SEC Consult

an Eviden business

Historically Grown Active Directory Environments

You have dead bodies in your basement and you don´t know about it

Michael Ritter
Principal Security Consultant
DEATHCon 2023

1.0 | 04/11/2023

SEC Consult

an Eviden business

01
About me

02
The tale of “DEATH Enterprises”

03
Evolution of AD attacks and security controls

04
The dead bodies in the basement

05
Classic challenges for admins

06
Conclusion

SEC Consult

an Eviden business

01 About me

01 | About me

Michael Ritter

- Principal Security Consultant at SEC Consult
- Working in the IT field since 2005
- In offensive security for 9+ years as a consultant
- Focus on Topics:
  - AD related security assessments
  - AD security workshops
  - Post-compromise taskforce

Disclaimer: Not a full-time detection engineer

GitHub michiiii

@BigM1ke_oNe

SEC Consult
an Eviden business

02 The tale of “DEATH Enterprises”

02 | AD from a historical view

The tale of “DEATH Enterprises” – early 2000´s

- Jimmy “The skid” Johnson is the IT magician of a little start-up called “DEATH Enterprises” in the early 2000´s tech boom
- Jimmy heard about a Microsoft product that simplifies management of IT resources.
- Jimmy decided to deploy Active Directory into the IT infrastructure of “DEATH Enterprises”

02/2000
Microsoft releases Active Directory with the release of Windows 2000 server

2000 2002 2004 2006 2008 2010 2012 2014 2016 2018 2020 2022 2024

02 | AD from a historical view

The tale of “DEATH Enterprises” – early 2000´s

- In 2002, Jimmy integrated Active Directory into the company's infrastructure, navigating a landscape with limited established best practices.
- The setup was basic: each user had one account, local admin accounts had static passwords, and third-party services ran under the default "Administrator" domain.
- Jimmy, as the sole IT professional, juggled the complexities of managing the Active Directory while also handling helpdesk responsibilities.
- To simplify his workload, Jimmy delegated some of his administrative tasks to his colleagues

02/2000
Microsoft releases Active Directory with the release of Windows 2000 server

2000 | 2002 | 2004 | 2006 | 2008 | 2010 | 2012 | 2014 | 2016 | 2018 | 2020 | 2022 | 2024

08/2002
Jimmy deployed ADDS into “DEATH Enterprises” IT infrastructure

02 | AD from a historical view

The tale of “DEATH Enterprises” – The first big AD security incident

- A bad guy infected one workstation of an employee with malware
- The employee called Jimmy and told him his computer behaved weird
- Jimmy connected to the workstation via RDP and therefore left his credentials on the attacker controlled workstation.
- The attacker got Jimmy´s credentials and moved laterally to steal important research data

Result of the incident: Important research data was stolen and published.

02/2000
Microsoft releases Active Directory with the release of Windows 2000 server

2000 | 2002 | 2004 | 2006 | 2008 | 2010 | 2012 | 2014 | 2016 | 2018 | 2020 | 2022 | 2024

08/2002
Jimmy deployed ADDS into “DEATH Enterprises” IT infrastructure

03/2015
“DEATH Enterprises” first security incident.

02 | AD from a historical view

The tale of “DEATH Enterprises” – Secure Active Directory v1

- The research data that was published was useful for the competitors and put “DEATH Enterprises” into a tough time
- As consequence of the incident “DEATH Enterprises” management decided to:
  - Dramatic increase of budget for IT security
  - Active Directory security became a key topic

02/2000
Microsoft releases Active Directory with the release of Windows 2000 server

08/2015
“DEATH Enterprises” established Secure Active Directory v1

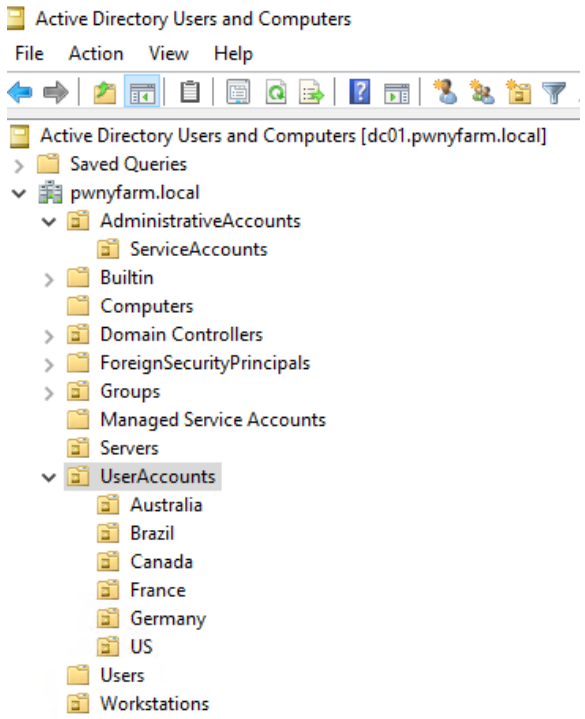
2000 2002 2004 2006 2008 2010 2012 2014 2016 2018 2020 2022 2024

08/2002
Jimmy deployed ADDS into “DEATH Enterprises” IT infrastructure

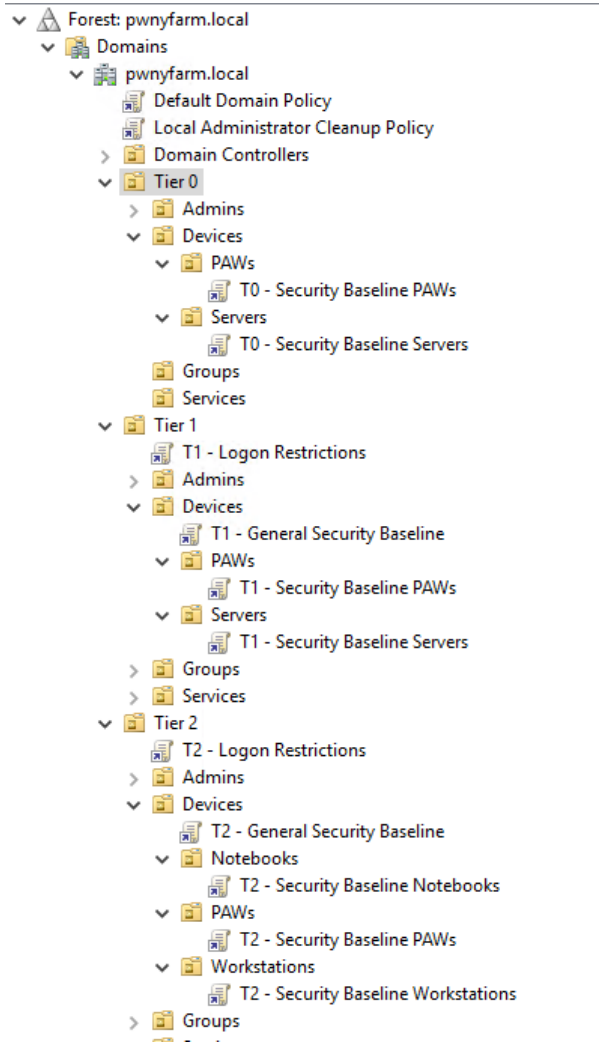
03/2015
“DEATH Enterprises” first security incident.

