Defendiendo Active Directory con Técnicas Ofensivas

Whoami

Pentester en Telefónica Tech

Creador de Deep Hacking (*deephacking.tech*)

- eJPTv1
- eCPPTv2
- eWPTv1
- eWPTX
- CRTP
- CARTP
- PNPT
- CWP
- OSWP
- OSCP
- OSEP

@sikumy

/in/juanantonio-gonzalez

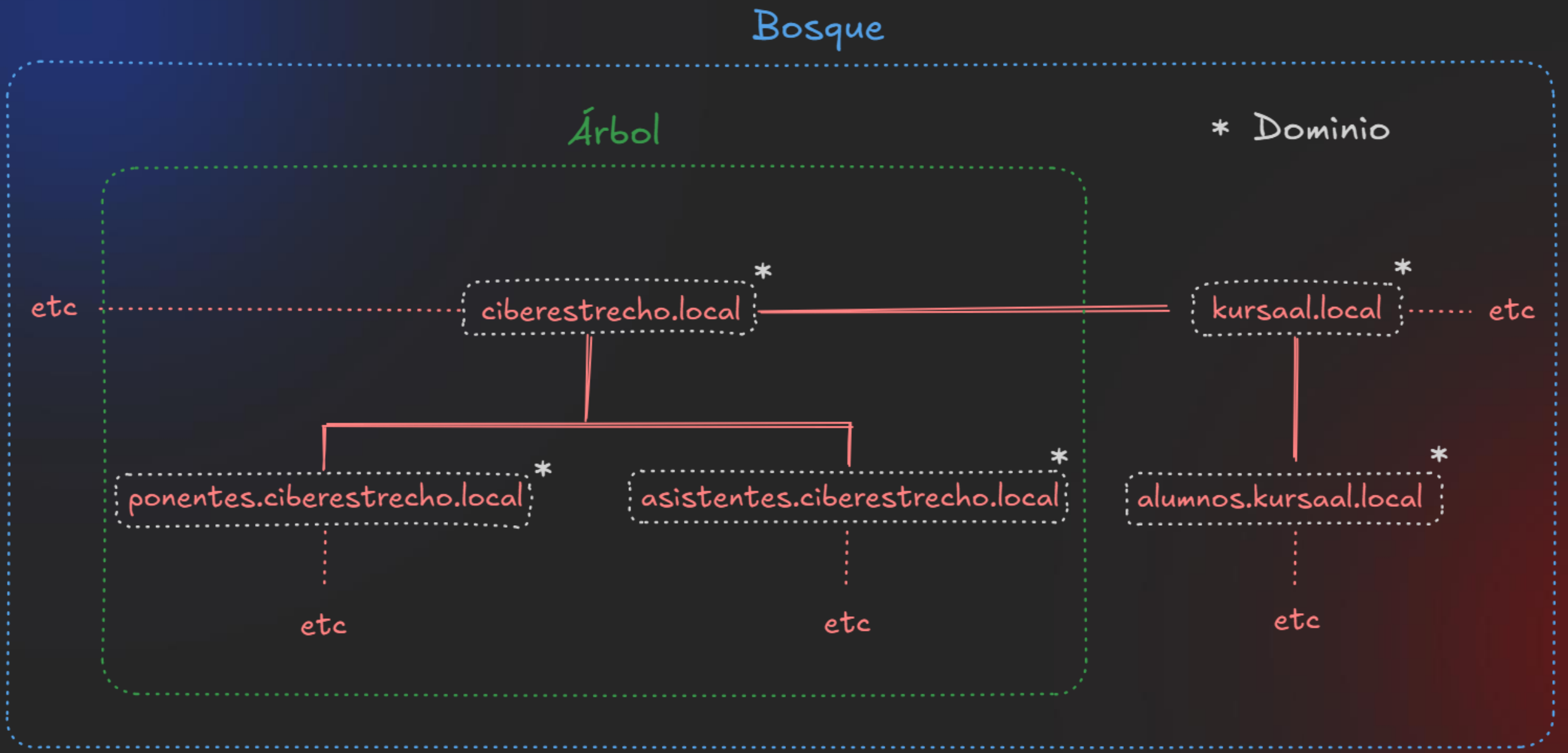
discord.gg/TVcDmHduAm

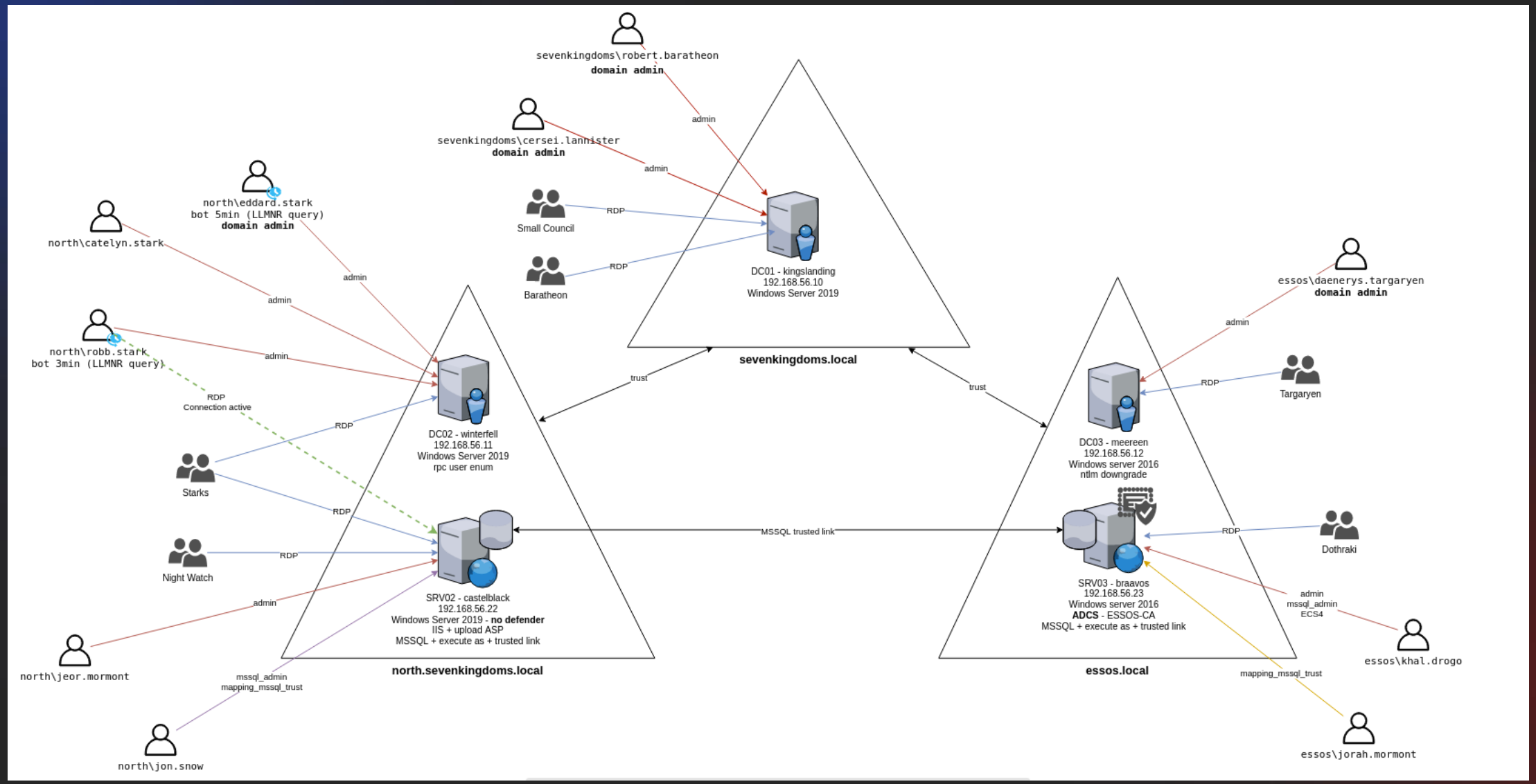
¿Qué vamos a ver?

- Introducción a Active Directory.
- Modelos de seguridad.
- BloodHound y extensiones.
- Fallos comunes.

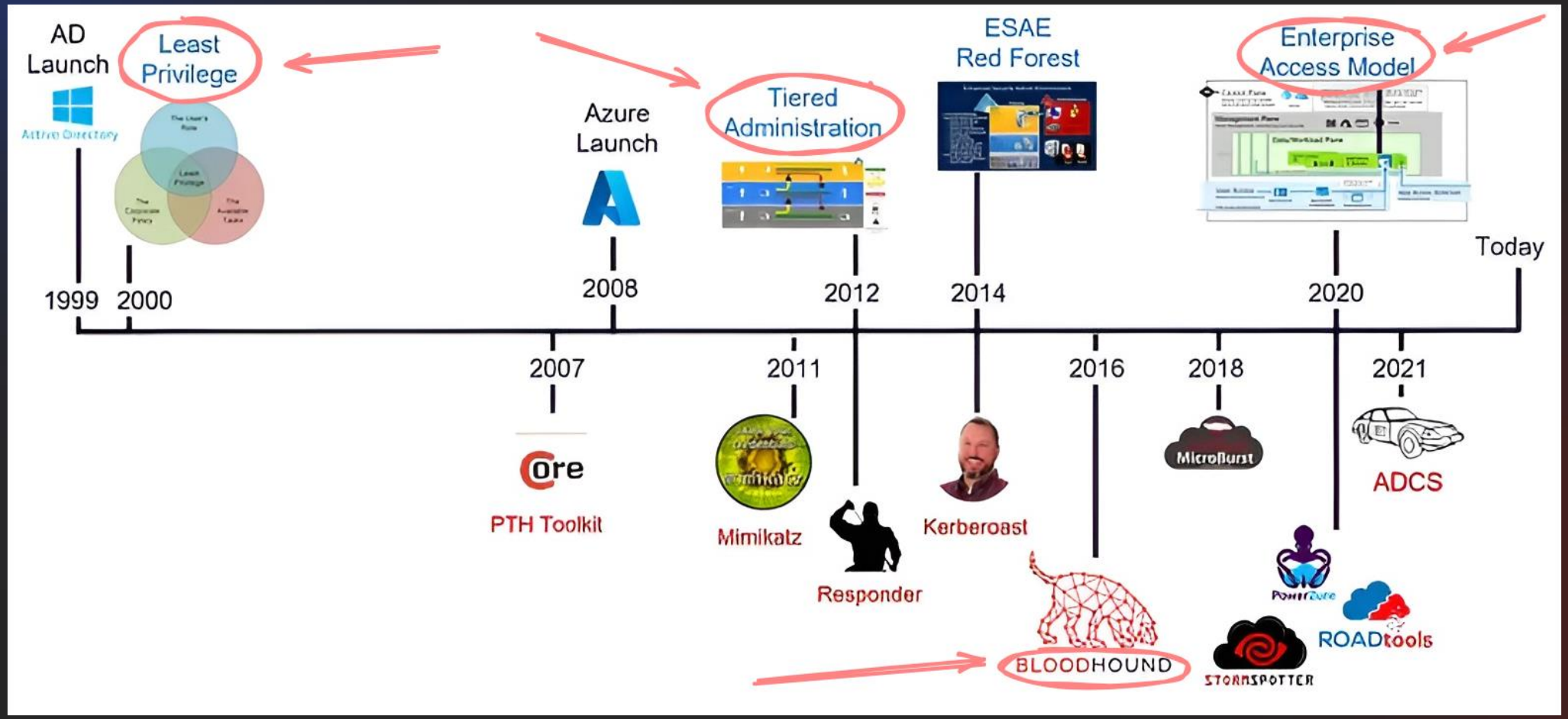
¿Qué es Active Directory?

