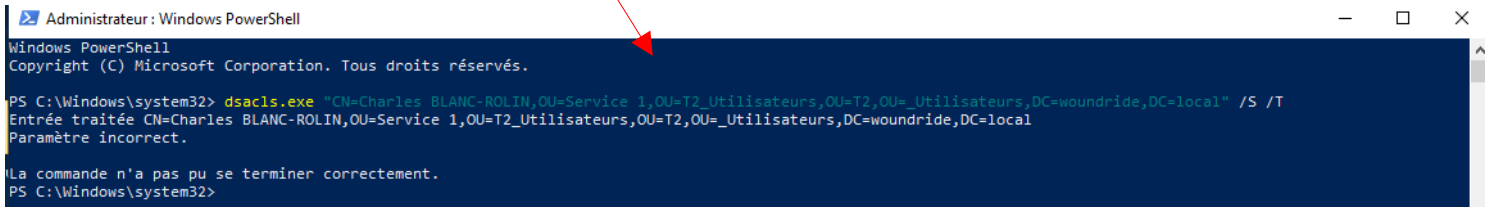
Agir sur les comptes concernés :

- *L'ANSSI recommande la désactivation des comptes concernés*

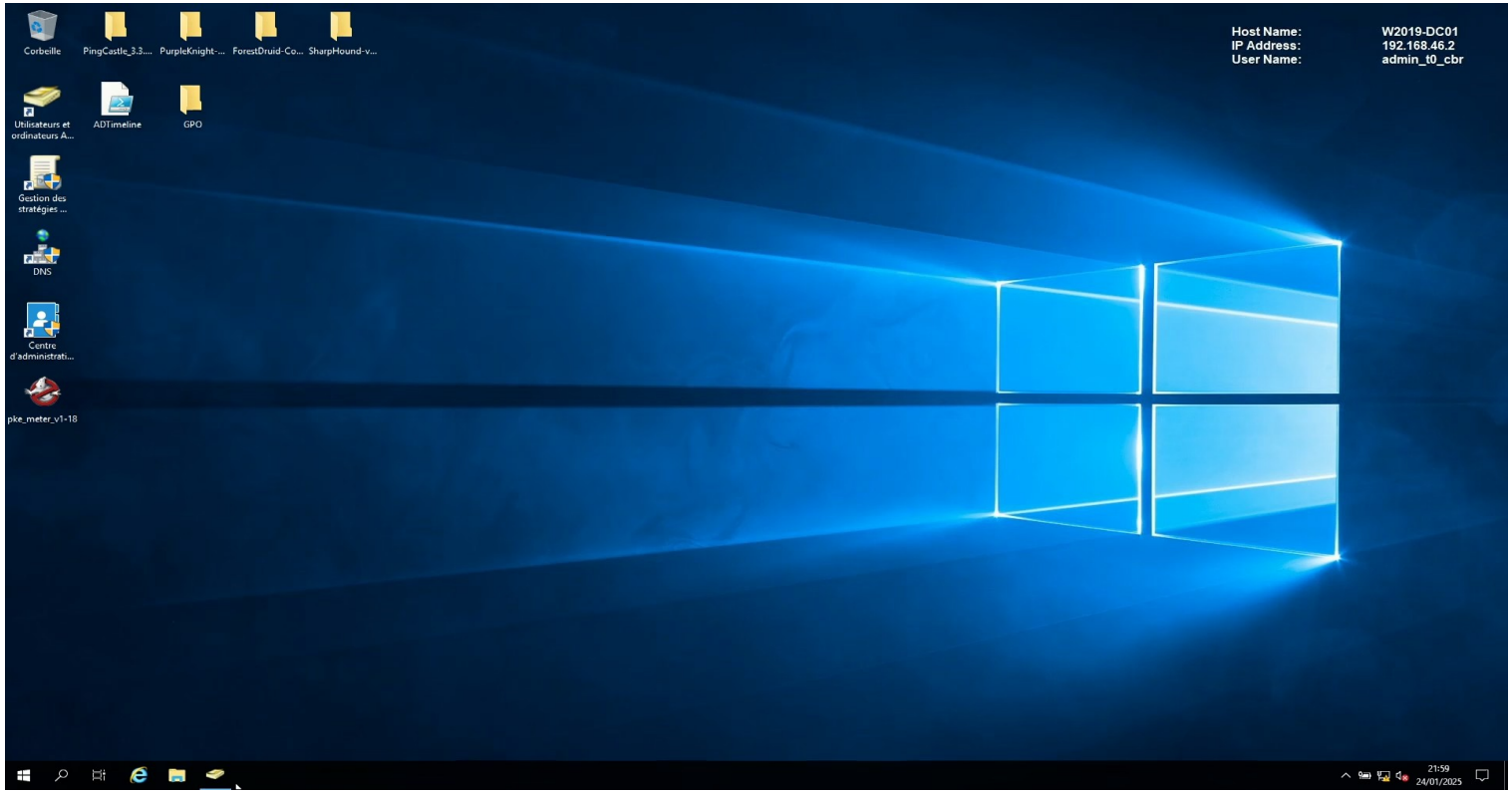
> **R40** - Priorité 1
>
> L'attribut *adminCount* doit être positionné à *1* uniquement sur les comptes membres d'un groupe d'administration protégé. Il est impératif de désactiver un compte lorsqu'il est retiré de la liste des membres d'un groupe d'administration protégé.



