



TEAL
ALWAYS CHALLENGING IT



Hidden Pathways: Exploring the Anatomy of ACL-Based Active Directory Attacks and Building Strong Defenses

Who we are

Alexander Schmitt

Co-CEO & Co-Founder
@ TEAL



 <https://www.teal-consulting.de/>

 [LinkedIn](#)

TEAL is the trusted advisor in all matters of information security. We share our experience and know-how in the area of Microsoft infrastructure and Active Directory security in customer-specific project implementations.



Jonas B. Knudsen

Product Architect
@ SpecterOps

 <https://specterops.io/>

 [LinkedIn](#)

SpecterOps provides expert knowledge of cyber attackers and resources to improve your security. The focus product BloodHound Enterprise quantifies and monitors attack vectors in Active Directory.

What do we talk about

- What are ACLs and ACL based attack primitives?
- Why is this relevant?
- What can we do about it?



What are AD ACLs and ACEs?

Security descriptor: CN=andy,CN=Users,DC=dumpster,DC=fire

Owner: DUMPSTER\Domain Admins

Group: DUMPSTER\Domain Admins

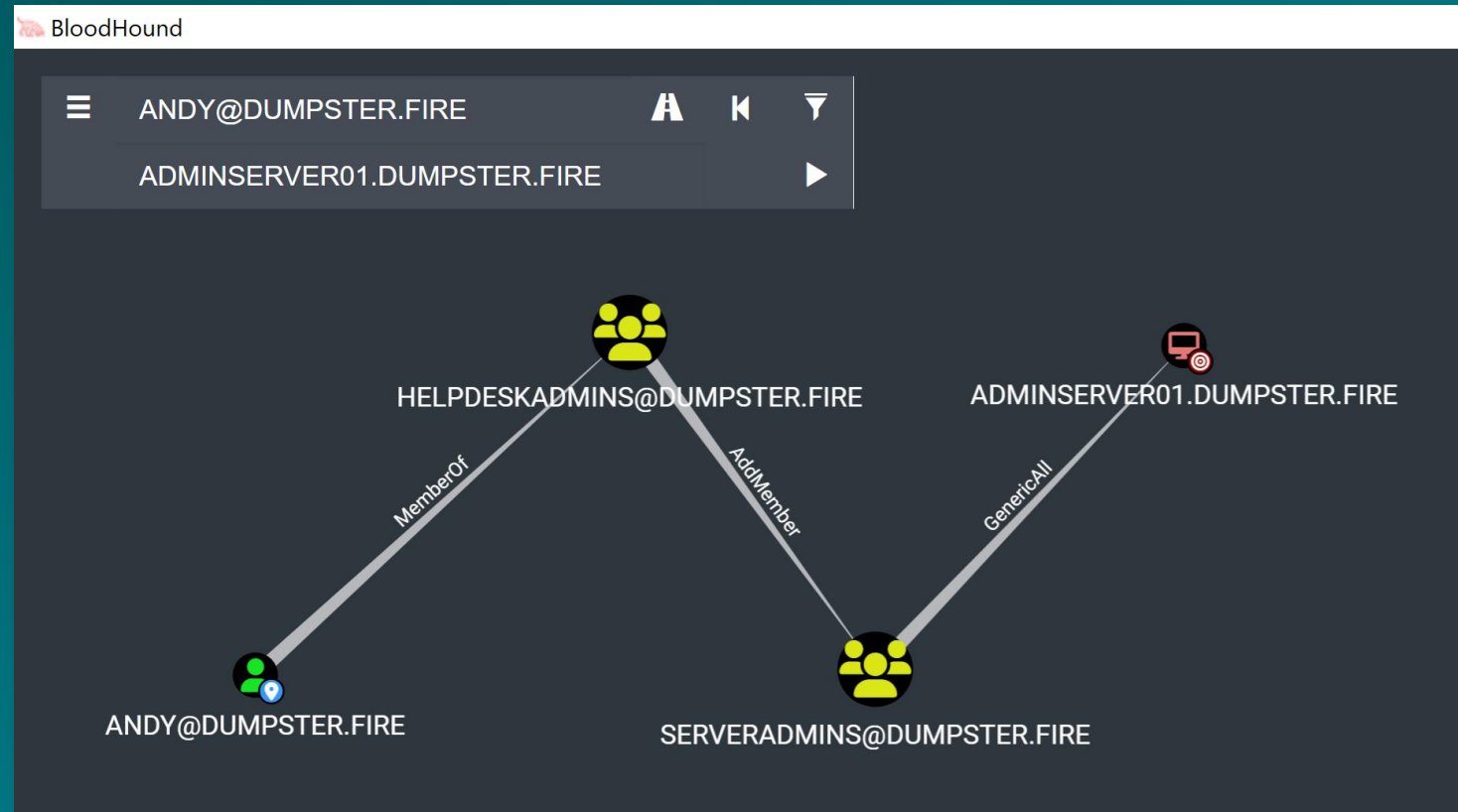
SD control

- SELF_RELATIVE
- OWNER_DEFAULTED
- GROUP_DEFAULTED
- DACL_PRESENT
- DACL_PROTECTED
- DACL_AUTO_INHERITED
- DACL_DEFAULTED

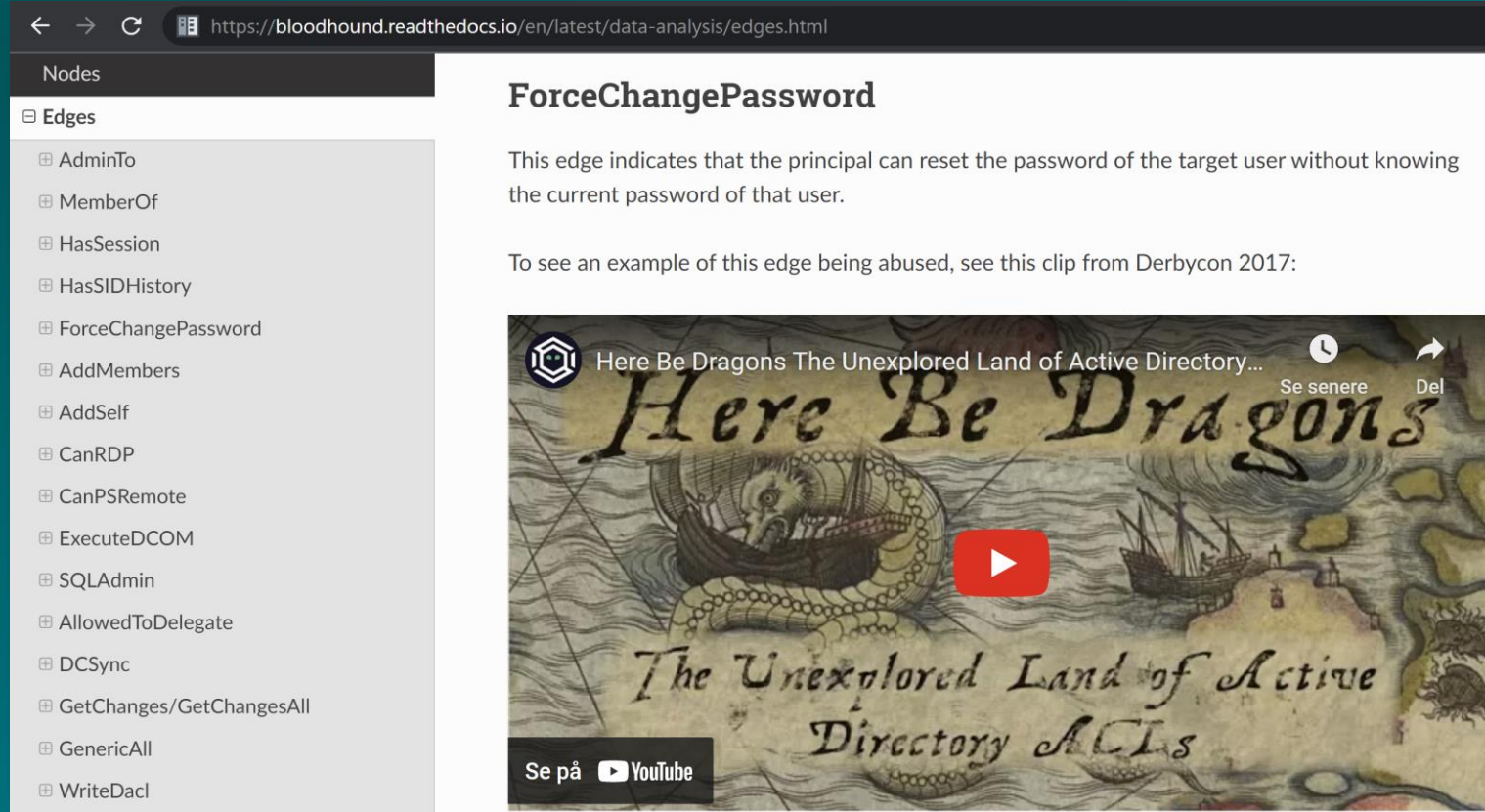
DACL (32 ACEs)