- Inicio a principios de los 90 y lanzamiento en 1999.
- Solución para la gestión de datos y recursos en grandes organizaciones.
- Estructura jerárquica: Dominios, árboles y bosques.
- Todo es un objeto (usuarios, equipos, grupos, etc.).


Bosque
Árbol
* Dominio
etc
ciberestrecho.local
*
kursaal.local
*
etc
ponentes.ciberestrecho.local
*
asistentes.ciberestrecho.local
*
alumnos.kursaal.local
*
etc
etc
etc


sevenkingdoms\robert.baratheon
domain admin
admin
sevenkingdoms\cersei.lannister
domain admin
admin
Small Council
RDP
Baratheon
RDP
DC01 - kingslanding
192.168.56.10
Windows Server 2019
sevenkingdoms.local
north\eddard.stark
bot 5min (LLMNR query)
domain admin
admin
north\catelyn.stark
admin
north\robb.stark
bot 3min (LLMNR query)
admin
RDP
Connection active
RDP
Starks
RDP
Night Watch
RDP
admin
north\jeor.mormont
mssql_admin
mapping_mssql_trust
north\jon.snow
DC02 - winterfell
192.168.56.11
Windows Server 2019
rpc user enum
SRV02 - castelblack
192.168.56.22
Windows Server 2019 - no defender
IIS + upload ASP
MSSQL + execute as + trusted link
north.sevenkingdoms.local
trust
trust
MSSQL trusted link
essos\daenerys.targaryen
domain admin
admin
RDP
Targaryen
DC03 - meereen
192.168.56.12
Windows server 2016
ntlm downgrade
RDP
Dothraki
admin
mssql_admin
ECS4
essos\khal.drogo
SRV03 - braavos
192.168.56.23
Windows server 2016
ADCS - ESSOS-CA
MSSQL + execute as + trusted link
mapping_mssql_trust
essos\jorah.mormont
essos.local

Evolución de la seguridad de Active Directory



Problemas al definir modelos de seguridad

- Cada entorno de Active Directory es único.
- Al ser único es imposible definir una correcta implementación de un modelo.
- Los modelos deben ser tratados de manera conceptual y no absoluta.
- Por este último punto, es posible encontrar diagramas que representen un modelo, pero que tengan ligeras modificaciones.

2000 – Mínimo Privilegio (PoLP)

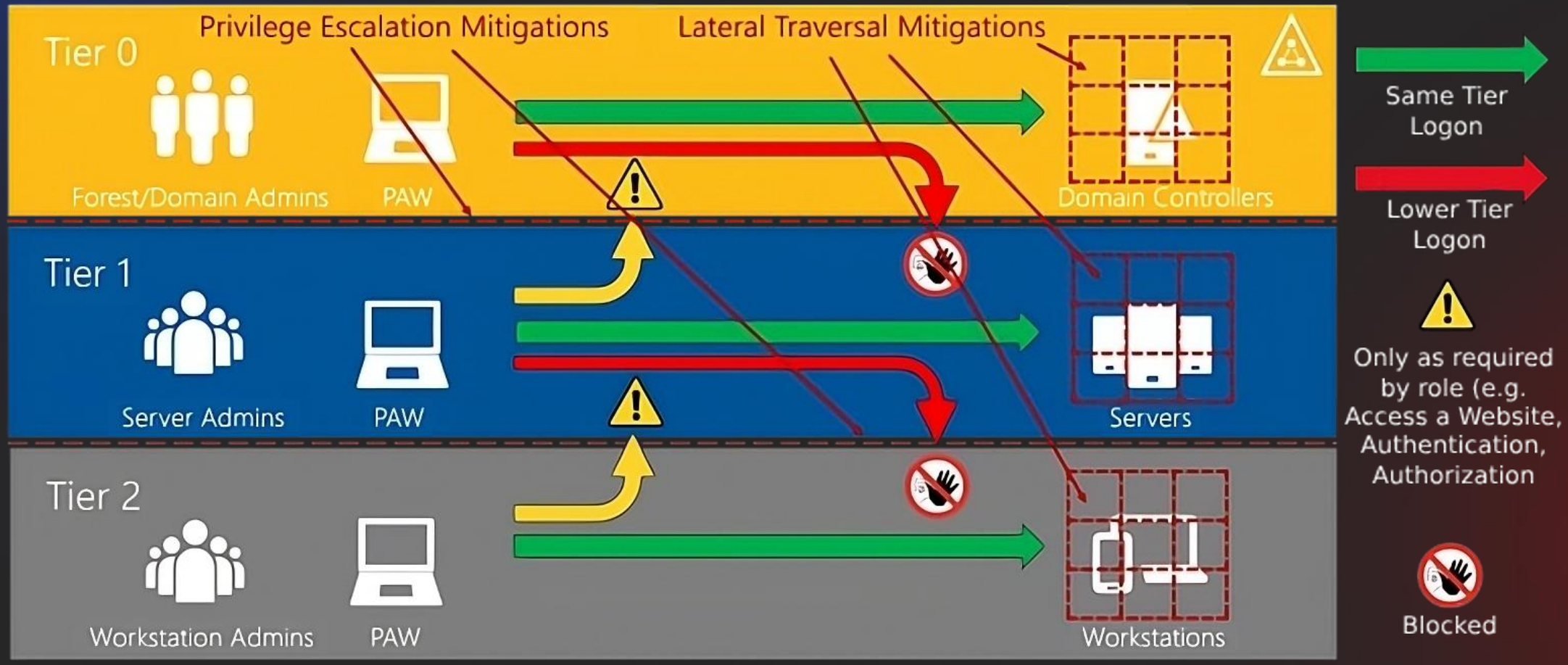
- Minimiza la superficie de ataque.
- Detiene la propagación de *malware*.
- Limita el impacto en caso de incidentes de seguridad.
- Sirve como base para modelos de seguridad más avanzados.

2012 – Administración por Niveles (*legacy*)

- Modelo centrado en Active Directory on-premises.
- La idea principal de este modelo es limitar el acceso usando el principio de mínimo privilegio.
- El modelo tradicional tiene 3 niveles (*tiers*): 0, 1 y 2
  - Tier 0: Encontramos los equipos más críticos*.
  - Tier 1: Servidores que no son lo suficientemente críticos como para estar en el Tier 0.
  - Tier 2: Estaciones de trabajo del día a día o servidores que ejecutan aplicaciones usadas por todos o casi todos los empleados.

"No Control UP, No Exposure DOWN"

The Microsoft Credential Tier Model



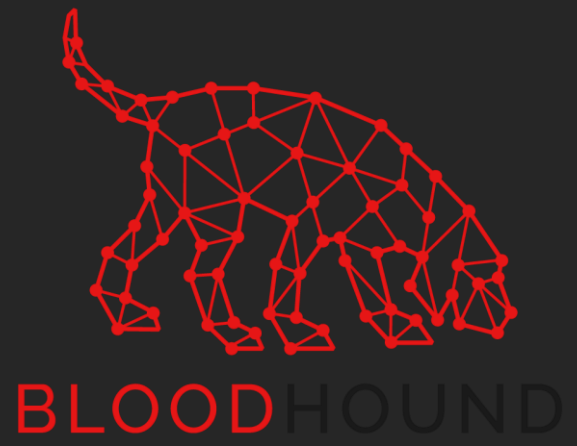
¿Qué ganamos con un modelo por niveles?

- Mayor organización y estructuración.
- Las credenciales robadas no son “atractivas”. Solo permitirá movimientos horizontales (dentro del mismo *Tier*).
- Si José Luís de recursos humanos se come un Phishing, no comprometerá de manera directa los activos más críticos.
- Este modelo no es perfecto, pero sí una capa más de protección.

2016 - BloodHound

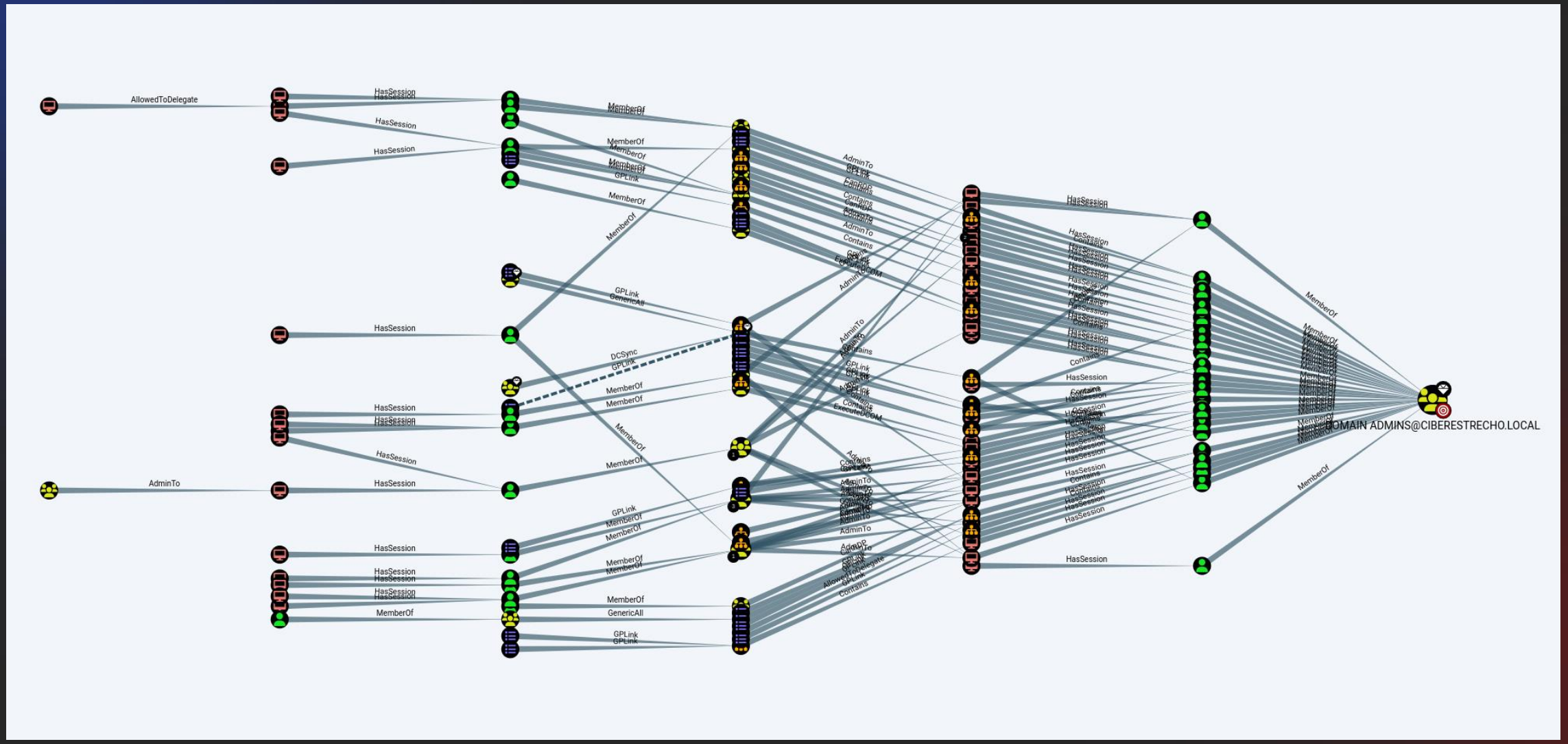
Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.