02 | AD from a historical view

The tale of “DEATH Enterprises” – Secure Active Directory v1 – 08/2015

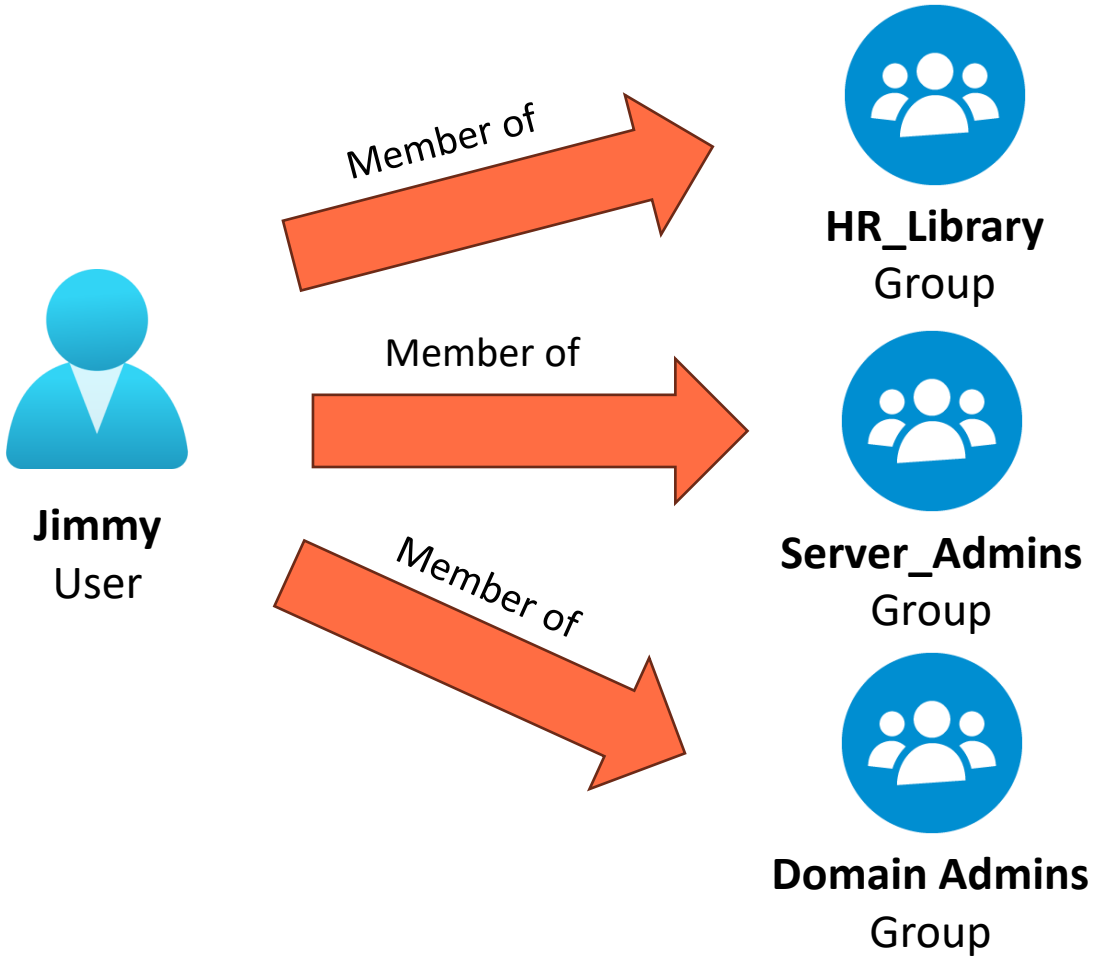


Transformation



02 | AD from a historical view

The tale of “DEATH Enterprises” – Secure Active Directory v1 – 08/2015

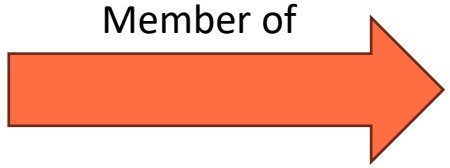


02 | AD from a historical view

The tale of “DEATH Enterprises” – Secure Active Directory v1 – 08/2015

Jimmy
T2 User

Member of

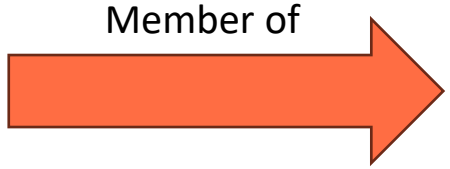


HR_Library
Group

Domain Admins
Group

T1_Jimmy_ADM
T1 Admin user

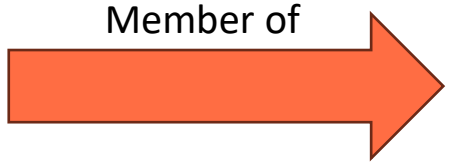
Member of



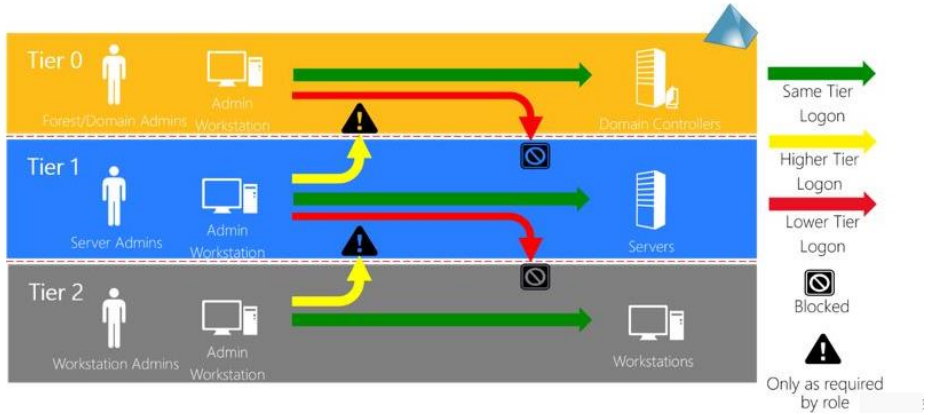
Server_Admins
Group

T2_Jimmy_ADM
T2 Admin user

Member of



Helpdesk_Admins
Group



02 | AD from a historical view

The tale of “DEATH Enterprises” – Secure Active Directory v1 – 08/2015

- As part of the implementation of the the Admin Tiering concept
  - Privileged access workstations PAW´s were introduced
  - Logon restriction were technically implemented

- Solution for the management of local administrators
  - LAPS was introduced to manage secrets of local administrative accounts
  - A GPO for the cleanup of local users and groups on all assets was implemented

- Helpdesk concept
  - User helpdesk was done with a remote support software that does not leave credentials

- External security firm was hired to conduct a security assessment which confirmed an overall good security posture

02 | AD from a historical view

The tale of “DEATH Enterprises” – Conclusion

- Take this story as an example how an Active Directory environment could have transformed during it´s lifecycle
  - Over its lifecycle within an organization, an Active Directory environment can undergo multiple transformations, reflecting changes in technology, organizational structure, security practices, and administrative philosophies.