Type	Trustee	Rights	Flags
Allow	BUILTIN\Account Operators	Full control	
Allow	BUILTIN\Administrators	Write, List object, Write DACL, Write owner, Create c...	Inherit, Inherited
Allow	BUILTIN\Pre-Windows 2000 Compatible Access	Read	Inherit, Inherited (user)
Allow	BUILTIN\Pre-Windows 2000 Compatible Access	Read	Inherit, Inherit only, Inherited (group)
Allow	BUILTIN\Pre-Windows 2000 Compatible Access	List	Inherit, Inherited
Allow	DUMPSTER\Cert Publishers	Read property, Write property (userCertificate)	
Allow	DUMPSTER\Domain Admins	Full control	
Allow	DUMPSTER\Enterprise Admins	Full control	Inherit, Inherited
Allow	DUMPSTER\service desk	Control access (Reset Password)	Inherit, Inherited (user)

ACL Enumeration: BloodHound



ACL Enumeration: BloodHound




The screenshot shows the BloodHound web interface. The browser address bar displays `https://bloodhound.readthedocs.io/en/latest/data-analysis/edges.html`. On the left, a sidebar lists various edges, with `ForceChangePassword` selected. The main content area displays the definition for `ForceChangePassword`.

ForceChangePassword

This edge indicates that the principal can reset the password of the target user without knowing the current password of that user.