John Lambert, Investigador de Seguridad en Microsoft - 2015



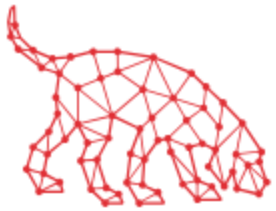
	A	B	C
1	LISTA DE SERVIDORES	IP	DESCRIPCIÓN
2	SRVDC01	192.168.1.10	Servidor principal para el dominio de Active Directory, gestiona autenticación y políticas de grupo.
3	SRVCA	192.168.1.11	Emite certificados de seguridad para autenticación y cifrado.
4	SRVMSSQL	192.168.1.12	Servidor donde se ejecuta Microsoft SQL Server para aplicaciones de bases de datos.
5	SRVFS01	192.168.1.13	Almacén de archivos entre usuarios en la red.
6	SRVEXCHANGE	192.168.1.14	Servidor de Microsoft Exchange para gestionar el correo electrónico corporativo.
7	SRVWEB01	192.168.1.15	Alojamiento de aplicaciones web internas o externas de la empresa.
8	SRVAPP01	192.168.1.16	Hospeda aplicaciones empresariales o de gestión.
9	SRVBACKUP	192.168.1.17	Almacena copias de seguridad de los datos y configuraciones críticas.
10	SRVPRINT	192.168.1.18	Gestiona impresoras en red.
11	SRVPROXY	192.168.1.19	Controla el acceso a Internet y filtra contenido para mejorar la seguridad.
12	SRVDNS	192.168.1.20	Resuelve los nombres de dominio interno, traduce nombres de dominio en direcciones IP.
13	SRVDHCP	192.168.1.21	Asigna direcciones IP dinámicas a los dispositivos en la red.
14	SRVLDAP	192.168.1.22	Proporciona un directorio de usuarios para aplicaciones que necesitan autenticación centralizada.
15	SRVMONITOR	192.168.1.23	Supervisa el estado y rendimiento de la infraestructura de TI.
16	SRVREPORT	192.168.1.24	Genera y almacena informes de rendimiento, actividad y auditoría.
17	SRVMAIL	192.168.1.25	Servidor SMTP para enviar correos salientes de aplicaciones internas.
18	SRVCRM	192.168.1.26	Hospeda el sistema de gestión de relaciones con clientes.
19	SRVFILE02	192.168.1.27	Servidor de redundancia y balanceo de carga de archivos.
20	SRVSEC01	192.168.1.28	Ejecuta herramientas de control como antivirus corporativo o firewall de aplicaciones.
21	SRVPN	192.168.1.29	Servidor VPN para el acceso seguro a la red corporativa.
22	SRVLOG	192.168.1.30	Almacena y gestiona los registros de eventos y dispositivos.
23	SRVINTRANET	192.168.1.31	Hospeda el portal interno de información y recursos corporativos.
24	SRVDATA	192.168.1.32	Almacena grandes volúmenes de datos para análisis o BI.
25	SRVDOC	192.168.1.33	Centraliza los documentos y archivos corporativos.
26	SRVTEST	192.168.1.34	Ambiente de prueba para aplicaciones y nuevas implementaciones.

- [x] ¿Existe un inventario de todos los servidores?
- [ ] ¿Se ha revisado la configuración de las plantillas de SRVCA?
- [ ] ¿Has configurado una política de contraseñas robustas?
- [x] ¿Se han eliminado los usuarios y equipos inactivos del dominio?
- [ ] ¿Has deshabilitado el acceso anónimo en el SRVFILE02?
- [ ] ¿Has modificado la contraseña por defecto de la app de SRVAPP01?


AllowedToDelegate
AdminTo
HasSession
MemberOf
GPLink
GenericAll
DCSync
Contains
AdminTo
DOMAIN ADMINS@CIBERESTRECHO.LOCAL

BloodHound: Six Degrees of Domain Admin

- Teoría de grafos
  - Nodos: Objetos como usuarios, grupos, ordenadores, etc.
  - Aristas: Relaciones entre objetos.
- Backend
  - Neo4j como base de datos.
  - Lenguaje de consulta Cypher.
- Ingestor (.exe, .ps1, .py, …)
  - Recolecta información del directorio activo y lo almacena en formato JSON.
- Frontend:
  - Aplicación JavaScript/HTML para mostrar los grafos, importar datos y realizar consultas.



BloodHound Legacy

Where it all started: Six Degrees of Domain Admin

Download on GitHub →

BLOODHOUND COMMUNITY EDITION

BloodHound CE

Map Active Directory and Azure Attack Paths

Download on Github →

BLOODHOUND ENTERPRISE

BloodHound Enterprise

Continuously Monitor, Prioritize, and Eliminate Attack Paths in Active Directory

INTERESTED IN A FREE TRIAL?

Contact Us →

BloodHound

DOMAIN ADMINS@CIBERESTRECHO.I

Database Info | Node Info | Analysis

DOMAIN ADMINS@CIBERESTRECHO.LOCAL

OVERVIEW

Sessions	33
Reachable High Value Targets	29

NODE PROPERTIES

Object ID	S-1-5-21-883232822-274137685-4173207997-512

EXTRA PROPERTIES

domain	CIBERESTRECHO.LOCAL
has_members	True
is_admin	True
is_da	True
is_da_dc	True
is_dag	True
	False
	25

Edge Filtering

Default Edges
- MemberOf
- HasSession
- AdminTo

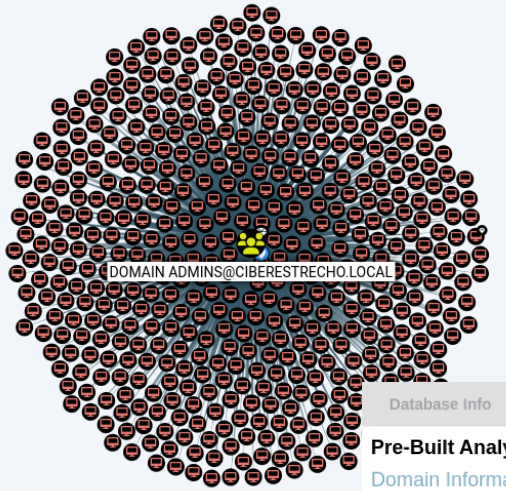
ACL Edges
- AllExtendedRights
- AddMember
- ForceChangePassword
- GenericAll
- GenericWrite
- Owns
- WriteDacl
- WriteOwner
- ReadLAPSPassword
- ReadGMSAPassword
- AddKeyCredentialLink
- WriteSPN
- AddSelf
- AddAllowedToAct
- WriteAccountRestrictions
- DCSync
- SyncLAPSPassword

Containers
- Contains
- GPLink

Special
- CanRDP
- CanPSRemote
- ExecuteDCOM
- AllowedToDelegate
- AllowedToAct
- SQLAdmin
- HasSIDHistory
- DumpSMSAPassword

Azure Edges
- AZAvereContributor
- AZContains
- AZContributor
- AZGetCertificates
- AZGetKeys
- AZGetSecrets
- AZHasRole
- AZMemberOf
- AZRunsAs
- AZVMContributor
- AZVMAdminLogin
- AZAddMembers
- AZAddSecret
- AZExecuteCommand
- AZGlobalAdmin
- AZPrivilegedAuthAdmin
- AZPrivilegedRoleAdmin
- AZResetPassword
- AZUserAccessAdministrator
- AZOwns
- AZCloudAppAdmin
- AZAppAdmin
- AZAddOwner
- AZManagedIdentity
- AZKeyVaultContributor
- AZNodeResourceGroup
- AZWebsiteContributor
- AZLogicAppContributor
- AZAutomationContributor
- AZAKSContributor

MS Graph App Roles
- AZMGAddSecret
- AZMGAddOwner
- AZMGAddMember
- AZMGGrantAppRoles
- AZMGGrantRole



Raw Query

Enter a cypher query. Your query must return nodes or paths.

Database Info | Node Info | Analysis

DB STATS

Address	bolt://localhost:7687
DB User	neo4j
Sessions	526
Relationships	8408
ACLs	1519
Azure Relationships	0

ON-PREM OBJECTS

Users	501
Groups	508
Computers	501
OUS	21
GPOs	22
Domains	1

Database Info | Node Info | Analysis

Pre-Built Analytics Queries

Domain Information

- Find all Domain Admins
- Map Domain Trusts
- Find Computers with Unsupported Operating Systems

Dangerous Privileges

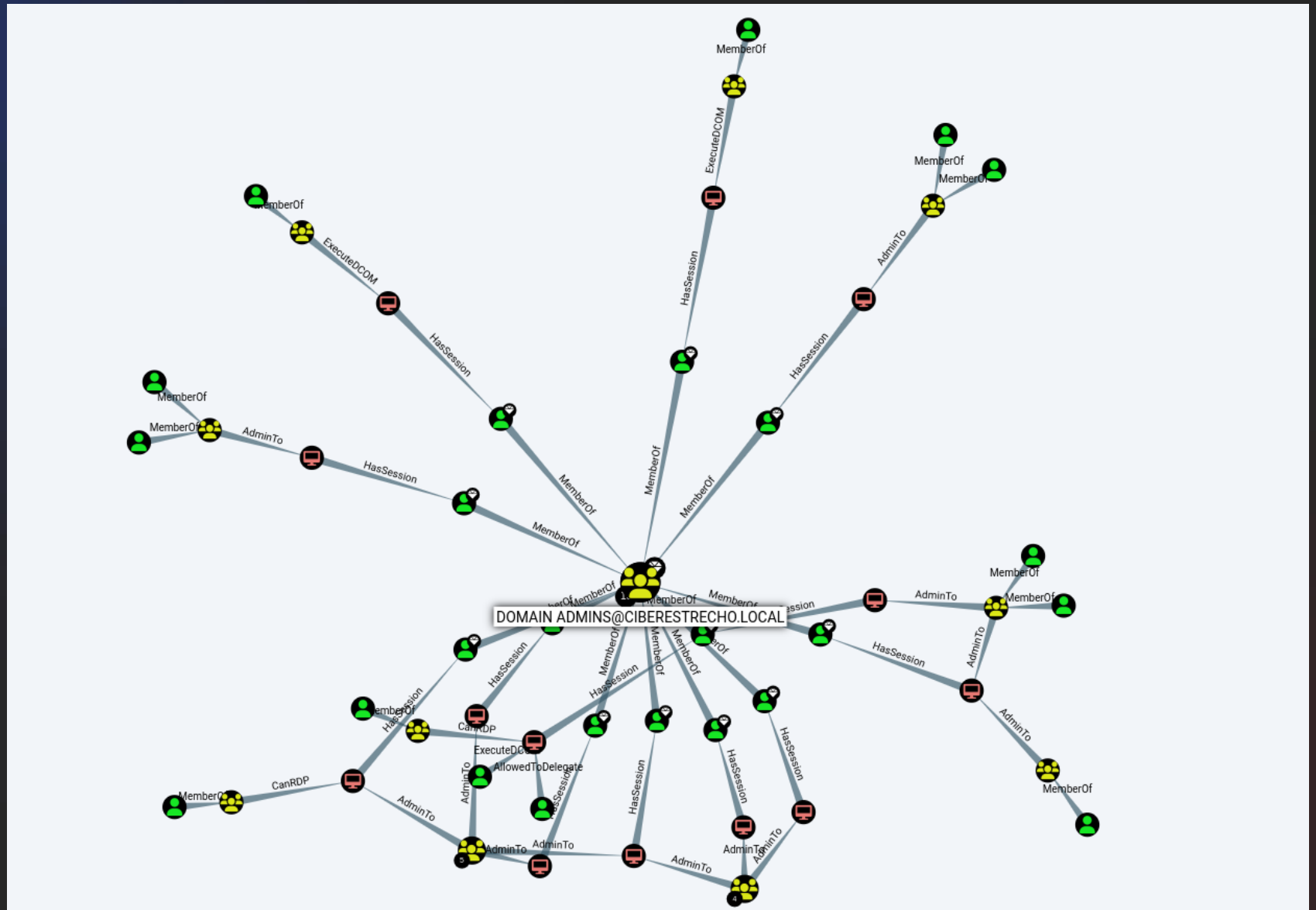
- Find Principals with DCSync Rights
- Users with Foreign Domain Group Membership
- Groups with Foreign Domain Group Membership
- Find Computers where Domain Users are Local Admin
- Find Computers where Domain Users can read LAPS passwords
- Find All Paths from Domain Users to High Value Targets
- Find Workstations where Domain Users can RDP
- Find Servers where Domain Users can RDP
- Find Dangerous Privileges for Domain Users Groups
- Find Domain Admin Logons to non-Domain Controllers