SEC Consult

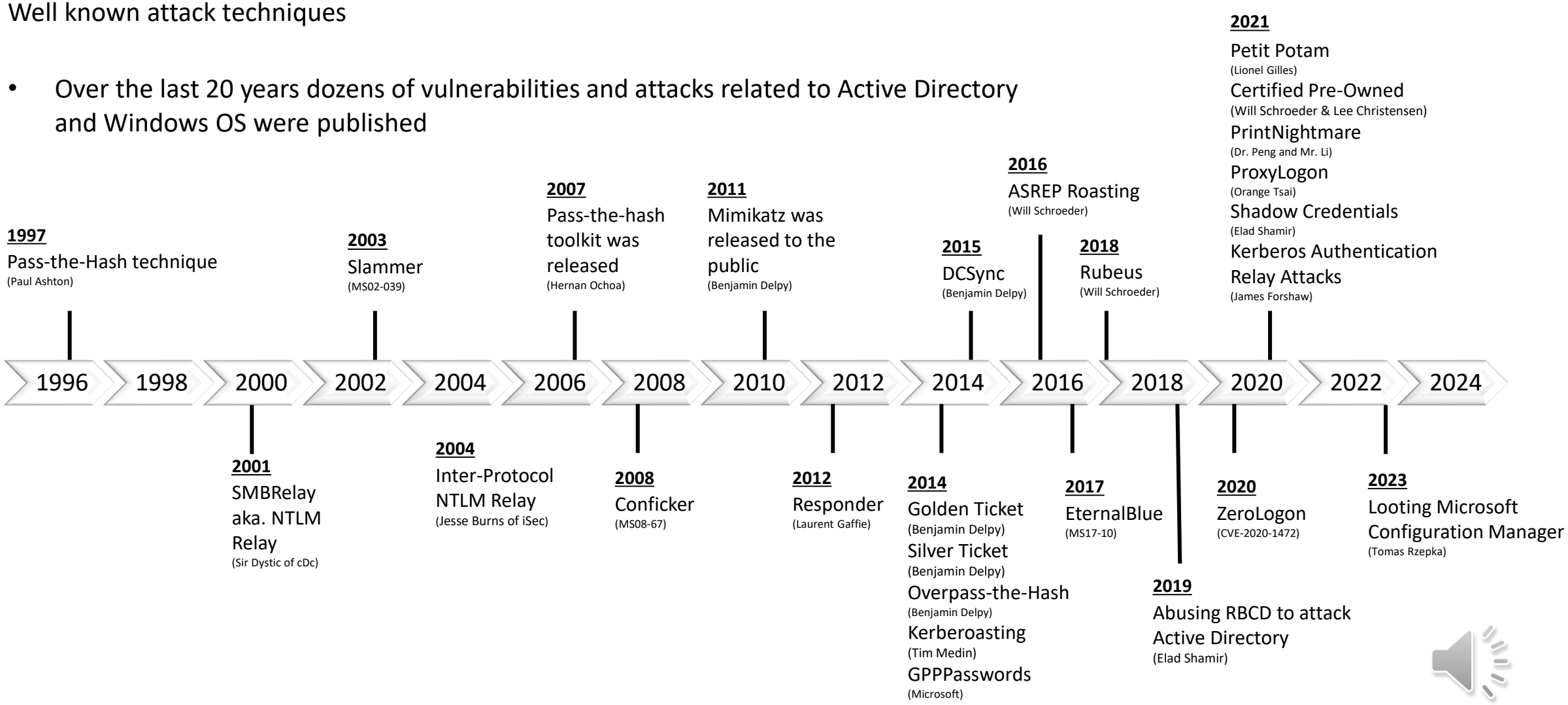
an Eviden business

03 Evolution of AD attacks and security controls

03 | Evolution of AD attacks and security controls

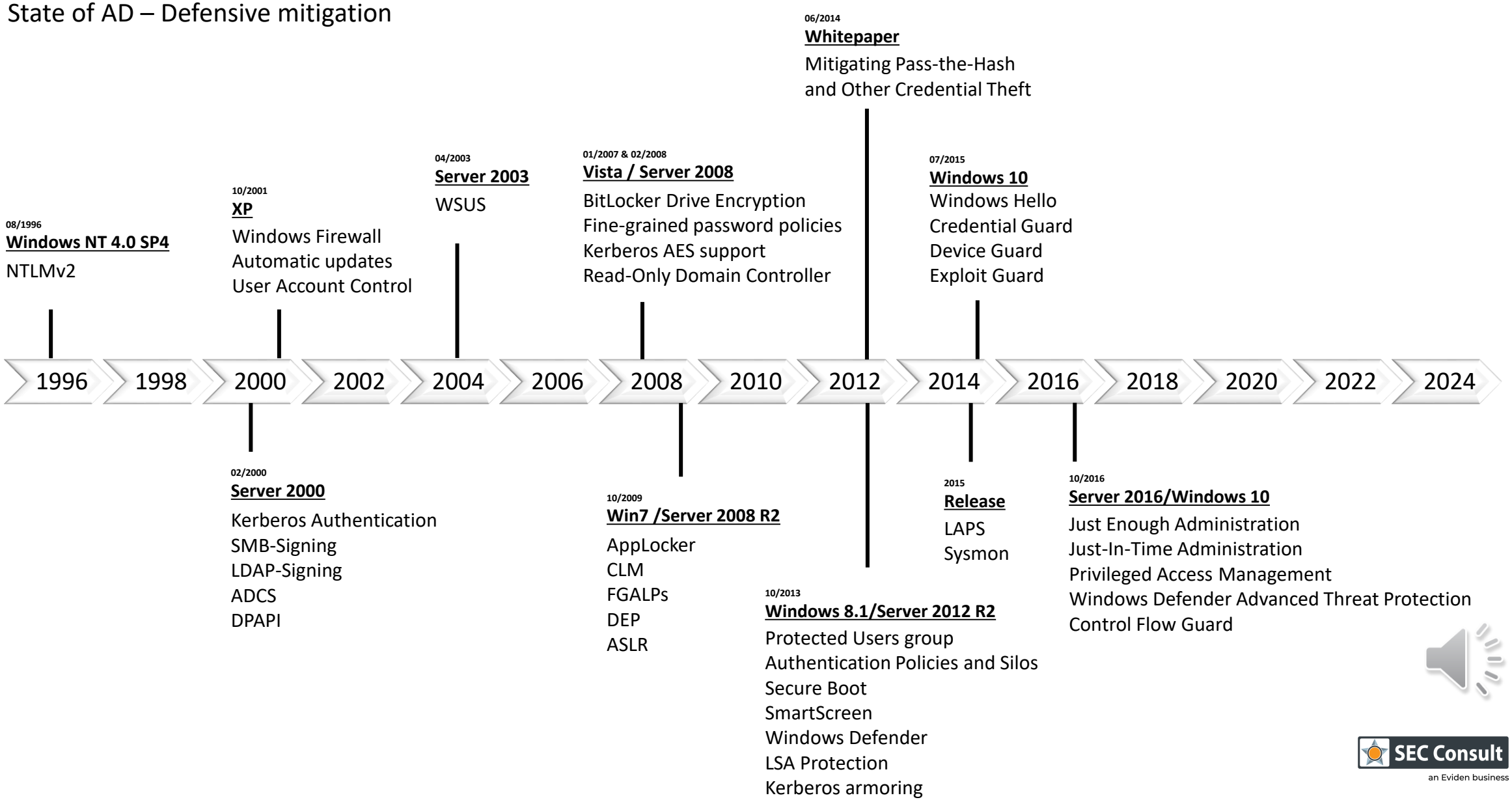
Well known attack techniques

- Over the last 20 years dozens of vulnerabilities and attacks related to Active Directory and Windows OS were published



03 | Evolution of AD attacks and security controls

State of AD – Defensive mitigation



SEC Consult
an Eviden business

4 The dead bodies in the basement

04 | The dead bodies in the basement

AD Object permissions – What happened?

- Over the last 20 years Jimmy and his IT colleagues created many:

User objects

Group objects

OU´s objects

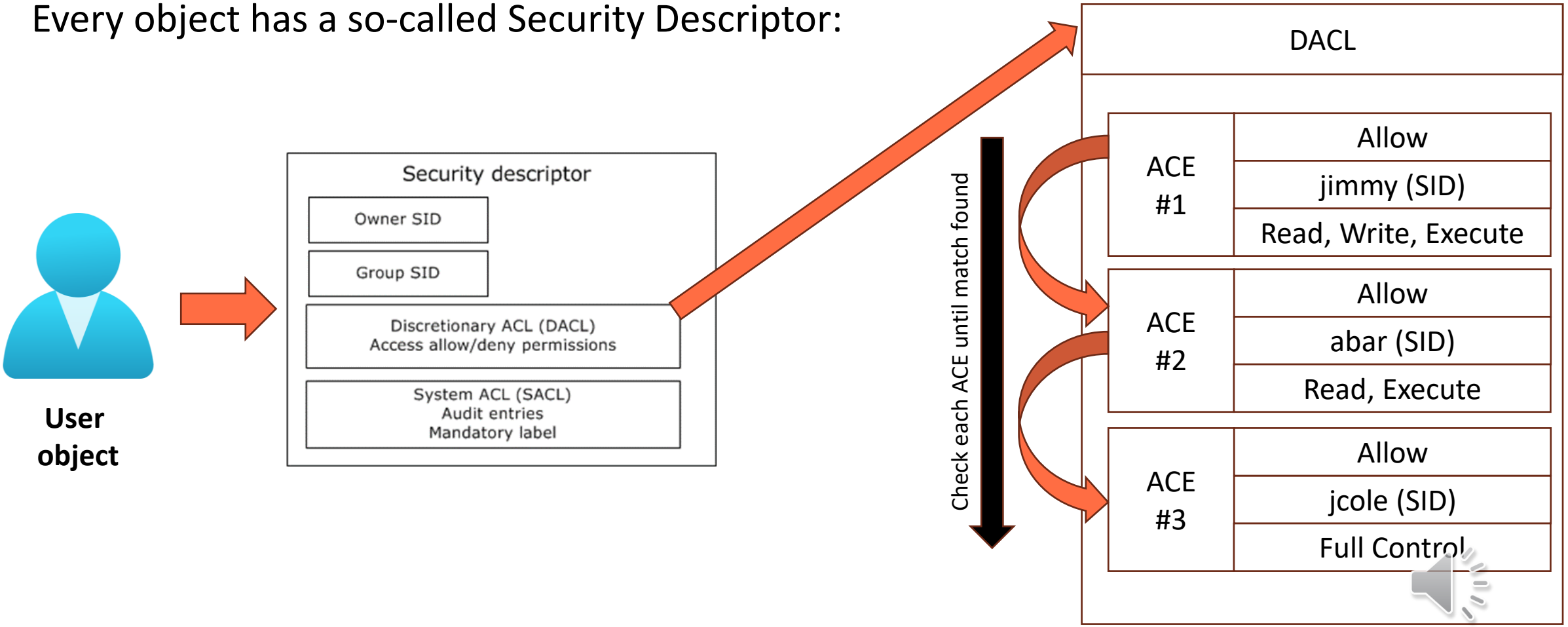
GPO objects

There are more object types in Active Directory… but let´s keep it simple

04 | The dead bodies in the basement

AD Object permissions – Security descriptors

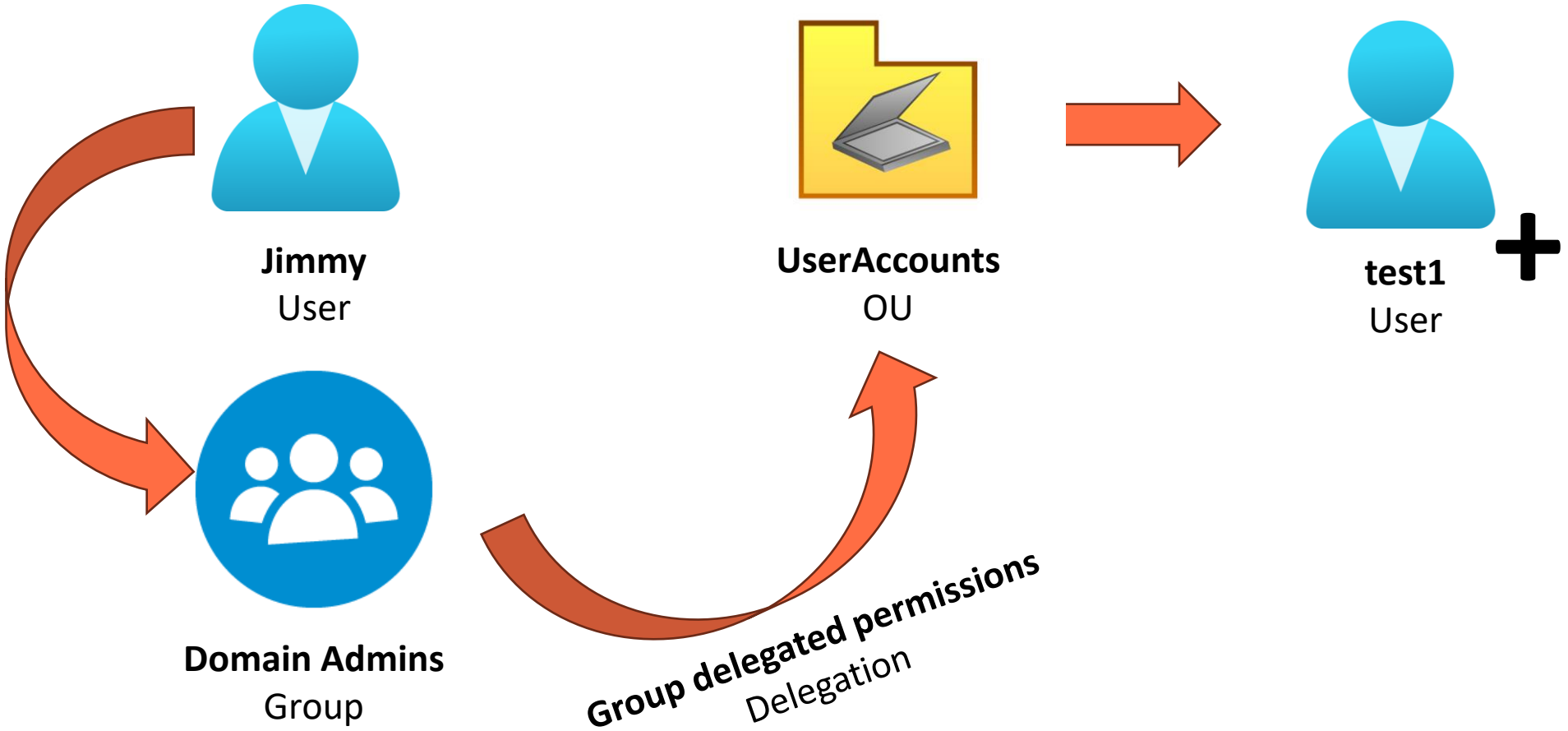
- Every object has a so-called Security Descriptor:



04 | The dead bodies in the basement

AD object permissions – What happens if you create an AD object

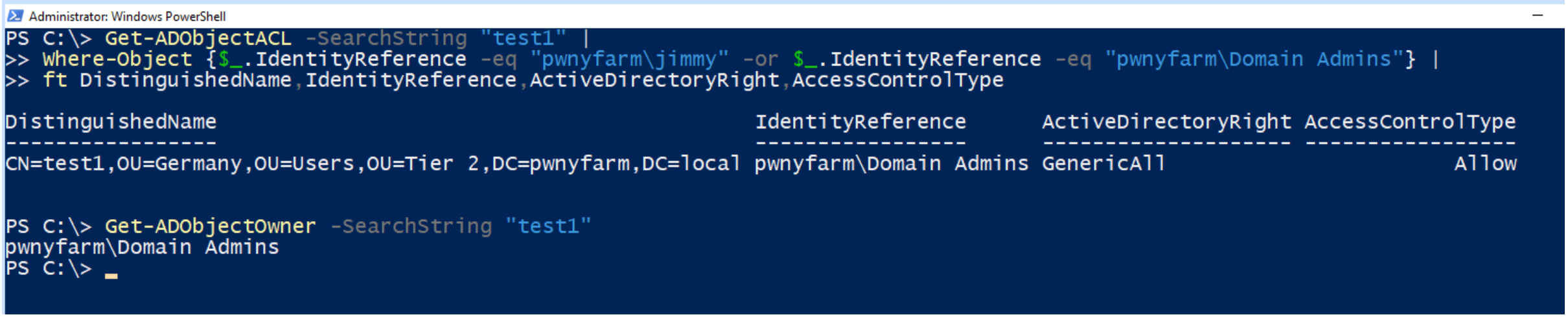
- Situation 1: Creating a AD object as Domain Administrator
  - User creation



04 | The dead bodies in the basement

AD object permissions – What happens if you create an AD object

- Situation 1: Creating a AD object as Domain Administrator
  - User creation



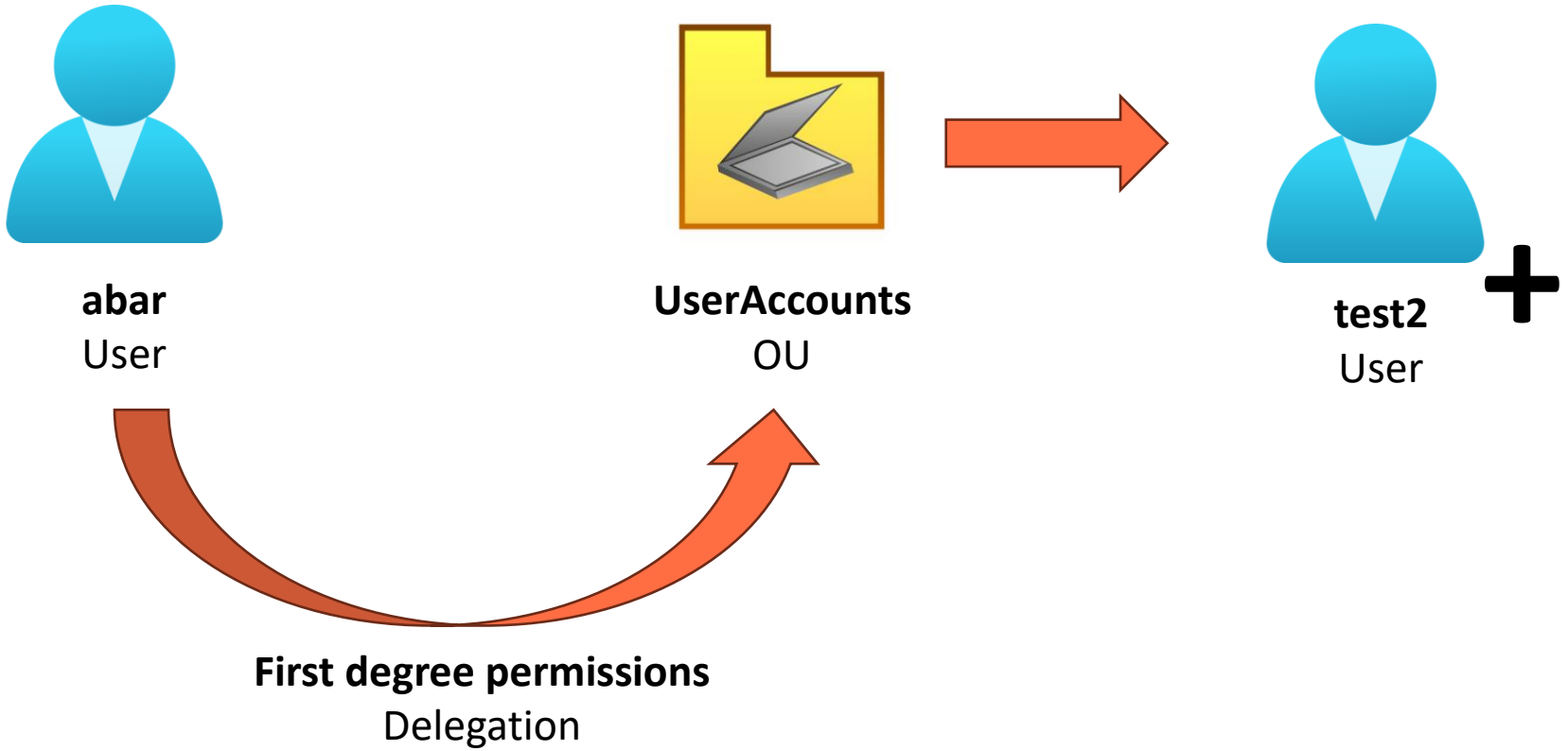
Object Owner:
- Domain Admins

ACL:
- No first degree permission for Jimmy
- Group delegated object control due to inheritance
  - Group membership of Domain Admins