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



Démonstration



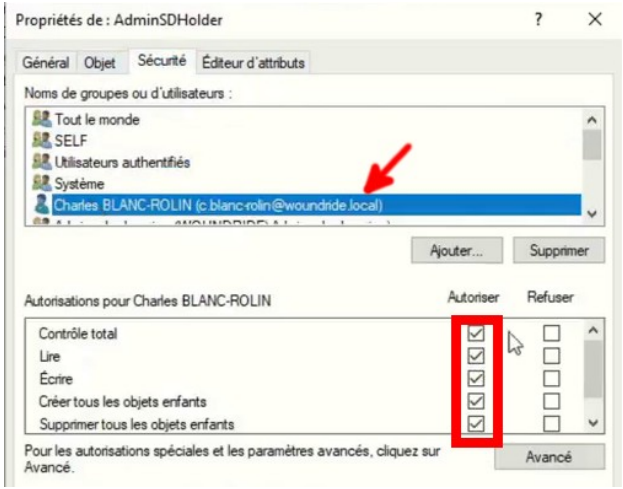
« AdminSDHolder Backdooring »

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

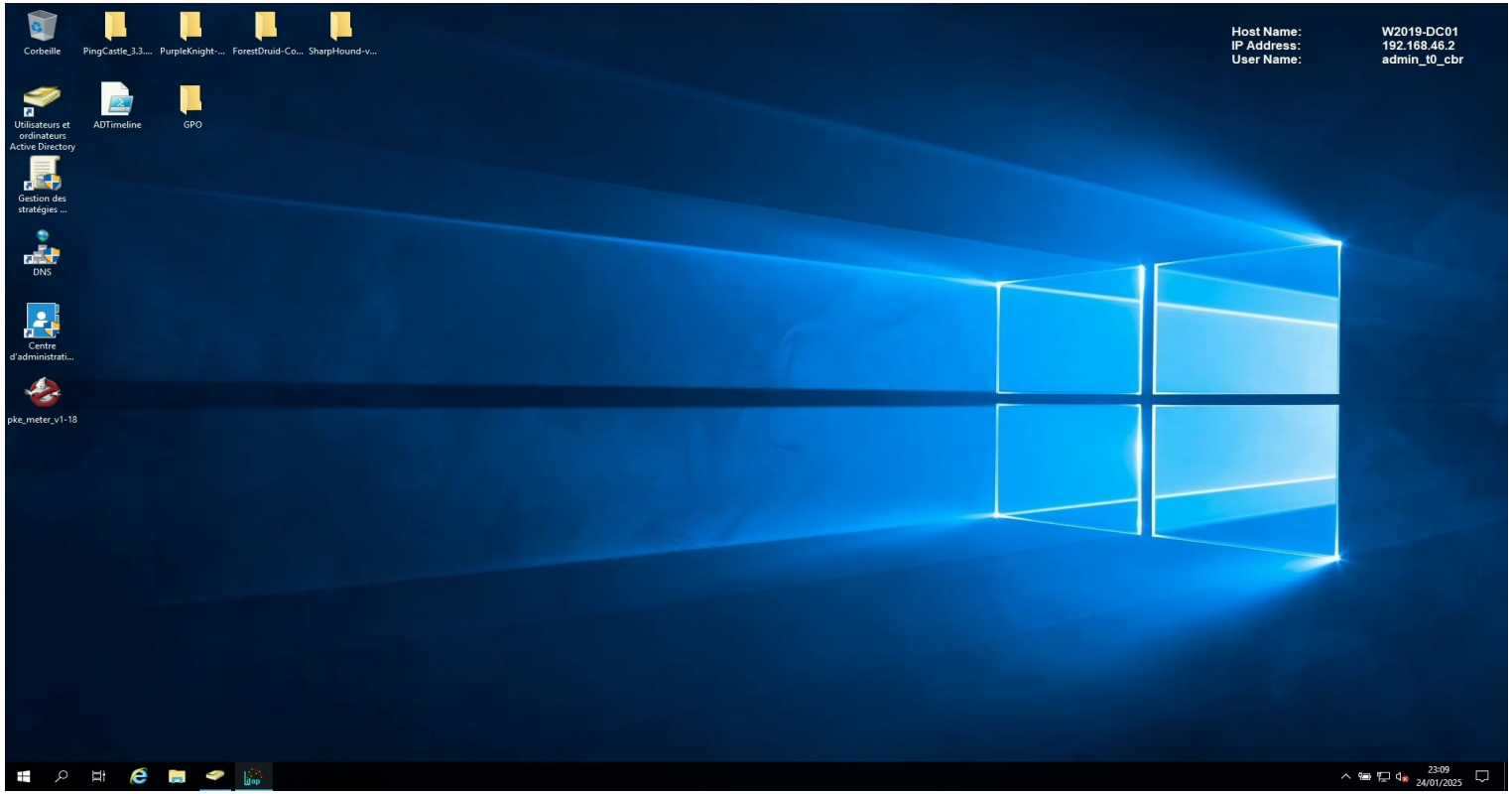
- S'il dispose temporairement de privilèges Administrateur sur le domaine (compromission, collaborateur malveillant)