Kerberos Interaction

Consultas Cypher

```
MATCH (n:User),
      (m:Group {name:'DOMAIN ADMINS@CIBERESTRECHO.LOCAL'}),
      p=shortestPath((
        n)-[r:MemberOf|HasSession|AdminTo|AllExtendedRights|
        AddMember|ForceChangePassword|GenericAll|GenericWrite|Owns|
        WriteDacl|WriteOwner|CanRDP|ExecuteDCOM|AllowedToDelegate|
        ReadLAPSPassword|Contains|GpLink|AddAllowedToAct|
        AllowedToAct*1..]->(m))
RETURN p
```

- MATCH: Busca nodos en el grafo.
- p, r, m, n: Variables arbitrarias usadas para nodos (n,m), caminos (p) y relaciones (r).
- User y Group: Tipo de nodo en el grafo.
- [:TYPE*minHops..maxHops]: Relación entre nodos con rango de saltos.
- -->, <--, --: Dirección de la arista entre los nodos.
- {key:value}: Propiedades para filtrar nodos.
- RETURN: Define los datos que son devueltos por la consulta.



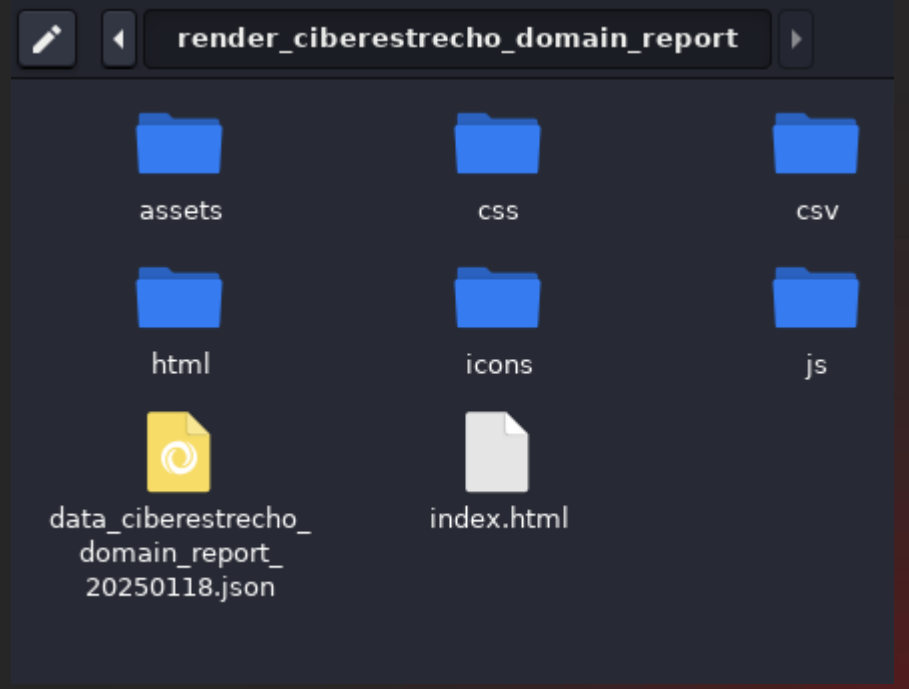
Raw Query

```
MATCH (n:User ),(m:Group {name:'DOMAIN ADMINS@CIBERESTRECHO.LOCAL'}),p=shortestPath((n)-[:MemberOf|HasSession|AdminTo|AllExtendedRights|AddMember|ForceChangePassword|(
```

Extendiendo BloodHound: AD_Miner

- Herramienta de auditoría de Active Directory.
- Aprovecha las consultas Cypher para extraer datos.
- Proporciona un reporte basado en web con una interfaz dinámica:
  - Listados detallados de debilidades identificadas.
  - Grafos dinámicos para un análisis visual.
  - Histórico de indicadores clave para observar los cambios en el tiempo.
  - Clasificación de riesgos para priorizar acciones y amenazas.

```
(ad-miner-py3.12) 19/01/25 21:32 [~/tools/AD_Miner]
❯ AD-miner -cf ciberestrecho_domain_report -u neo4j -p bloodhound
[+] Your neo4j database uses neo4j version 4.4.26
[+] Group : 507 | Domain : 1 | GPO : 21 | OU : 21 | GPO : 1 | Computer : 501 | User : 499 | User : 1 | User : 1 | Relations : 8408
[1/162] [+] Requesting : Checking if Graph Data Science neo4j plugin is installed
[+] GDS plugin not installed.
[+] Not using exploitability for paths computation.
[-] Done in 0.03 s - 1 objects
[2/162] [+] Requesting : Delete orphan objects that have no labels
[-] Done in 0.03 s - 0 objects
[3/162] [+] Requesting : Clean AD Miner custom attributes
[-] Done in 0.05 s - 0 objects
[4/162] [+] Requesting : Delete objects for which SID could not resolved
[-] Done in 0.03 s - 0 objects
[5/162] [+] Requesting : Delete ADLocalGroup objects
[-] Done in 0.01 s - 0 objects
[6/162] [+] Requesting : Checking relation types
[!] The following relations are not used (yet) for general AD Miner path finding:
[!] GpLink
[-] Done in 0.03 s - 17 objects
[7/162] [+] Requesting : Set domain names to upper case when not the case
[-] Done in 0.02 s - 0 objects
[8/162] [+] Requesting : Set domain attributes to domain objects when not the case
[-] Done in 0.02 s - 0 objects
[9/162] [+] Requesting : Check for unexisting domain objects
[-] Done in 0.02 s - 1 objects
[10/162] [+] Requesting : Check for Group objects without domain attribute
[-] Done in 0.03 s - 0 objects
[11/162] [+] Requesting : Clean AD Miner custom relations
[-] Done in 0.01 s - 0 objects
[12/162] [+] Requesting : Set is_server=TRUE to computers for which operatingsystem contains Server)
[-] Done in 0.02 s - 0 objects
[13/162] [+] Requesting : Set is_server=FALSE to other computers )
[-] Done in 0.02 s - 0 objects
[14/162] [+] Requesting : Set dc=TRUE to computers that are domain controllers)
[-] Done in 0.03 s - 0 objects
[15/162] [+] Requesting : Set dc=FALSE to computers that are not domain controllers)
[-] Done in 0.02 s - 0 objects
[16/162] [+] Requesting : Set is_dcg=TRUE to domain controllers groups
[-] Done in 0.02 s - 0 objects
[17/162] [+] Requesting : Set is_dcg=TRUE to domain controllers groups
[-] Done in 0.02 s - 0 objects
[18/162] [+] Requesting : Set isacl to TRUE for ADCS privilege escalation paths (ADCSESCxx)
```




```
[+] Generating control non-dc_with_unconstrained_delegations
[+] Generate paths to Kerberos Unconstrained Delegations
[-] Done in 0.0s
[+] Done in 24.44 s! Program finished. Report generated in render_ciberestrecho_domain_report
(ad-miner-py3.12) 19/01/25 21:33 [~/tools/AD_Miner]
❯
```

AD Miner

ciberestrecho_domain_report - 18/01/2025

On-premise Risk rating

CRITICAL

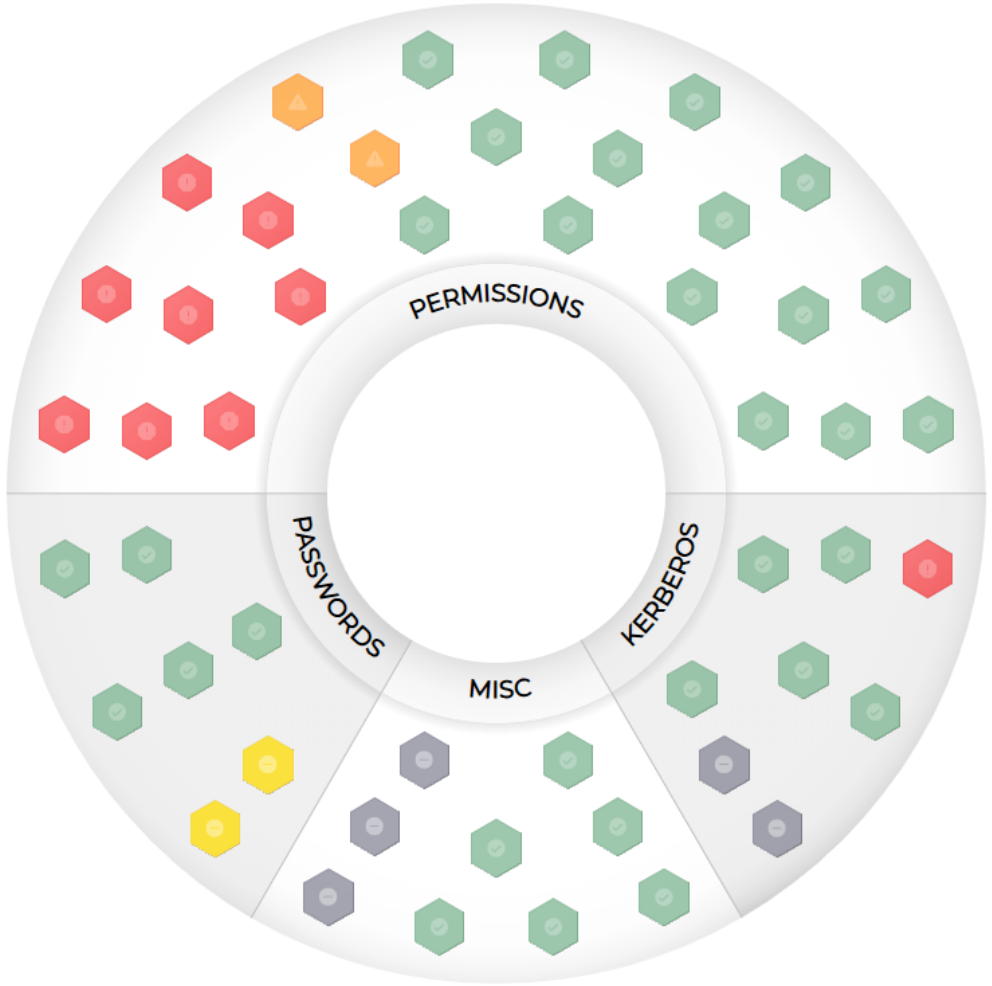
Indicators of exposures breakdown

Immediate risk	9
Potential risk	2
Minor risk	2
Handled risk	31

Recap | Users | Computers | OS

1 Domain (1 collected)	Details
1 domain controllers	Details
25 domain admins	Details
500 users	Details
508 groups	Details
501 computers	Details
0 ADCS servers	Details