04 | The dead bodies in the basement

AD object permissions – What happens if you create an AD object

- Situation 2: Creating a AD object as delegated user
  - User creation



04 | The dead bodies in the basement

AD object permissions – What happens if you create an AD object

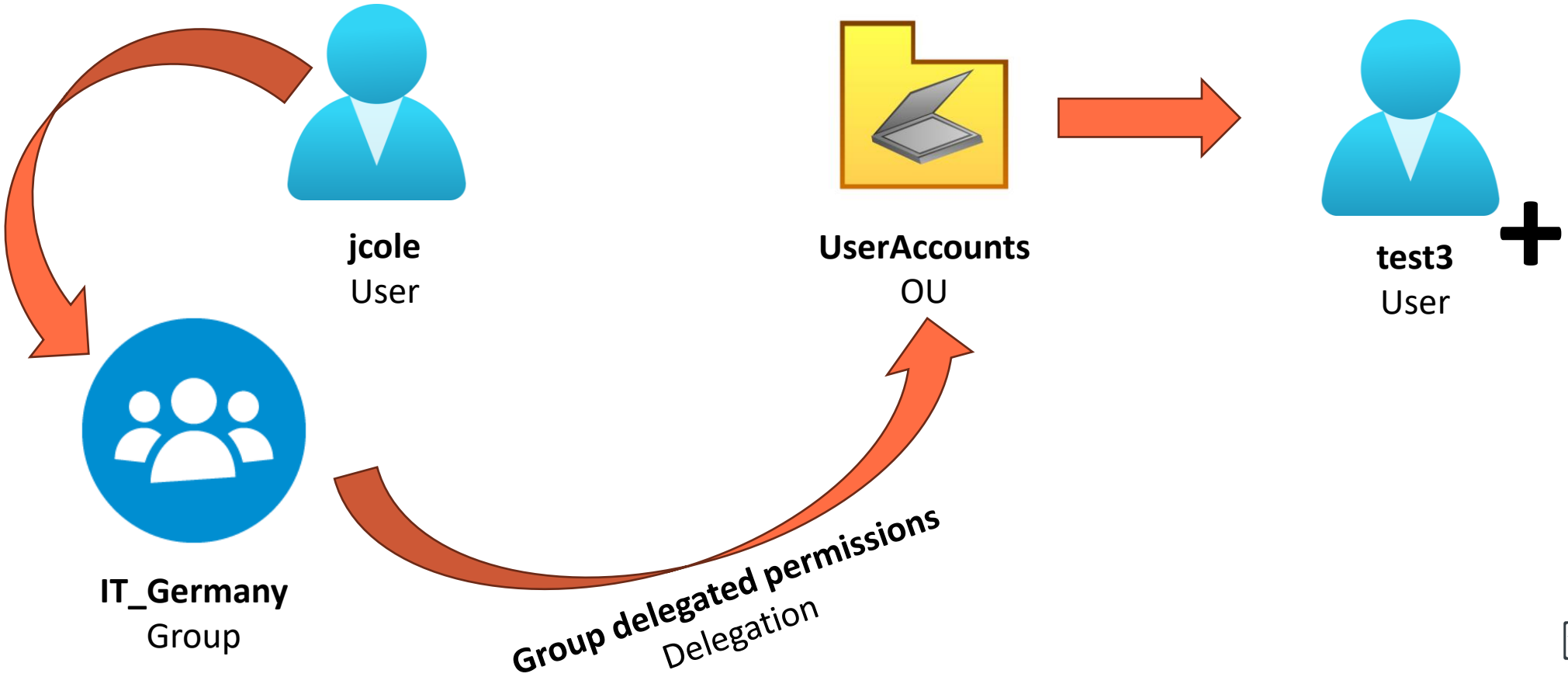
- Situation 2: Creating a AD object as delegated user
  - User creation

Object Owner
- abar

ACL
- First degree permission for abar

AD object permissions – What happens if you create an AD object

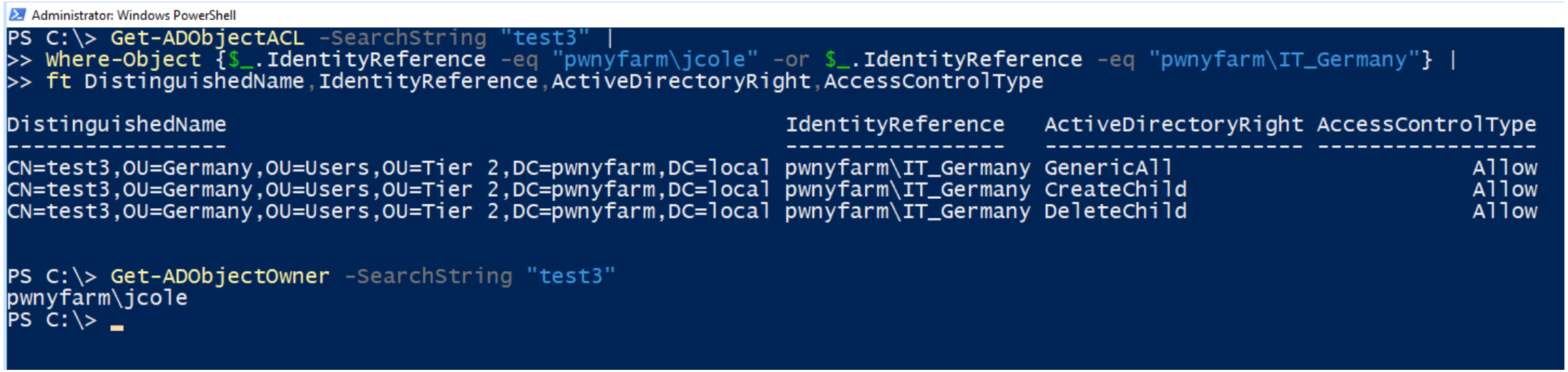
- Situation 3: Creating a AD object as group delegated user
  - User creation



04 | The dead bodies in the basement

AD object permissions – What happens if you create an AD object

- Situation 3: Creating a AD object as group delegated user
  - User creation



Object Owner
- jcole

ACL
- No first degree permission for jcole
- Group delegated object control due to inheritance

04 | The dead bodies in the basement

AD object permissions – What happens if you create an AD object – Conclusion of the results

- Results for the object owner in Situation 1 and 3 should be the same but they are not:
  - Situation 1: The delegated group is the object owner
  - Situation 2: The user that is member of the group delegated is the object owner
- The result in Situation 2: In general it is bad practice to give first degree object permissions directly to a user… but it happens

Question:

- Why could this be a problem in historically grown AD environments?

04 | The dead bodies in the basement

AD object permissions – What happens if you create an AD object – Conclusion of the results

Active Directory Users and Computers

File Action View Help

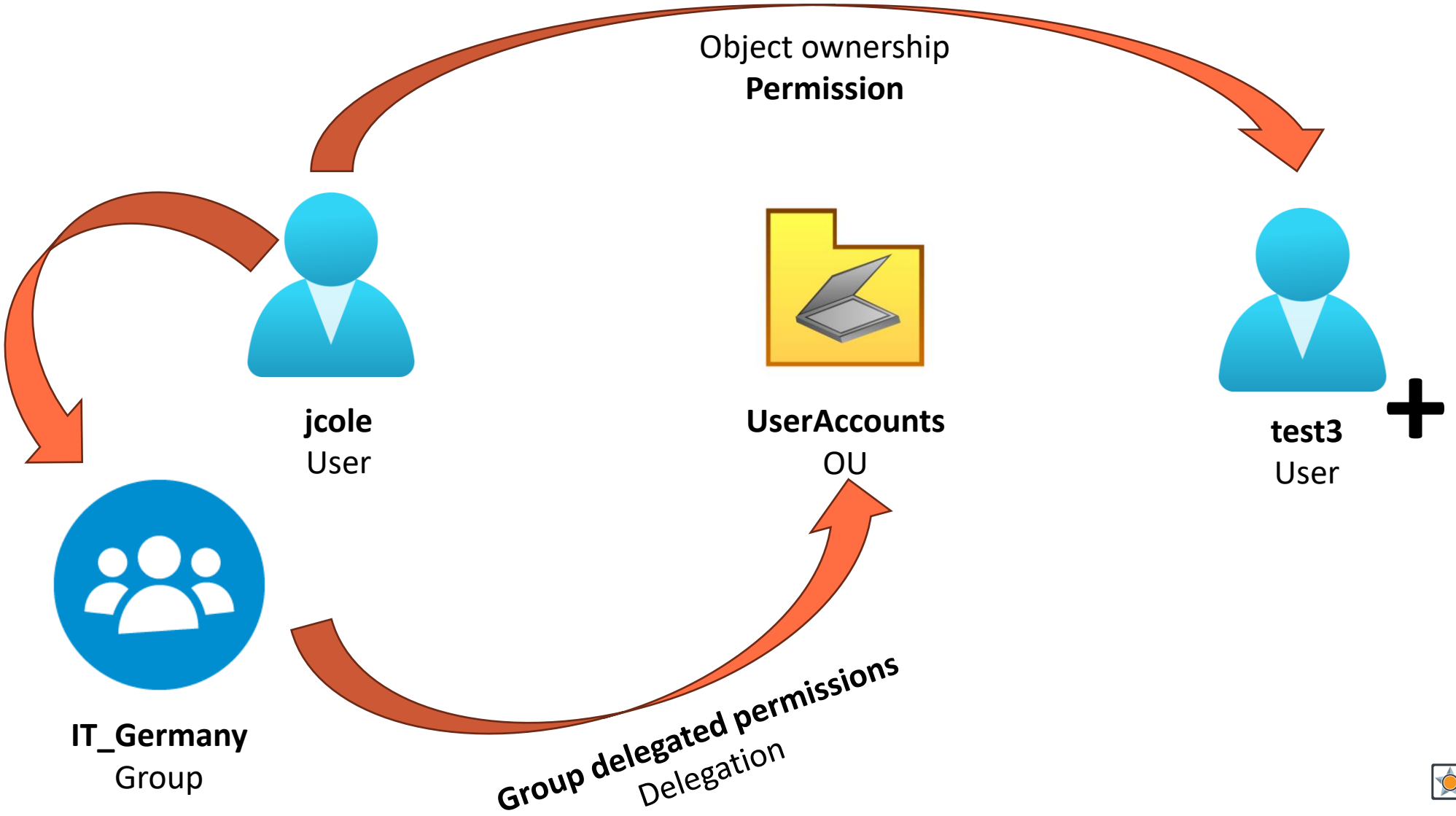
- Active Directory Users and Computers [dc01.pwnyfarm.local]
  - Saved Queries
  - pwnyfarm.local
    - AdministrativeAccounts
      - ServiceAccounts
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Groups
    - Managed Service Accounts
    - Servers
    - UserAccounts
      - Australia
      - Brazil
      - Canada
      - France
      - Germany
      - US
    - Users
    - Workstations