- 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}
```

AD TIMELINE

ADobjects_woundride.local.xml

home > charles > Téléchargements > ADobjects_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

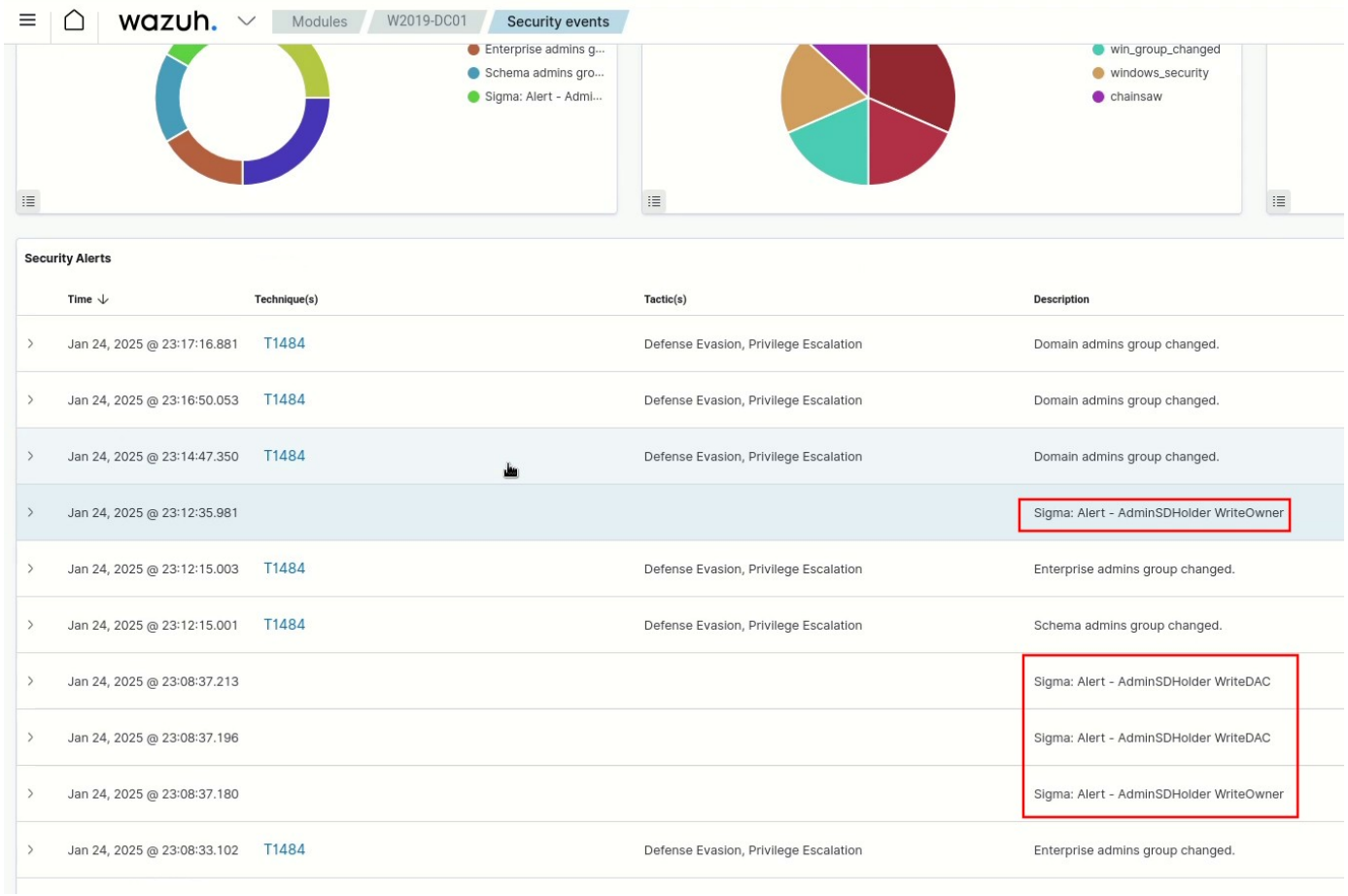