Overview | Indicators of exposure breakdown



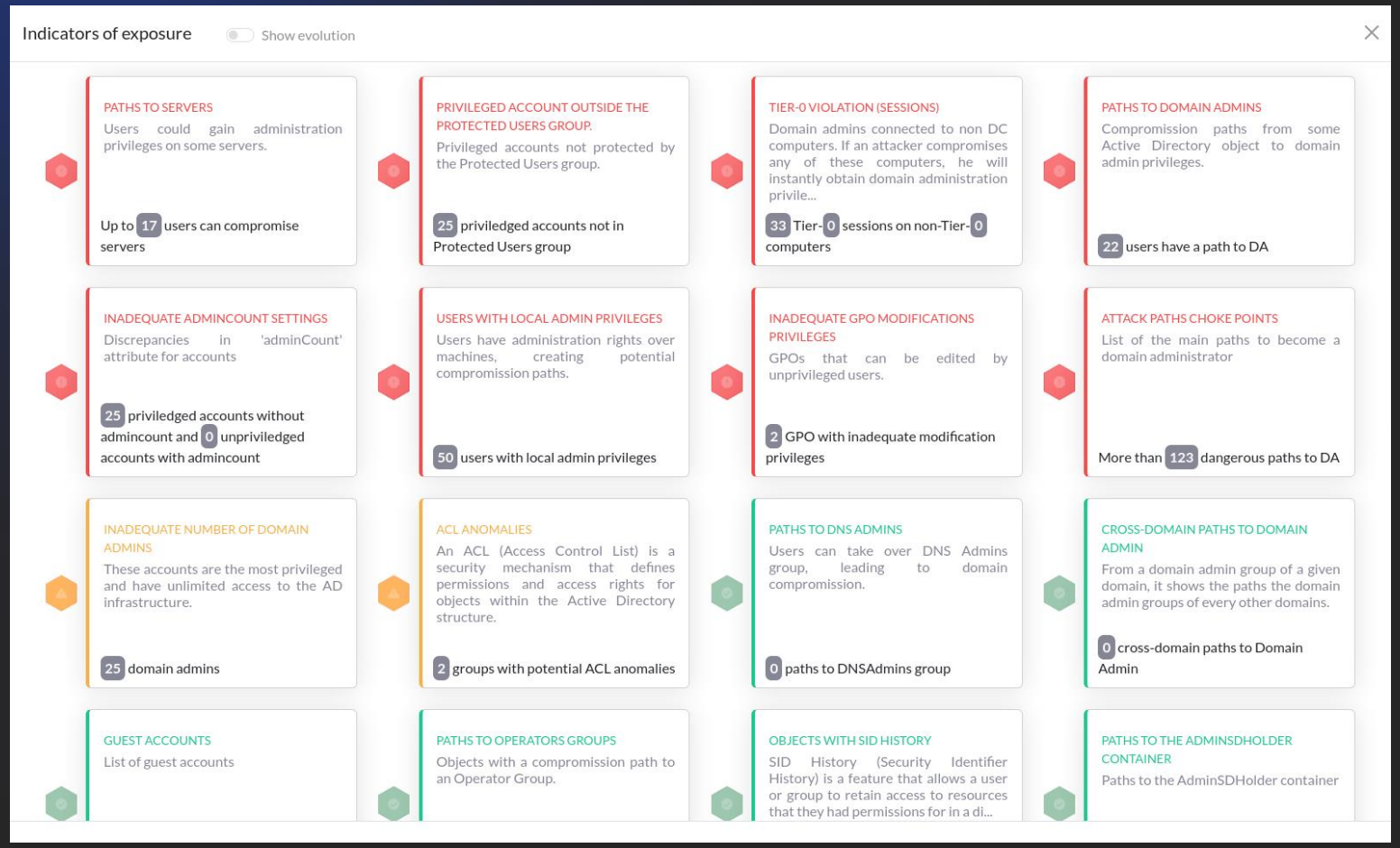
9 Dangerous issues

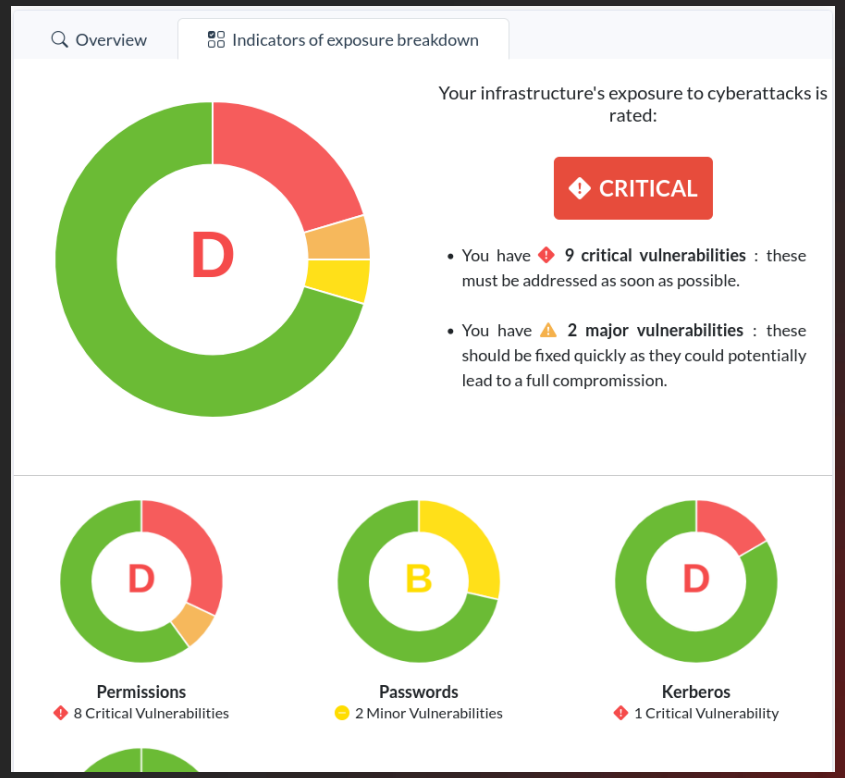
Must be solved as soon as possible

- Paths to servers
- Kerberoastable accounts
- Privileged account outside the protected users group.
- Tier-0 violation (sessions)
- Paths to Domain Admins
- Inadequate AdminCount settings
- Users with local admin privileges
- Inadequate GPO modifications privileges
- Attack paths choke points

2 Alerts

These issues should be looked into

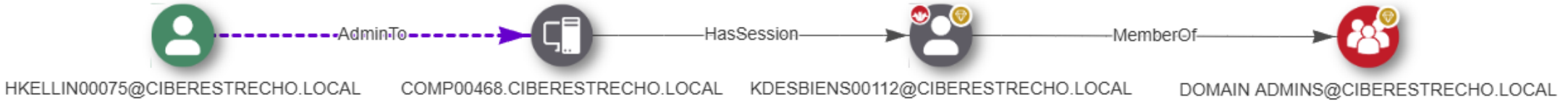

Indicators of exposure
Show evolution
PATHS TO SERVERS
Users could gain administration privileges on some servers.
Up to 17 users can compromise servers
PRIVILEGED ACCOUNT OUTSIDE THE PROTECTED USERS GROUP.
Privileged accounts not protected by the Protected Users group.
25 priviledged accounts not in Protected Users group
TIER-0 VIOLATION (SESSIONS)
Domain admins connected to non DC computers. If an attacker compromises any of these computers, he will instantly obtain domain administration privile...
33 Tier-0 sessions on non-Tier-0 computers
PATHS TO DOMAIN ADMINS
Compromission paths from some Active Directory object to domain admin privileges.
22 users have a path to DA
INADEQUATE ADMINCOUNT SETTINGS
Discrepancies in 'adminCount' attribute for accounts
25 priviledged accounts without admincount and 0 unpriviledged accounts with admincount
USERS WITH LOCAL ADMIN PRIVILEGES
Users have administration rights over machines, creating potential compromission paths.
50 users with local admin privileges
INADEQUATE GPO MODIFICATIONS PRIVILEGES
GPOs that can be edited by unprivileged users.
2 GPO with inadequate modification privileges
ATTACK PATHS CHOKE POINTS
List of the main paths to become a domain administrator
More than 123 dangerous paths to DA
INADEQUATE NUMBER OF DOMAIN ADMINS
These accounts are the most privileged and have unlimited access to the AD infrastructure.
25 domain admins
ACL ANOMALIES
An ACL (Access Control List) is a security mechanism that defines permissions and access rights for objects within the Active Directory structure.
2 groups with potential ACL anomalies
PATHS TO DNS ADMINS
Users can take over DNS Admins group, leading to domain compromission.
0 paths to DNSAdmins group
CROSS-DOMAIN PATHS TO DOMAIN ADMIN
From a domain admin group of a given domain, it shows the paths the domain admin groups of every other domains.
0 cross-domain paths to Domain Admin
GUEST ACCOUNTS
List of guest accounts
PATHS TO OPERATORS GROUPS
Objects with a compromission path to an Operator Group.
OBJECTS WITH SID HISTORY
SID History (Security Identifier History) is a feature that allows a user or group to retain access to resources that they had permissions for in a di...
PATHS TO THE ADMINSDHOLDER CONTAINER
Paths to the AdminSDHolder container


Overview
Indicators of exposure breakdown
D
Your infrastructure's exposure to cyberattacks is rated:
CRITICAL
• You have 9 critical vulnerabilities : these must be addressed as soon as possible.
• You have 2 major vulnerabilities : these should be fixed quickly as they could potentially lead to a full compromission.
D
Permissions
8 Critical Vulnerabilities
B
Passwords
2 Minor Vulnerabilities
D
Kerberos
1 Critical Vulnerability

AD Miner

Users with local admin privileges

User	Kerberoastable	Last Password Change	List Of Computers	Path To Computers	Path To DA
BBANNAN00019@CIBERESTRECHO.LOCAL	-	Never	4 Computers	Path to computers	-
MROMULUS00025@CIBERESTRECHO.LOCAL	-	11 months and 25 days	501 Computers	Path to computers	50 paths to DA (1 domain)
RDETTORI00030@CIBERESTRECHO.LOCAL	-	Never	500 Computers	Path to computers	50 paths to DA (1 domain)
BBOIANI00057@CIBERESTRECHO.LOCAL	-	Never	501 Computers	Path to computers	50 paths to DA (1 domain)
LSMALLIDGE00059@CIBERESTRECHO.LOCAL	-	Never	425 Computers	Path to computers	43 paths to DA (1 domain)
BWOLLARD00067@CIBERESTRECHO.LOCAL	-	Never	501 Computers	Path to computers	50 paths to DA (1 domain)
HKELLIN00075@CIBERESTRECHO.LOCAL	-	Never	18 Computers	Path to computers	1 path to DA (1 domain)
CCAVIN00093@CIBERESTRECHO.LOCAL	-	7 days	1 Computer	Path to computers	-
FTARSKI00103@CIBERESTRECHO.LOCAL	-	Never	501 Computers	Path to computers	50 paths to DA (1 domain)
KQUEST00108@CIBERESTRECHO.LOCAL	-	Never	501 Computers	Path to computers	50 paths to DA (1 domain)
KDESBIENS00112@CIBERESTRECHO.LOCAL	-	Never	501 Computers	Path to computers	50 paths to DA (1 domain)
ACROUSHORN00113@CIBERESTRECHO.LOCAL	-	Never	5 Computers	Path to computers	1 path to DA (1 domain)
BSOHR00126@CIBERESTRECHO.LOCAL	-	4 months and 18 days	427 Computers	Path to computers	40 paths to DA (1 domain)



Extendiendo BloodHound: Cypheroth

- Script en bash que automatiza la ejecución de consultas Cypher.
- Extensible. Puedes añadir las consultas que quieras.
- 60 consultas predefinidas.