Transformation

- Forest: pwnyfarm.local
  - Domains
    - pwnyfarm.local
      - Default Domain Policy
      - Local Administrator Cleanup Policy
      - Domain Controllers
      - Tier 0
        - Admins
        - Devices
          - PAWs
            - T0 - Security Baseline PAWs
          - Servers
            - T0 - Security Baseline Servers
        - Groups
        - Services
      - Tier 1
        - T1 - Logon Restrictions
        - Admins
        - Devices
          - T1 - General Security Baseline
          - PAWs
            - T1 - Security Baseline PAWs
          - Servers
            - T1 - Security Baseline Servers
        - Groups
        - Services
      - Tier 2
        - T2 - Logon Restrictions
        - Admins
        - Devices
          - T2 - General Security Baseline
          - Notebooks
            - T2 - Security Baseline Notebooks
          - PAWs
            - T2 - Security Baseline PAWs
          - Workstations
            - T2 - Security Baseline Workstations
        - Groups

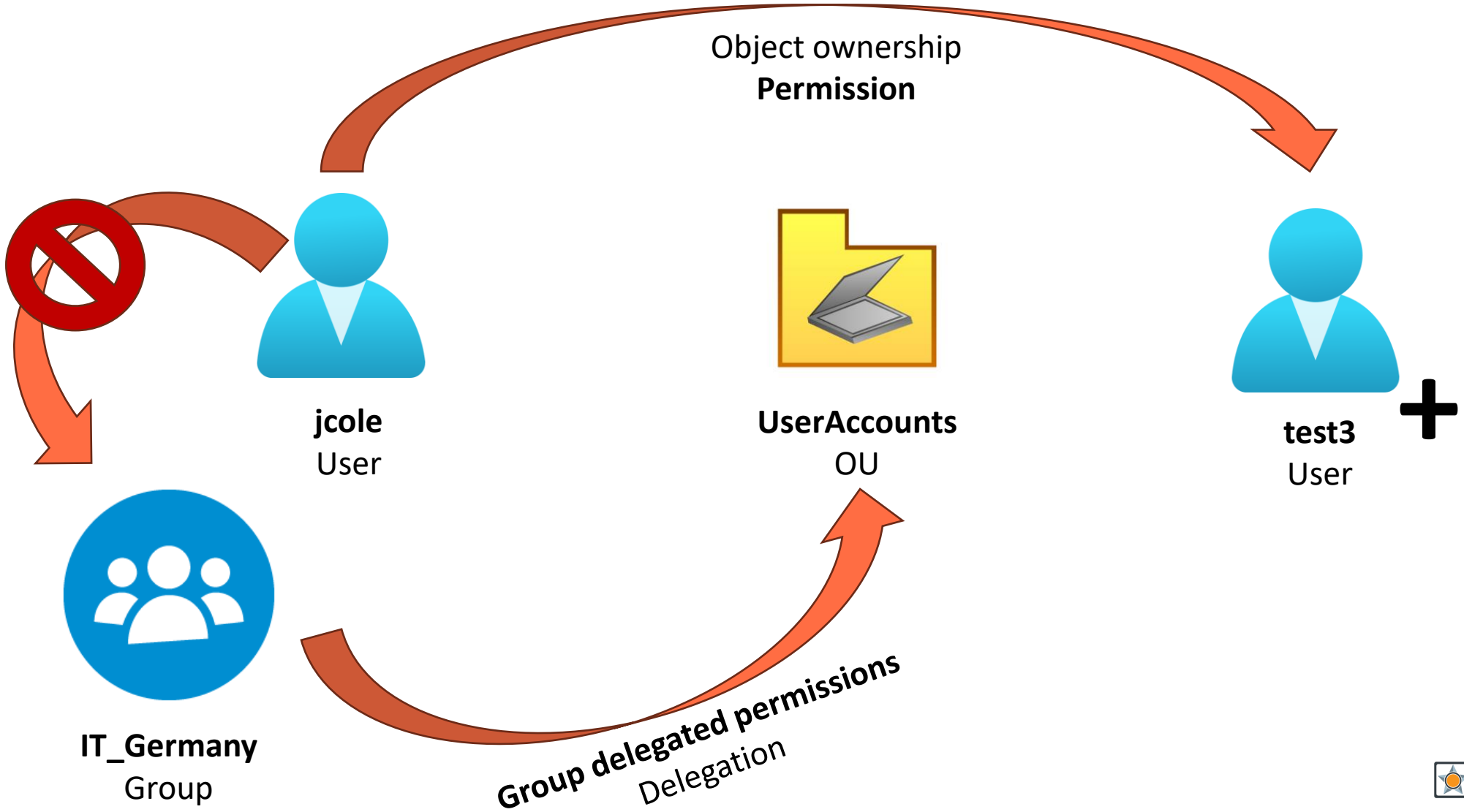
04 | The dead bodies in the basement

AD object permissions – What happens if you create an AD object – Conclusion of the results



04 | The dead bodies in the basement

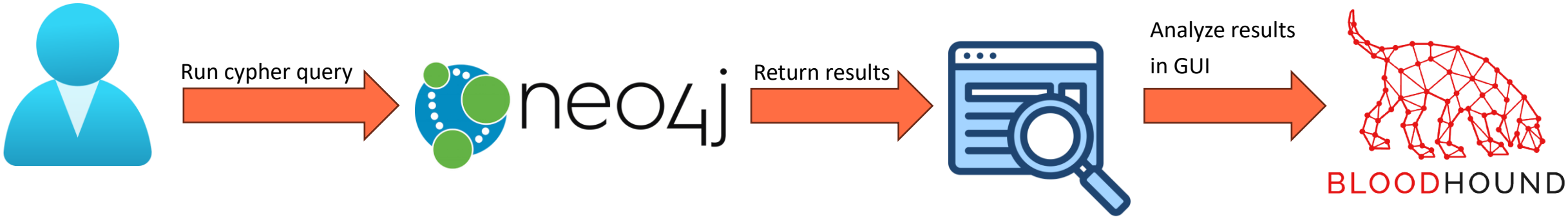
AD object permissions – What happens if you create an AD object – Conclusion of the results



04 | The dead bodies in the basement

AD object permissions – How to hunt for these kind of issues

- To identify these kind of permission issues we can use existing tooling



04 | The dead bodies in the basement

AD object permissions – How to hunt for these kind of issues

- Let´s have a look on which users own how many objects using a cypher query:

```
MATCH (u:User)-[:Owns]->(n) RETURN
count(DISTINCT(n.name)) AS OwnedObjects,
u.name AS USER ORDER BY
count(DISTINCT(n.name)) DESC
```

```
neo4j$ MATCH (u:User)-[:Owns]→(n) RETURN count(DISTINCT(n.name)) AS OwnedObjects, u.name AS USER ORDER BY count(DISTINCT(n.name)) DESC
```