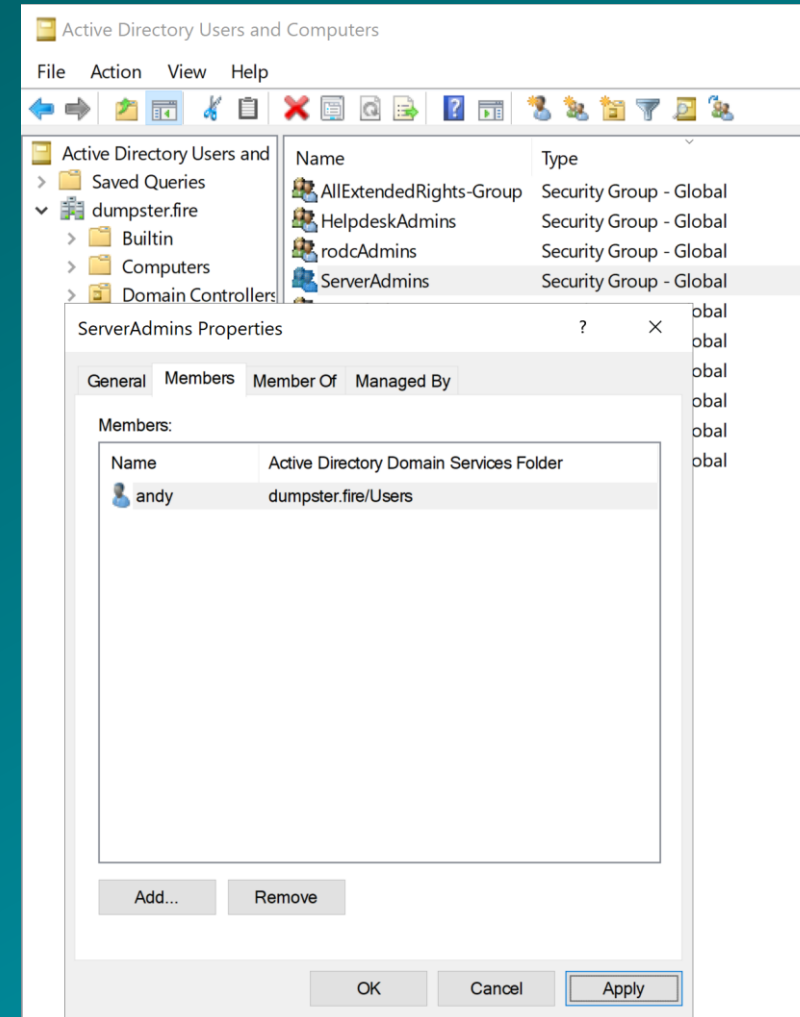
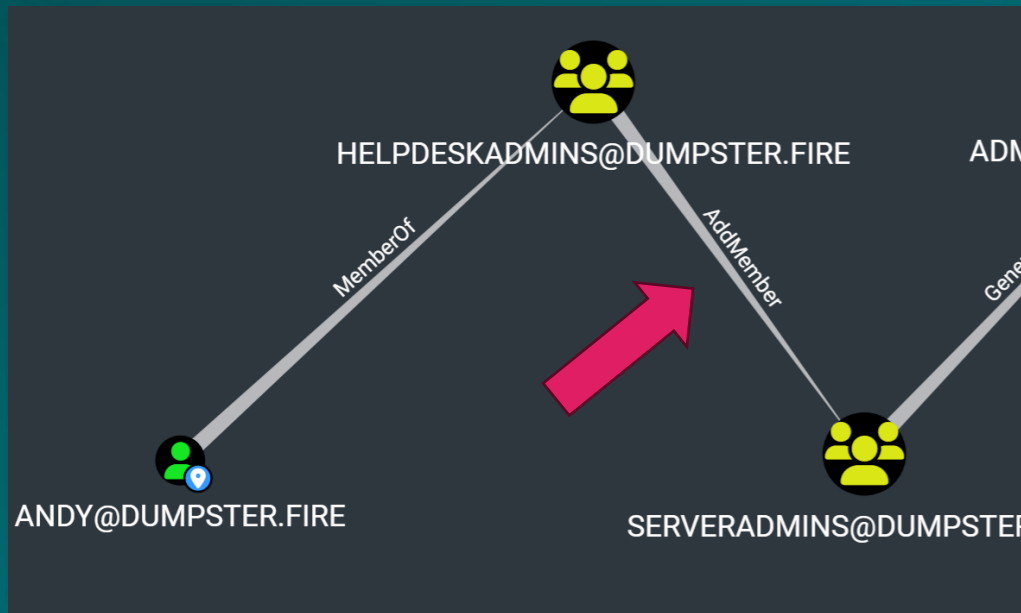
To see an example of this edge being abused, see this clip from Derbycon 2017:



The video thumbnail features a map with a dragon and a ship, with the text `Here Be Dragons` and `The Unexplored Land of Active Directory ACLs`. The video player interface includes a play button, a channel icon, and controls for 'Se senere' and 'Del'.

ACE abuse examples

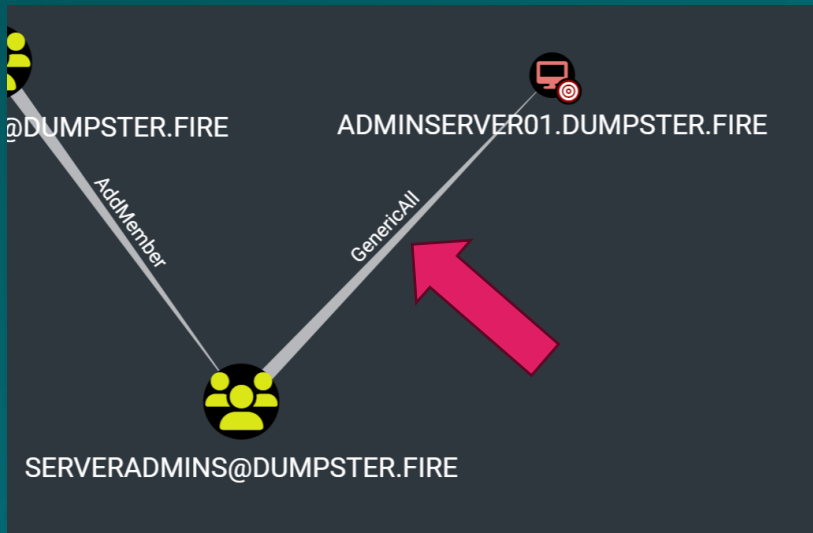
AddMember



ACE abuse examples

GenericAll on a computer

LAPS? -> Read LAPS password



AdminServer01 Properties

General	Operating System	Member Of	Delegation	Password Replication	
Location	Managed By	Object	Security	Dial-in	Attribute Editor