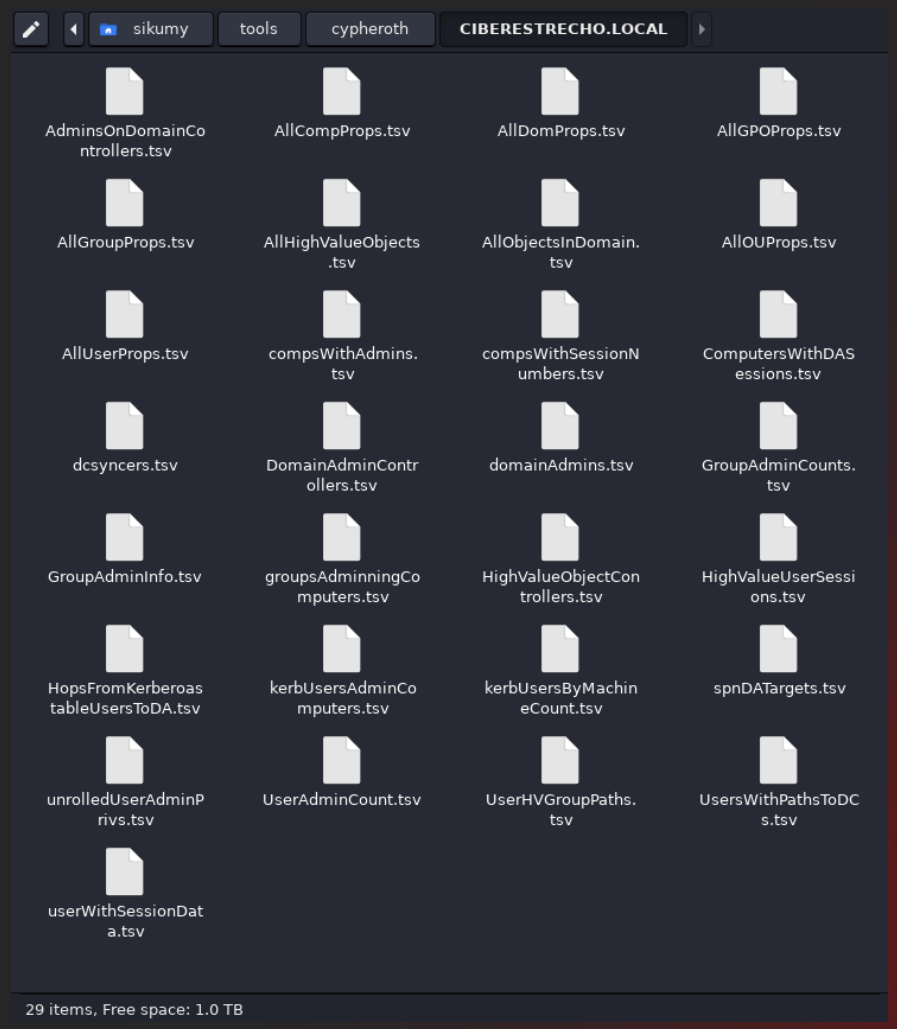
```
19/01/25 21:43 [~/tools/cypheroth]
❯ ./cypheroth.sh -d CIBERESTRECHO.local -u neo4j -p bloodhound -v true 2> /dev/null
 ☑Neo4j started
 ☑Connected to the database.


Running Cypheroth queries.

All Objects that are members of High Value Groups
Saved to ./CIBERESTRECHO.LOCAL/AllHighValueObjects.tsv
Sample:
ObjectType      ObjectName      HighValueGroupName
[Computer       "Base"]         FLLABDC@CIBERESTRECHO.LOCAL     "DOMAIN CONTROLLERS@CIBERESTRECHO.LOCAL"
[Computer       "Base"]         FLLABDC@CIBERESTRECHO.LOCAL     "ENTERPRISE DOMAIN CONTROLLERS@CIBERESTRECHO.LOCAL"
[User    "Base"]        WHORNACK00191@CIBERESTRECHO.LOCAL       "DOMAIN ADMINS@CIBERESTRECHO.LOCAL"
[User    "Base"]        LLEDEC00378@CIBERESTRECHO.LOCAL         "DOMAIN ADMINS@CIBERESTRECHO.LOCAL"
[User    "Base"]        CMUZYKA00346@CIBERESTRECHO.LOCAL        "DOMAIN ADMINS@CIBERESTRECHO.LOCAL"
[User    "Base"]        NROSARO00488@CIBERESTRECHO.LOCAL        "DOMAIN ADMINS@CIBERESTRECHO.LOCAL"
[User    "Base"]        KCIANFLONE00425@CIBERESTRECHO.LOCAL     "DOMAIN ADMINS@CIBERESTRECHO.LOCAL"
[User    "Base"]        MROMULUS00025@CIBERESTRECHO.LOCAL       "DOMAIN ADMINS@CIBERESTRECHO.LOCAL"
[User    "Base"]        KDESBIENS00112@CIBERESTRECHO.LOCAL      "DOMAIN ADMINS@CIBERESTRECHO.LOCAL"
[User    "Base"]        KSTANBERY00376@CIBERESTRECHO.LOCAL      "DOMAIN ADMINS@CIBERESTRECHO.LOCAL"
[User    "Base"]        MLOVERICH00199@CIBERESTRECHO.LOCAL      "DOMAIN ADMINS@CIBERESTRECHO.LOCAL"
[User    "Base"]        TOKANE00276@CIBERESTRECHO.LOCAL         "DOMAIN ADMINS@CIBERESTRECHO.LOCAL"
[User    "Base"]        JANA00178@CIBERESTRECHO.LOCAL   "DOMAIN ADMINS@CIBERESTRECHO.LOCAL"
[User    "Base"]        OALSTOTT00230@CIBERESTRECHO.LOCAL       "DOMAIN ADMINS@CIBERESTRECHO.LOCAL"
Line Count: 28

All users with SPN in Domain Admin group, with enabled status and unconstrained delegation status displayed
Saved to ./CIBERESTRECHO.LOCAL/spnDATargets.tsv
Sample:
Username        DisplayName     Enabled         UnconstrainedDelegation
BBOIANI00057@CIBERESTRECHO.LOCAL        Brandie Boiani  TRUE    NULL
FTARSKI00103@CIBERESTRECHO.LOCAL        Francene Tarski         TRUE    NULL
KDESBIENS00112@CIBERESTRECHO.LOCAL      Kip Desbiens    TRUE    NULL
AMCGOWAN00159@CIBERESTRECHO.LOCAL       Ashli Mcgowan   TRUE    NULL
TOKANE00276@CIBERESTRECHO.LOCAL  Tawanna Okane   TRUE    NULL
KSTANBERY00376@CIBERESTRECHO.LOCAL      Karren Stanbery         TRUE    NULL
FLOSCO00383@CIBERESTRECHO.LOCAL  Forrest Losco   TRUE    NULL
DFILKINS00399@CIBERESTRECHO.LOCAL       Doloris Filkins         TRUE    NULL
Line Count: 9

All Domain Admins
Saved to ./CIBERESTRECHO.LOCAL/domainAdmins.tsv
Sample:
UserName        DisplayName     Domain  Enabled         HighValue       SID     Description     Title   Email   LastLogon       LLDate  LLTimeStamp     Passwors
MROMULUS00025@CIBERESTRECHO.LOCAL       Marcy Romulus   CIBERESTRECHO.LOCAL     TRUE    TRUE    S-1-5-21-883232822-274137685-4173207997-1525    NULL    NULL    L
BBOIANI00057@CIBERESTRECHO.LOCAL        Brandie Boiani  CIBERESTRECHO.LOCAL     TRUE    TRUE    S-1-5-21-883232822-274137685-4173207997-1557    NULL    NULL    L
BWOLLARD00067@CIBERESTRECHO.LOCAL       Berneice Wollard        CIBERESTRECHO.LOCAL     TRUE    TRUE    S-1-5-21-883232822-274137685-4173207997-1567    NULL    L
FTARSKI00103@CIBERESTRECHO.LOCAL        Francene Tarski         CIBERESTRECHO.LOCAL     TRUE    TRUE    S-1-5-21-883232822-274137685-4173207997-1603    NULL    L
KQUEST00108@CIBERESTRECHO.LOCAL  Kimberley Quest         CIBERESTRECHO.LOCAL     TRUE    TRUE    S-1-5-21-883232822-274137685-4173207997-1608    NULL    NULL    L
KDESBIENS00112@CIBERESTRECHO.LOCAL      Kip Desbiens    CIBERESTRECHO.LOCAL     TRUE    TRUE    S-1-5-21-883232822-274137685-4173207997-1612    NULL    NULL    L
FMEGA00158@CIBERESTRECHO.LOCAL   Filomena Mega   CIBERESTRECHO.LOCAL     TRUE    TRUE    S-1-5-21-883232822-274137685-4173207997-1658    NULL    NULL    NULL    L
AMCGOWAN00159@CIBERESTRECHO.LOCAL       Ashli Mcgowan   CIBERESTRECHO.LOCAL     TRUE    TRUE    S-1-5-21-883232822-274137685-4173207997-1659    NULL    NULL    L
```



```
21/01/25 12:45 [~/tools/cypheroth/CIBERESTRECHO.LOCAL]
❯ cat spnDATargets.tsv | column -s $'\t' -t
Username                              DisplayName       Enabled   UnconstrainedDelegation
BBOIANI00057@CIBERESTRECHO.LOCAL      Brandie Boiani    TRUE      NULL
FTARSKI00103@CIBERESTRECHO.LOCAL      Francene Tarski   TRUE      NULL
KDESBIENS00112@CIBERESTRECHO.LOCAL    Kip Desbiens      TRUE      NULL
AMCGOWAN00159@CIBERESTRECHO.LOCAL     Ashli Mcgowan     TRUE      NULL
TOKANE00276@CIBERESTRECHO.LOCAL       Tawanna Okane     TRUE      NULL
KSTANBERY00376@CIBERESTRECHO.LOCAL    Karren Stanbery   TRUE      NULL
FLOSCO00383@CIBERESTRECHO.LOCAL       Forrest Losco     TRUE      NULL
DFILKINS00399@CIBERESTRECHO.LOCAL     Doloris Filkins   TRUE      NULL
21/01/25 12:45 [~/tools/cypheroth/CIBERESTRECHO.LOCAL]
❯
```

```
21/01/25 12:44 [~/tools/cypheroth/CIBERESTRECHO.LOCAL]
❯ cat dcsyncers.tsv | column -s $'\t' -t
user                                  ObjectType
ADMINISTRATORS@CIBERESTRECHO.LOCAL    [Group       "Base"]
AMCGOWAN00159@CIBERESTRECHO.LOCAL     [User        "Base"]
BBOIANI00057@CIBERESTRECHO.LOCAL      [User        "Base"]
BWOLLARD00067@CIBERESTRECHO.LOCAL     [User        "Base"]
CMUZYKA00346@CIBERESTRECHO.LOCAL      [User        "Base"]
DFILKINS00399@CIBERESTRECHO.LOCAL     [User        "Base"]
DOMAIN ADMINS@CIBERESTRECHO.LOCAL     [Group       "Base"]
FLLABDC@CIBERESTRECHO.LOCAL           [Computer    "Base"]
FLOSCO00383@CIBERESTRECHO.LOCAL       [User        "Base"]
FMEGA00158@CIBERESTRECHO.LOCAL        [User        "Base"]
FTARSKI00103@CIBERESTRECHO.LOCAL      [User        "Base"]
JANA00178@CIBERESTRECHO.LOCAL         [User        "Base"]
KCIANFLONE00425@CIBERESTRECHO.LOCAL   [User        "Base"]
KDESBIENS00112@CIBERESTRECHO.LOCAL    [User        "Base"]
KQUEST00108@CIBERESTRECHO.LOCAL       [User        "Base"]
KSTANBERY00376@CIBERESTRECHO.LOCAL    [User        "Base"]
LBOLUDA00465@CIBERESTRECHO.LOCAL      [User        "Base"]
LLEDEC00378@CIBERESTRECHO.LOCAL       [User        "Base"]
LZAFFALON00186@CIBERESTRECHO.LOCAL    [User        "Base"]
MLOVERICH00199@CIBERESTRECHO.LOCAL    [User        "Base"]
MROMULUS00025@CIBERESTRECHO.LOCAL     [User        "Base"]
MRUSSE00419@CIBERESTRECHO.LOCAL       [User        "Base"]
NBENGOCHIA00331@CIBERESTRECHO.LOCAL   [User        "Base"]
NROSARO00488@CIBERESTRECHO.LOCAL      [User        "Base"]
OALSTOTT00230@CIBERESTRECHO.LOCAL     [User        "Base"]
SADAMEK00408@CIBERESTRECHO.LOCAL      [User        "Base"]
TOKANE00276@CIBERESTRECHO.LOCAL       [User        "Base"]
WHORNACK00191@CIBERESTRECHO.LOCAL     [User        "Base"]
```