Table | Text | Code

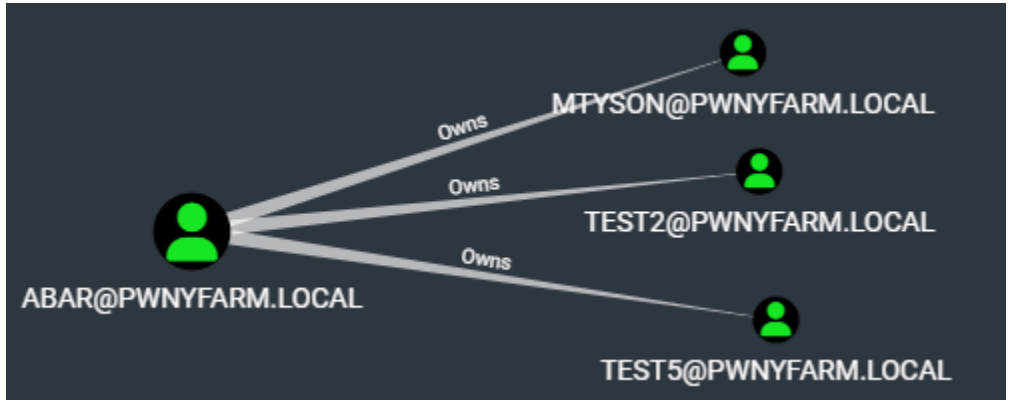
	OwnedObjects	USER
1	3	"ABAR@PWNYFARM.LOCAL"
2	2	"JCOLE@PWNYFARM.LOCAL"

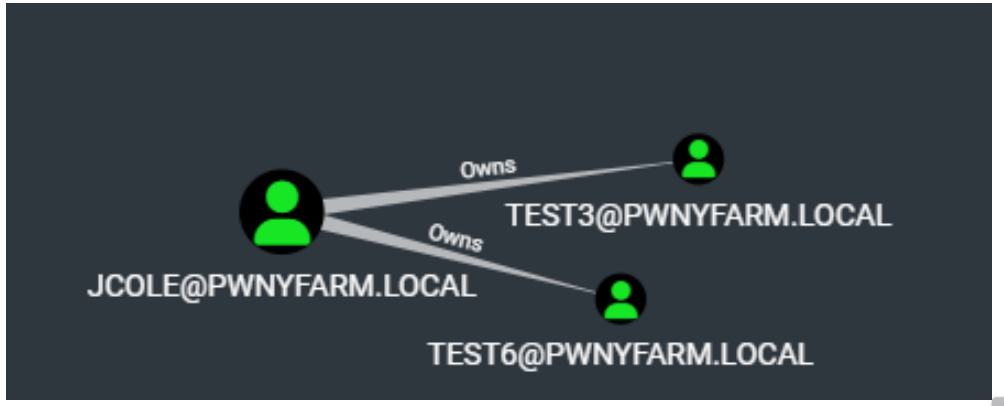
04 | The dead bodies in the basement

AD object permissions – How to hunt for these kind of issues

- Let´s have a look on which users own how many objects using a cypher query:

```
MATCH (n:User) WHERE n.name =~ 'ABAR@PWNYFARM.LOCAL'
MATCH (m) WHERE NOT m.name = n.name
MATCH p=allShortestPaths((n)-[r:Owns|SQLAdmin*1..]->(m))
RETURN p
```





04 | The dead bodies in the basement

AD object permissions – Conclusions

- There is a common misconception that cleaning up the group memberships during a AD transformation project will remove all critical permissions
- We can identify these issues by using neo4j and Bloodhound
- After identification, we can start fixing the issues

- There are three more useful neo4j queries I will leave you for the workshop

04 | The dead bodies in the basement

File permissions – What happens if you create a file on a share

- Let´s focus on some critical shares

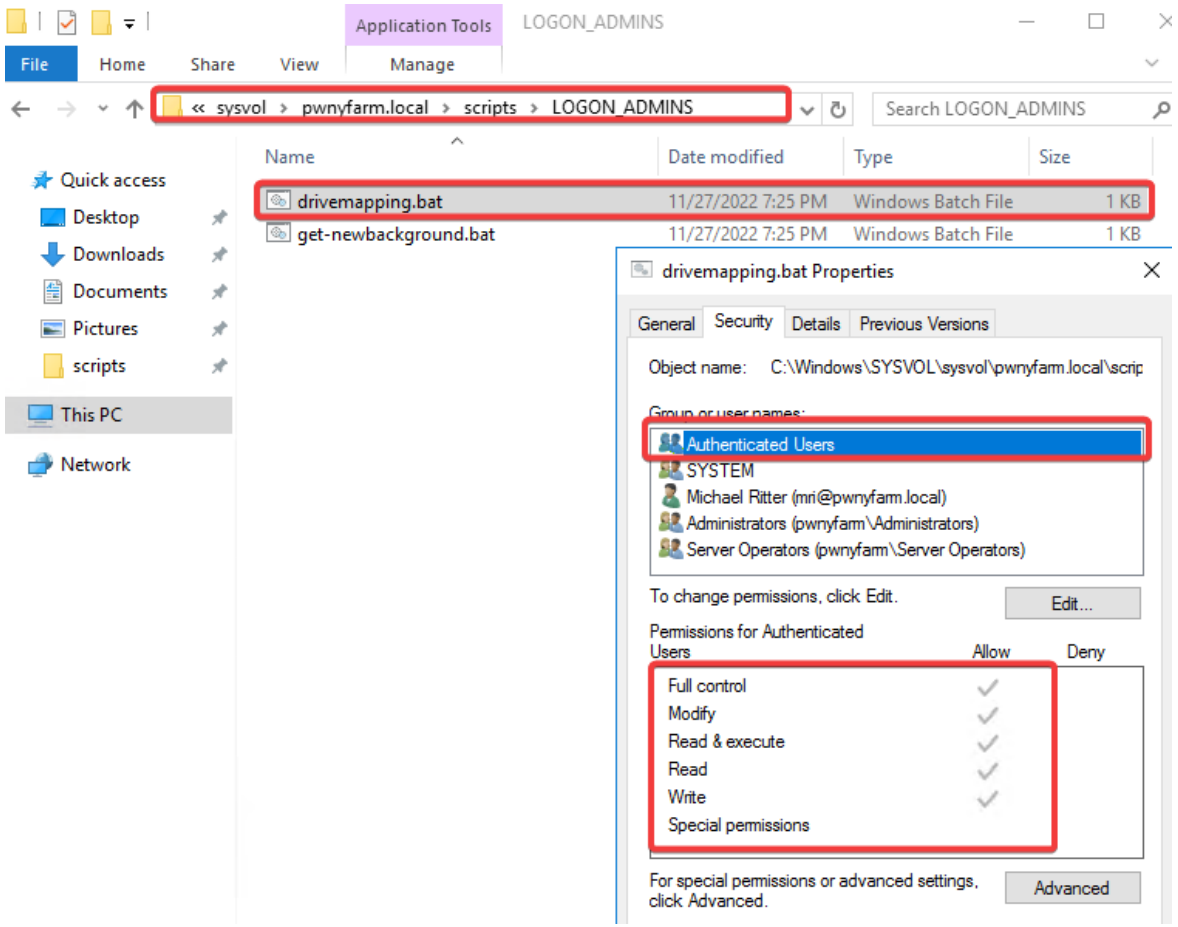
Why these shares?

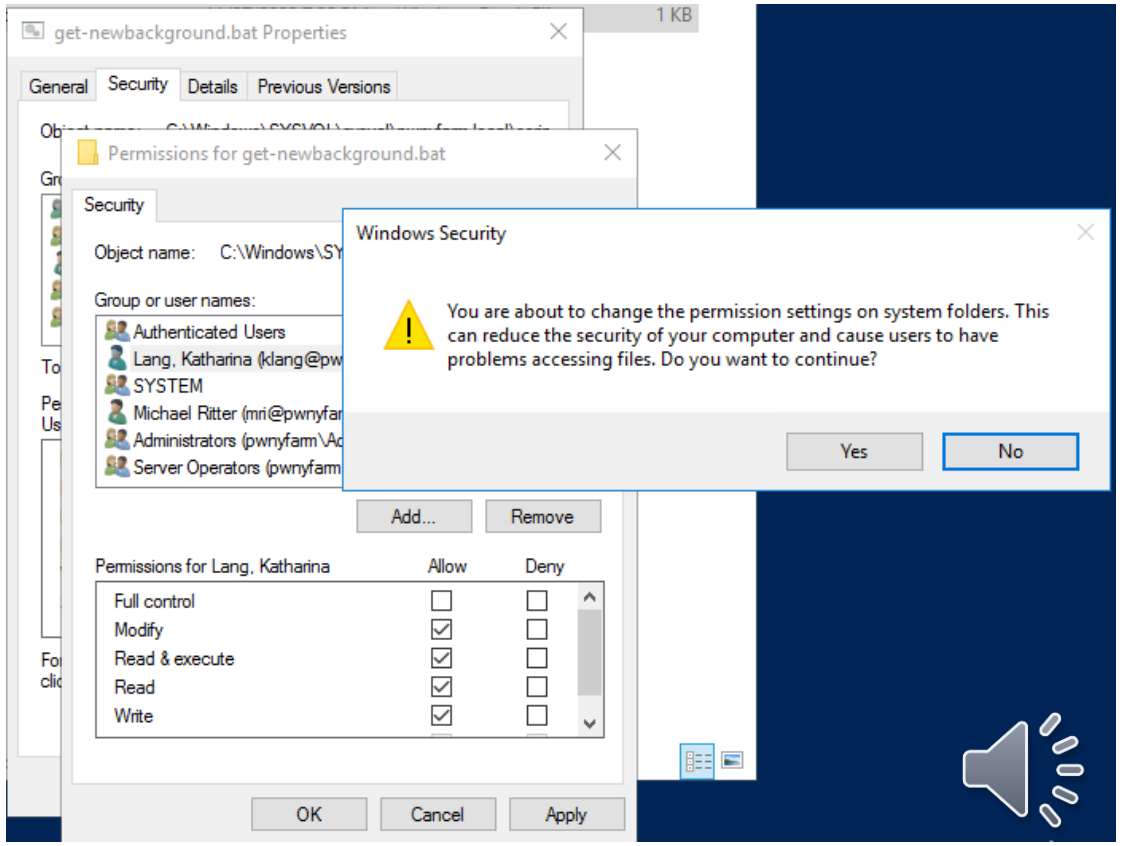
- Because they are very critical, since they are hosting settings and logon script that are deployed throughout the environment.