Fichier Édition Affichage Insertion Format Styles Feuille Données Outils Fenêtre Aide

Liberation Sans 10 pt

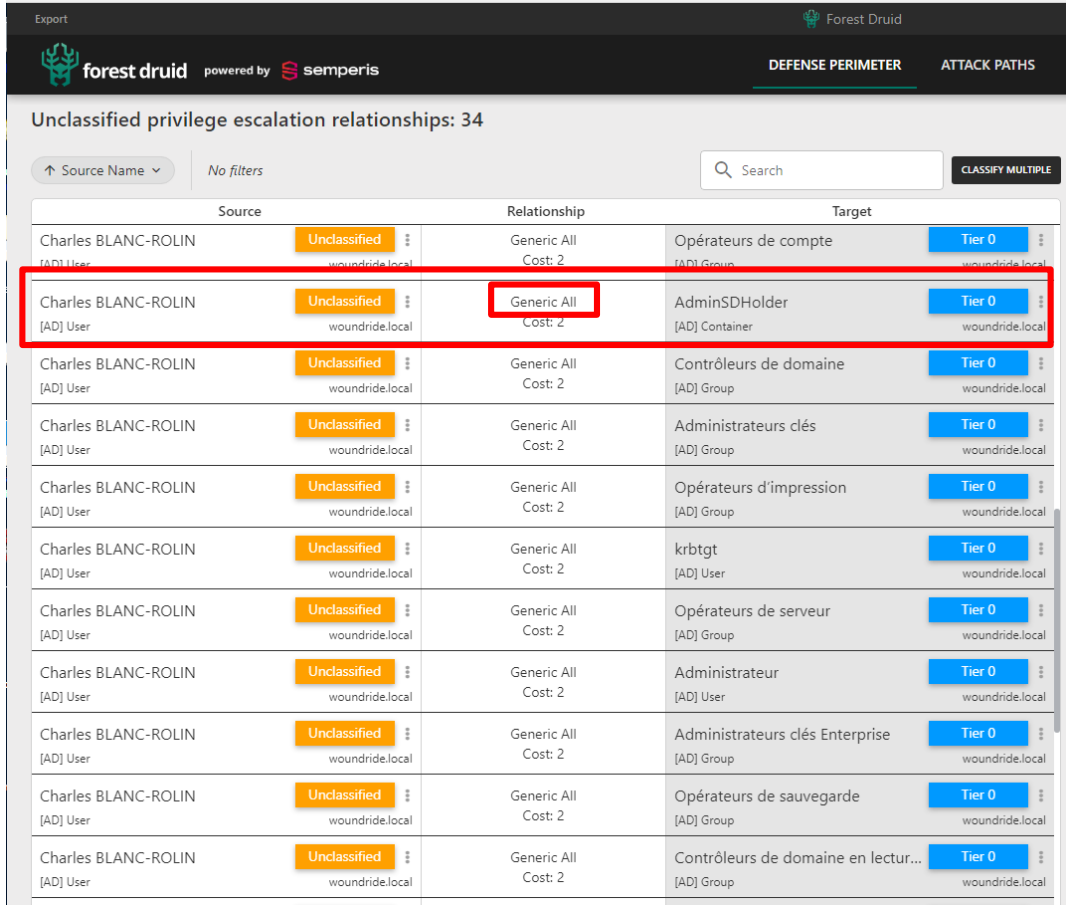
C8793 = "nTSecurityDescriptor"

	A	B	C	D	
8789	"2023-11-05T17:29:26Z"	"Charles BLANC-ROLIN"	"ntPwdHistory"	"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 d