Extendiendo BloodHound: PlumHound

- Herramienta para Blue Teamers y Purple Teamers.
- Automatiza consultas Cypher y convierte los resultados en informes accionables.
- Generación de informes en HTML.
- Compatible con “tasklists” comunitarias.

```
(PlumHound-ofuf) 19/01/25 21:48 [~/tools/PlumHound]
❯ ls tasks
BlueHound.tasks              default-csv.tasks          EntraID-AADConnect.tasks          GPOs.tasks
broken.tasks                 default-enabledonly.tasks  EntraID-AttackPaths.tasks         hunt.tasks
Certificates.tasks           default-faster             EntraID-General.tasks             Kerberoasting.tasks
ConstrainedDelegation.tasks  default.tasks              EntraID-MSGraph.tasks             long.tasks
DCSync.tasks                 DomainUsers.tasks          EntraID-Principals-ManageID.tasks testing.tasks
(PlumHound-ofuf) 19/01/25 21:48 [~/tools/PlumHound]
❯
```

```
(PlumHound-ofuf) 21/01/25 10:13 [~/tools/PlumHound]
❯ python PlumHound.py -x tasks/default.tasks -p bloodhound

        PlumHound 1.6
        For more information: https://github.com/plumhound
        ------------------------------------
        Server: bolt://localhost:7687
        User: neo4j
        Password: *****
        Encryption: False
        Timeout: 300
        ------------------------------------
        Tasks: Task File
        TaskFile: tasks/default.tasks
        Found 119 task(s)
        ------------------------------------


on 119:         Completed Reports Archive: reports//Reports.zip
         Executing Tasks |                                        | Tasks 119 / 119  in 7.8s (14.97/s)

        Completed 119 of 119 tasks.


(PlumHound-ofuf) 21/01/25 10:14 [~/tools/PlumHound]
❯
```

```
(PlumHound-ofuf) 21/01/25 10:15 [~/tools/PlumHound]
❯ ls reports
AdminGroups.csv                                  DCSyncDirect.csv                                 Kerberoastable_Users.html                        SchemaAdmins.html
AdminGroups.html                                 DCSyncDirect.html                                LapsDeploymentCount.csv                          UserSessionsCount.html
AdminGroupsPopulatedCount.csv                    DCSyncDirectNonDAUsers.csv                       LapsDeploymentCount.html                         Users_gt006MoOldPasswords.csv
AdminGroupsPopulatedCount.html                   DCSyncDirectNonDAUsers.html                      LapsDeploymentCount-OS.csv                       Users_gt006MoOldPasswords.html
AdminsWithoutSensitiveFlag.html.csv              DCSyncDirectNonDCComputers.csv                   LapsDeploymentCount-OS.html                      Users_gt012MoOldPasswords.csv
AdminsWithoutSensitiveFlag.html.html             DCSyncDirectNonDCComputers.html                  LAPSNotEnabled.html                              Users_gt012MoOldPasswords.html
CertificateAuthorties.csv                        DomainAdmins.html                                LocalAdmin_Computers_.csv                        Users_gt060MoOldPasswords.csv
CertificateAuthorties.html                       DomainComputers.csv                              LocalAdmin_Computers_.html                       Users_gt060MoOldPasswords.html
CertificateTemplateEnrollRights.csv              DomainComputers.html                             LocalAdmin_Groups_Count.html                     Users_gt120MoOldPasswords.csv
CertificateTemplateEnrollRights.html             DomainControllers.csv                            LocalAdmin_Groups.html                           Users_gt120MoOldPasswords.html
CertificateTemplates.csv                         DomainControllers.html                           LocalAdmins_Computers_count.html                 Users_gt180MoOldPasswords.csv
CertificateTemplates_ESC1.csv                    DomainControllers_ReadOnly.csv                   LocalAdmin_UsersCount.html                       Users_gt180MoOldPasswords.html
CertificateTemplates_ESC1.html                   DomainControllers_ReadOnly.html                  LocalAdmin_Users.html                            Users_gt240MoOldPasswords.csv
CertificateTemplates_ESC2.csv                    DomainGroups.csv                                 OS_Count.csv                                     Users_gt240MoOldPasswords.html
CertificateTemplates_ESC2.html                   DomainGroups.html                                OS_Count.html                                    Users_le01DOldPasswords.csv
CertificateTemplates_ESC3.csv                    Domains.csv                                      OS_Unsupported_Count.csv                         Users_le01DOldPasswords.html
CertificateTemplates_ESC3.html                   Domains.html                                     OS_Unsupported_Count.html                        Users_lt07DOldPasswords.csv
CertificateTemplates_ESC6.csv                    DomainTrusts.csv                                 OS_Unsupported.csv                               Users_lt07DOldPasswords.html
CertificateTemplates_ESC6.html                   DomainTrusts.html                                OS_Unsupported.html                              Users_lt30DOldPasswords.csv
CertificateTemplates_ESC8.csv                    DomainUsers.csv                                  OUs_ComputerCount.html                           Users_lt30DOldPasswords.html
CertificateTemplates_ESC8.html                   DomainUsers.html                                 OUs_GroupCount.html                              Users_NeverActive_Enabled.csv
CertificateTemplates.html                        EA_Sessions.html                                 OUs_UserCount.html                               Users_NeverActive_Enabled.html
CertPublishers.html                              EnterpriseAdmins.html                            Owned-Computers-Groups-DirectDistinct.html       Users_NeverExpirePasswords.csv
Computers_LocalAdminEnumeration.csv              GMSA_CanReadPassword.csv                         Owned-Computers-Groups.html                      Users_NeverExpirePasswords.html
Computers_LocalAdminEnumeration.html             GMSA_CanReadPassword.html                        Owned-Computers.html                             Users_NoKerbReq.csv
Computers_MSSQL.csv                              GPOCreatorOwners.html                            Owned-Groups.html                                Users_NoKerbReq.html
Computers_MSSQL.html                             GPO_OU_Links.csv                                 Owned-Objects-AdminTo-Direct.html                UsersnonadminAddMemberGroups.csv
Computers_UnconstrainedDelegation.csv            GPO_OU_Links.html                                Owned-Objects-GMSARead-Direct.html               UsersnonadminAddMemberGroups.html
Computers_UnconstrainedDelegation.html           GPOOwners-Detail.csv                             Owned-Objects.html                               UsersNotActive120mo.csv
Computers_UnconstrainedDelegationNonDC.csv       GPOOwners-Detail.html                            Owned-Objects-MemberOf-Direct.html               UsersNotActive120mo.html
Computers_UnconstrainedDelegationNonDC.html      GPOOwners-NonDA.csv                              Owned-Users-Groups-DirectDistinct.html           UsersNotActive12mo.csv
Computers_WithDescriptions.csv                   GPOOwners-NonDA.html                             Owned-Users-Groups.html                          UsersNotActive12mo.html
Computers_WithDescriptions.html                  GPOOwners-Summary.csv                            Owned-Users.html                                 UsersNotActive60mo.csv
ConstrainedDelegation-All.csv                    GPOOwners-Summary.html                           PreWindows2000.html.csv                          UsersNotActive60mo.html
ConstrainedDelegation-All.html                   GPOs.csv                                         PreWindows2000.html.html                         UsersNotActive6mo.csv
ConstrainedDelegation-ComputersNonDC.csv         GPOs.html                                        ProtectedUsers.html                              UsersNotActive6mo.html
ConstrainedDelegation-ComputersNonDC.html        GPOs-NonDA-WithInterestingPermissions.csv        RDPableGroupsCount.html                          Users_PasswordNotRequired.html
ConstrainedDelegation-Users.csv                  GPOs-NonDA-WithInterestingPermissions.html       RDPableGroups.html                               Users_PasswordNotRequiredNeverSet.html
ConstrainedDelegation-Users.html                 Groups_CanResetPasswordsCount.html               Relationships-AuthenticatedUsers.html            Users_Sessions_Count.html
ConstrainedDelegation-UsersNonDA.csv             Groups-HighValue-members.csv                     Relationships-DomainComputers.html               Users_Sessions.csv
ConstrainedDelegation-UsersNonDA.html            Groups-HighValue-members.html                    Relationships-DomainUsers.html                   Users_Sessions.html
DA_Sessions.html                                 HuntComputersWithPassInDescription.html          Relationships-Everyone.html                      Users_UnconstrainedDelegation.csv
DCOwners.csv                                     HuntUsersWithChangeInDescription.html            Relationships-Guests.html                        Users_UnconstrainedDelegation.html
DCOwners.html                                    HuntUsersWithPassInDescription.html              Relationships-PreW2KCA.html                      Users_userpassword.csv
DCOwners-Users.csv                               HuntUsersWithVPNGroup.html                       Relationships-Users.html                         Users_userpassword.html
DCOwners-Users.html                              index.html                                       Reports.zip                                      Workstations_RDP.html
(PlumHound-ofuf) 21/01/25 10:16 [~/tools/PlumHound]
❯
```