04 | The dead bodies in the basement

File permissions – What happens if you create a file on a share

- Example:

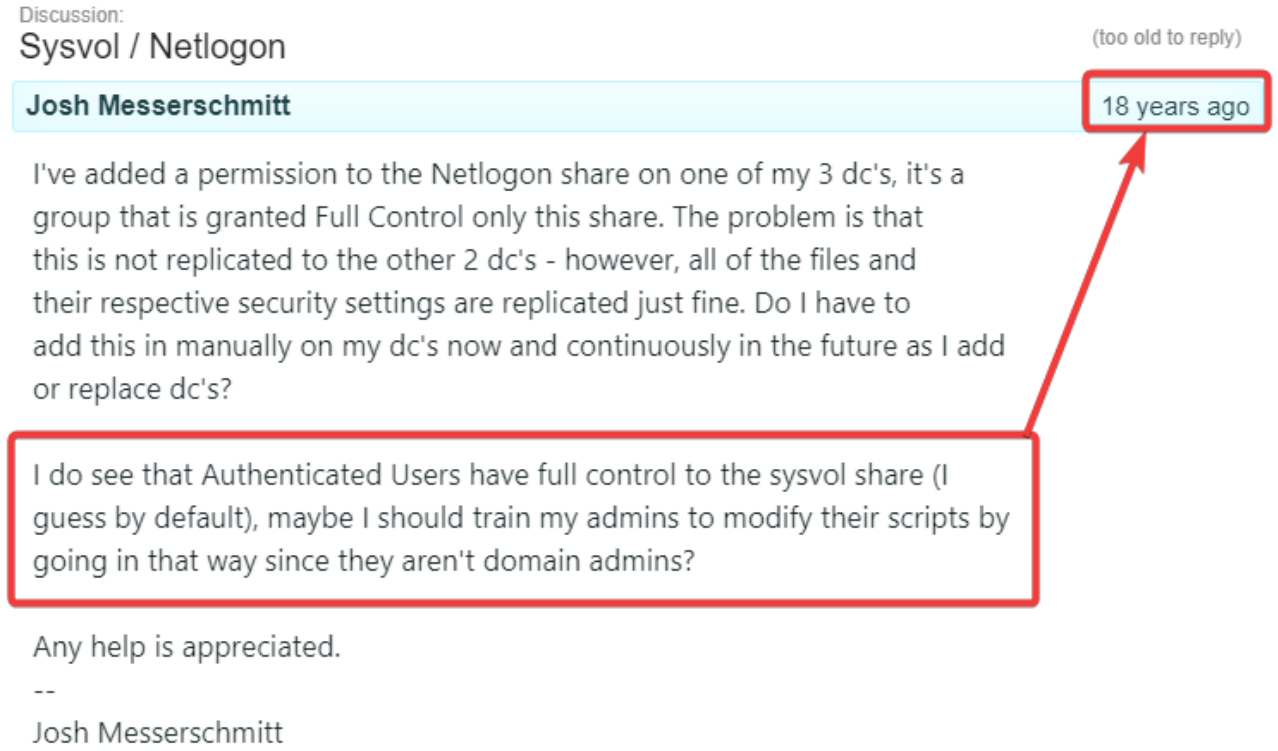




04 | The dead bodies in the basement

File permissions – The internet never forgets

- Plus I found this article during my research
  - https://microsoft.public.windows.server.active-directory.narkive.com/SBmR8YhL/sysvol-netlogon



Discussion:
Sysvol / Netlogon

(too old to reply)

Josh Messerschmitt — 18 years ago

I've added a permission to the Netlogon share on one of my 3 dc's, it's a group that is granted Full Control only this share. The problem is that this is not replicated to the other 2 dc's - however, all of the files and their respective security settings are replicated just fine. Do I have to add this in manually on my dc's now and continuously in the future as I add or replace dc's?

I do see that Authenticated Users have full control to the sysvol share (I guess by default), maybe I should train my admins to modify their scripts by going in that way since they aren't domain admins?

Any help is appreciated.
--
Josh Messerschmitt

04 | The dead bodies in the basement

File permissions – What happens if you create

- How to analyze the shares for interesting permissions?

```
# Download and load required functions
- https://github.com/michiiii/Get-FileShareAccessRights

# Collect the permissions
$permissions = Get-FileShareCriticalPermissions -NetworkSharePath \\pwnyfarm.local\netlogon

# Get an overview of users that have potential critical permissions
Get-CriticalPermissionOverview -SharePermissions $permissions
```

```
PS C:\Users\abar\Downloads\SharpHound-v2.0.1> Get-CriticalPermissionOverview -SharePermis

Name                                Count
----                                -----
NT AUTHORITY\Authenticated Users       36
pwnyfarm\mri                           18
pwnyfarm\lkaiser                        7
pwnyfarm\jcole                          9
```

04 | The dead bodies in the basement

File permissions – What happens if you create

```
# Finally, you can filter the results for intersting user/groups
Get-CriticalPermissionsByUser -SharePermissions $permissions -UserName mri
```

```
Administrator: Windows PowerShell
PS C:\Users\abar\Downloads\SharpHound-v2.0.1> Get-CriticalPermissionsByUser -SharePermissions $permissions -UserName mri

Path                                                    Username     AccessRight            IsInherited
----                                                    --------     -----------            -----------
\\pwnyfarm.local\netlogon\LOGON_ADMINS\drivemapping.bat pwnyfarm\mri WriteData                       True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\drivemapping.bat pwnyfarm\mri CreateFiles                     True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\drivemapping.bat pwnyfarm\mri AppendData                      True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\drivemapping.bat pwnyfarm\mri WriteExtendedAttributes         True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\drivemapping.bat pwnyfarm\mri WriteAttributes                 True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\drivemapping.bat pwnyfarm\mri Write                           True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\drivemapping.bat pwnyfarm\mri Delete                          True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\drivemapping.bat pwnyfarm\mri ChangePermissions               True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\drivemapping.bat pwnyfarm\mri TakeOwnership                   True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\get-newbackground.bat pwnyfarm\mri WriteData                  True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\get-newbackground.bat pwnyfarm\mri CreateFiles                True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\get-newbackground.bat pwnyfarm\mri AppendData                 True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\get-newbackground.bat pwnyfarm\mri WriteExtendedAttributes    True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\get-newbackground.bat pwnyfarm\mri WriteAttributes            True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\get-newbackground.bat pwnyfarm\mri Write                      True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\get-newbackground.bat pwnyfarm\mri Delete                     True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\get-newbackground.bat pwnyfarm\mri ChangePermissions          True
\\pwnyfarm.local\netlogon\LOGON_ADMINS\get-newbackground.bat pwnyfarm\mri TakeOwnership              True
```

04 | The dead bodies in the basement

File permissions – Conclusions

- File permission issues on NETLOGON and SYSVOL can have severe consequences for the overall security in an Active Directory environment
- I still have no explanation why this issue is present in so many “older” environments
  - I am still not able to reproduce this issue in an modern environment
  - The default inheritance settings are usually passed to any file that is created on the SYSVOL or NETLOGON share
  - Maybe in the past there was a silent patch that fixed a permission issue

I would love to get feedback about the results you get when analyzing your environment?

SEC Consult
an Eviden business

5 Conclusion

Thank you!

Dou you have any further questions?
For more information please contact:

Michael Ritter
Principal Security Consultant

https://www.linkedin.com/in/michiiii/
https://github.com/michiiii
https://twitter.com/BigM1ke_oNe