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"	"isDeleted"	"container"	"CN=Deleted Obj

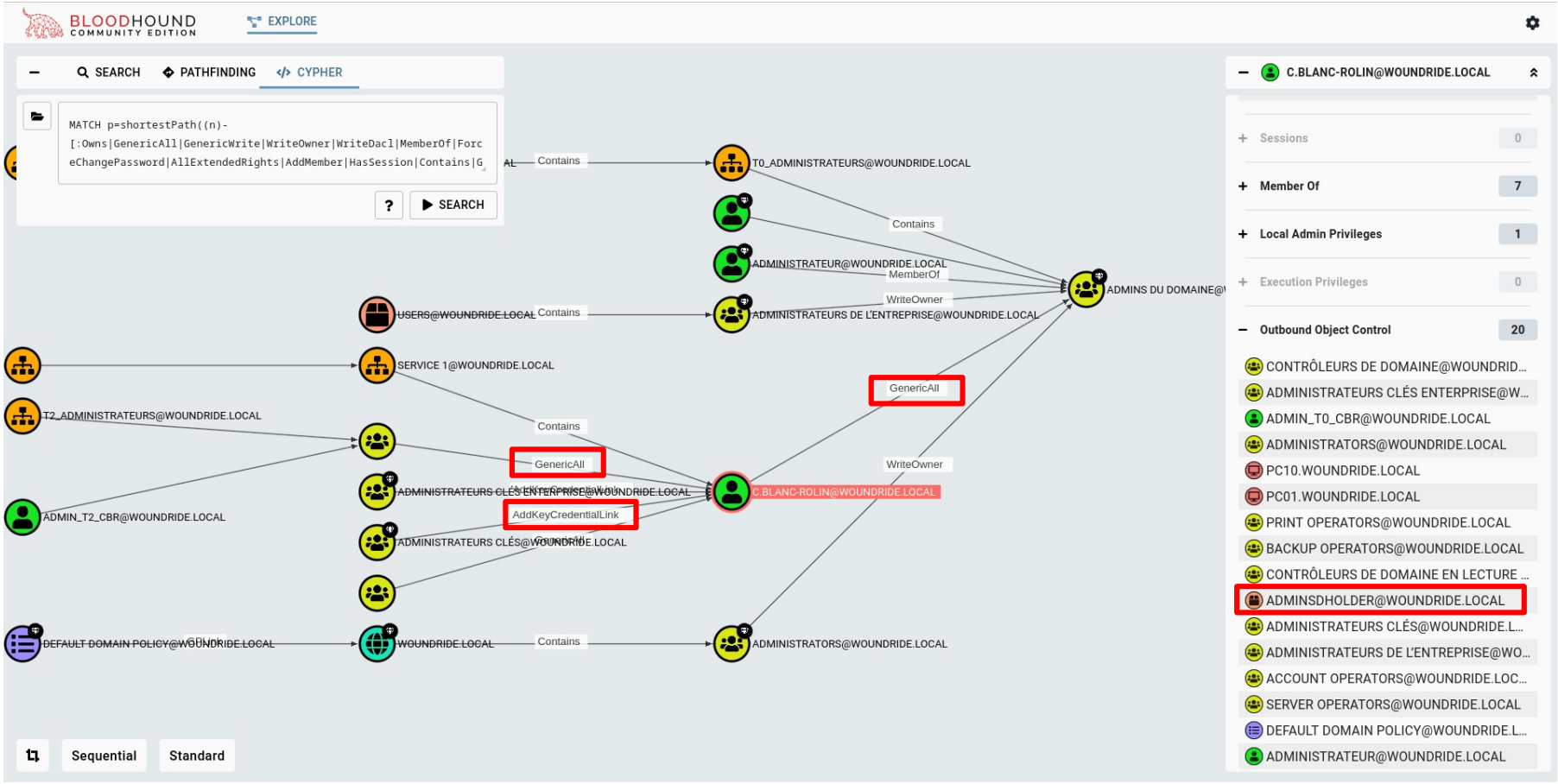
Détection via les journaux de sécurité



Détection via les chemins de contrôle (Forest Druid)



Détection via les chemins de contrôle (BloodHound)



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