Full Report Details

Report Date: 2025-01-21

Total Rows: 115
Filtered Rows: 115

Title	Count	Further Details
Domains	1	Details - CSV
Domain Trusts	0	Details - CSV
Domain Controllers	1	Details - CSV
Domain Controllers - Read Only	0	Details - CSV
Enterprise Admins (Direct)	0	Details
Schema Admins (Direct)	0	Details
Domain Admins (Direct)	25	Details
Admin Groups	3	Details - CSV
Admin Groups Direct Population	1	Details - CSV
Domain User Accounts	501	Details - CSV
Domain Computer Accounts	501	Details - CSV
Domain Groups	0	Details - CSV
OUs By Computer Member Count	1	Details
OUs By User Member Count	1	Details
OUs By Group Member Count	0	Details
Cert Publishers (Direct)	0	Details
DA Sessions	33	Details
EA Sessions	0	Details
User Sessions Count	0	Details
HighValue Group Members (Direct) (Limited to 1000)	25	Details - CSV
Protected Users Group (Direct)	0	Details
Admins Without Sensitive Protection Flag	0	Details - CSV
Kerberoastable Users	17	Details
Pre-Windows 2000 Compatibility Access Direct Members	0	Details - CSV
RDPable Servers	0	Details
Domain Controller Owners	0	Details - CSV
Domain Controller Owned by Users	0	Details - CSV
Unconstrained Delegation Users with SPN	0	Details - CSV
Unconstrained Delegation Computers with SPN	0	Details - CSV
Unconstrained Delegation Computers with SPN Non-DC	0	Details - CSV

Operating Systems Unsupported

Report Date: 2025-01-21 10:15:29

Total Rows: 350
Filtered Rows: 350

Computer	UnsupportedOS	Enabled	PWDLastSet	LastLogonTimeStamp
COMP00002.CIBERESTRECHO.LOCAL	Windows Server 2003	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00007.CIBERESTRECHO.LOCAL	Windows 7	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00010.CIBERESTRECHO.LOCAL	Windows 7	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00012.CIBERESTRECHO.LOCAL	Windows Server 2012	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00013.CIBERESTRECHO.LOCAL	Windows 7	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00014.CIBERESTRECHO.LOCAL	Windows 7	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00015.CIBERESTRECHO.LOCAL	Windows Server 2012	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00016.CIBERESTRECHO.LOCAL	Windows Server 2008	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00017.CIBERESTRECHO.LOCAL	Windows Server 2008	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00018.CIBERESTRECHO.LOCAL	Windows Server 2008	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00019.CIBERESTRECHO.LOCAL	Windows Server 2008	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00020.CIBERESTRECHO.LOCAL	Windows 7	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00021.CIBERESTRECHO.LOCAL	Windows Server 2008	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00022.CIBERESTRECHO.LOCAL	Windows Server 2008	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00025.CIBERESTRECHO.LOCAL	Windows 7	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00026.CIBERESTRECHO.LOCAL	Windows 7	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00027.CIBERESTRECHO.LOCAL	Windows Server 2012	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00028.CIBERESTRECHO.LOCAL	Windows 7	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00029.CIBERESTRECHO.LOCAL	Windows 7	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z
COMP00030.CIBERESTRECHO.LOCAL	Windows 7	True	1970-01-01T00:00:00Z	1970-01-01T00:00:00Z

COMP00500.CIBERESTRECHO.LOCAL	Windows 7	True

Cypher Query:

```
MATCH (c:Computer) WHERE c.operatingsystem =~ '.*(2000|2003|2008|2012|xp|vista|7|me).*' RETURN c.name as Computer, c.operatingsystem
as UnsupportedOS, c.enabled as Enabled, toString(datetime({epochSeconds: ToInteger(coalesce(c.pwdlastset,0))})) as PWDLastSet,
toString(datetime({epochSeconds: ToInteger(coalesce(c.lastlogontimestamp,0))})) as LastLogonTimeStamp
```

Report Title: Operating Systems Unsupported
Report Date: 2025-01-21 10:15:29
Produced by PlumHound
Special thanks to Defensive Origins and Black Hills Information Security

2020 – Modelo de Acceso Empresarial

- El modelo de administración por niveles se centraba en contener una escalada de privilegios no autorizada en entornos on-premises.

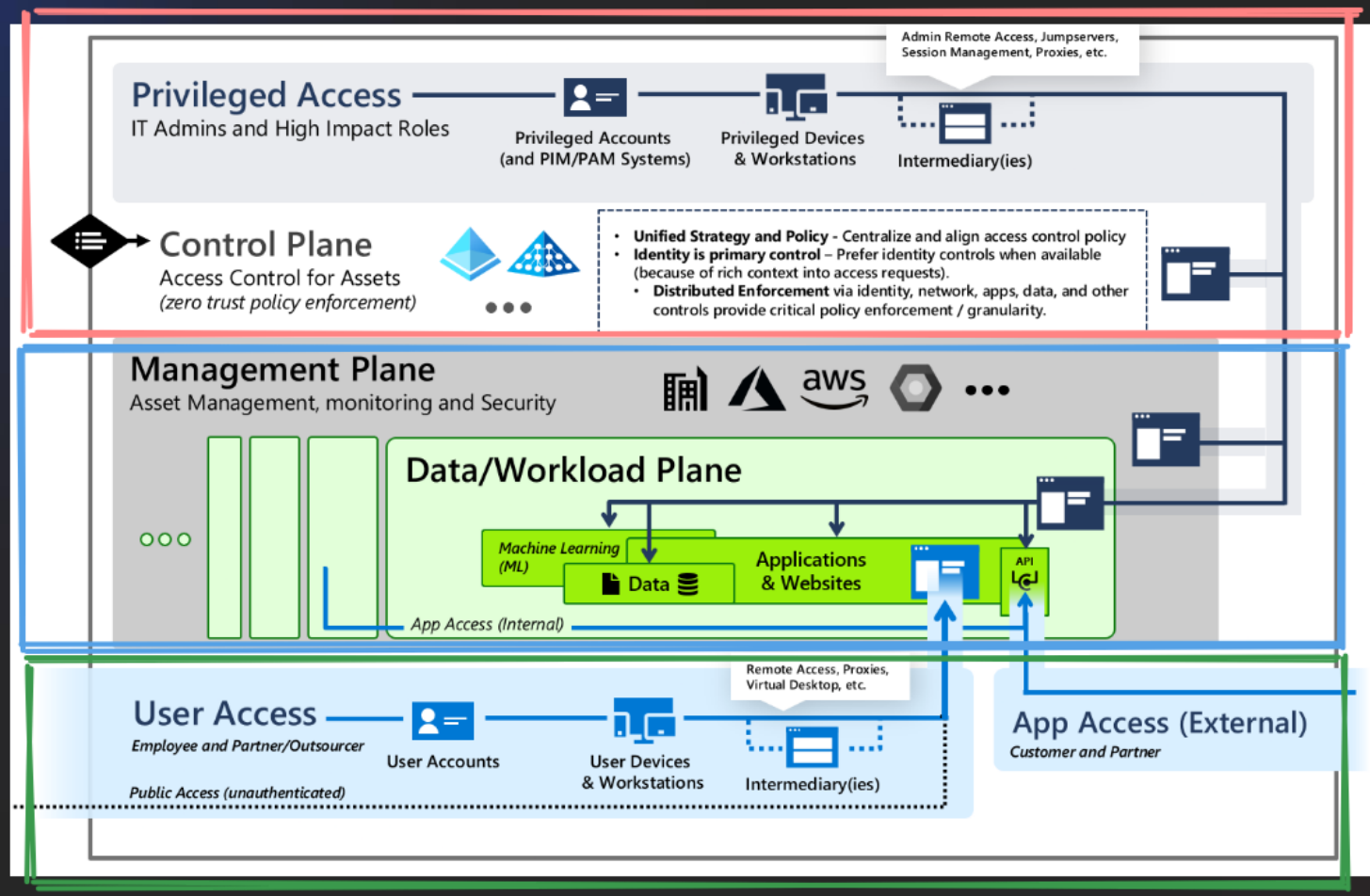
- El modelo empresarial incorpora todo esto además de:
  - Gestión de accesos en entornos híbridos.
  - Uso de múltiples nubes.
  - Aplicación de políticas de acceso condicional.

- En resumen: se adapta a la actualidad y la implementación de la nube.

Tier 0

Tier 1

Tier 2



Privileged Access

Enables IT administrators and other high impact roles to access to sensitive systems and data. *Stronger security for higher impact accounts*

Control and Management Planes

Provide unified access and management for workloads and assets *(and provide attackers shortcut for illicit objectives)*

Data/Workloads

Create and store business value in

- Business processes (in apps/workloads)
- Intellectual property (in data and apps)

User and App Access

How employees, partners, and customers access these resources

Para finalizar: ~~Ataques~~ Fallos Comunes

~~Extrae la contraseña de un administrador local y comprueba si se reutiliza en otros administradores locales de otros equipos~~ 😈

Haz uso de LAPS para asegurar que la contraseña de cada administrador local es única e impredecible 😋

~~Extrae la parte cifrada de los TGS para intentar crackear la contraseña de la cuenta que ejecuta el servicio~~ 😈

Haz uso de gMSA para asegurar que la contraseña de cada usuario de servicio es única e impredecible 😋

~~Lee los atributos de los usuarios (o de los equipos) para ver si hay alguna contraseña expuesta, sobre todo en el campo descripción~~ 😈

Nunca coloques información sensible en ningún campo de LDAP 😋

~~Comprueba la política de contraseñas para ver cuantos intentos tienes para probar contraseñas en usuarios, a veces se configura sin límite~~ 😈

Configura la política de contraseñas para establecer un limite de intentos y contraseñas robustas 😋

~~Comprueba a que recursos compartidos puedes acceder, muchas veces los usuarios de dominio sin privilegios pueden acceder a recursos que no deberían~~ 😈

Revisa los permisos de los recursos compartidos de todos los equipos 😋

Y por último, pero no menos importante

~~No apliques nada de lo aprendido en este charla, no soluciones los fallos de configuración, no revises las políticas, no mires los permisos y sobre todo no apliques actualizaciones ni parches~~ 😟

Aplica todo lo que acabamos de ver 😋

END OF PRESENTATION

ANY QUESTION ?

PLEASE NO

https://github.com/sikumy/talks

Referencias

- What is Tier Zero, Part 1 – SpecterOps
- Credential Tiering, an overview – SCIP
- The Fundamentals of AD tiering – itm8
- Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft – Microsoft
- BloodHound Unleashed