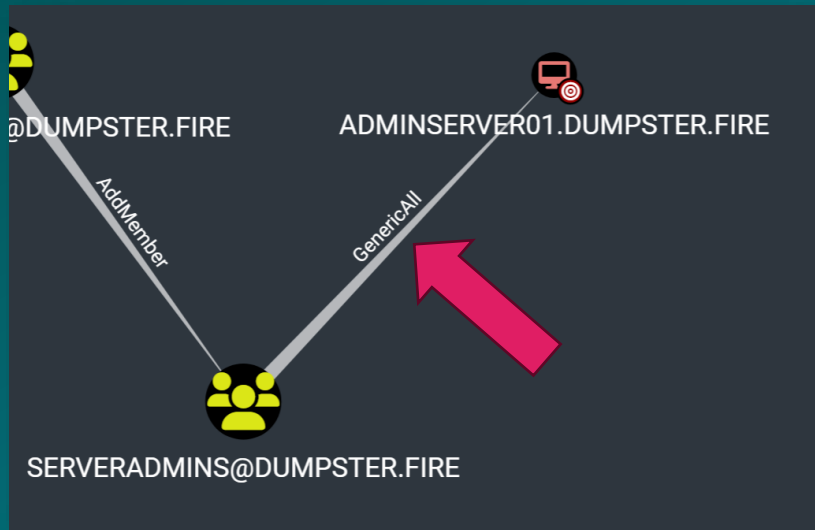
Attributes:

Attribute	Value
msIS-FTPDir	<not set>
msIS-FTPRoot	<not set>
msImaging-HashAlgorithm	<not set>
msImaging-ThumbprintHash	<not set>
ms-Mcs-AdmPwd	7,%-.68h4li!1L
ms-Mcs-AdmPwdExpirationTi...	133305430304707991
mSMQDigests	<not set>
mSMQDigestsMig	<not set>

ACE abuse examples

GenericAll on a computer

No LAPS? -> Two other options



Option 1: Shadow credentials ¹

- Add alternative credentials to the target, allowing for obtaining a TGT and the NTLM hash for the target.

Option 2: Resource-Based Constrained Delegation (RBCD) attack ²

- Configure RBCD on target to allow a compromised principal to impersonate any user against the target.

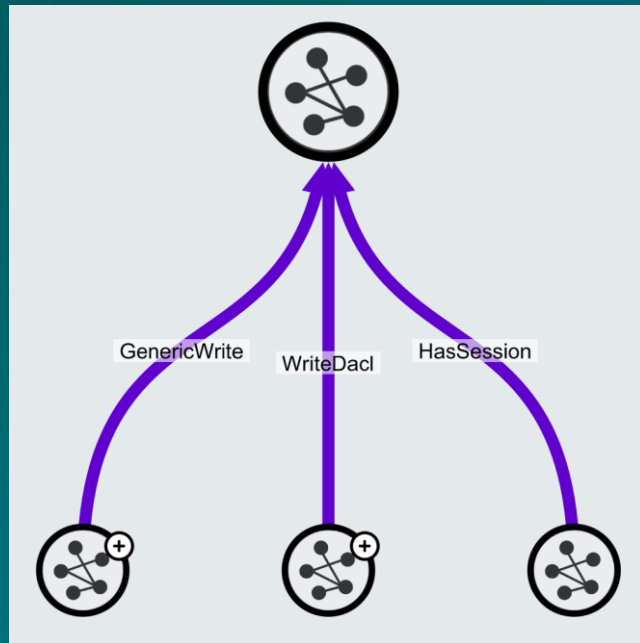
¹ <https://eladshamir.com/2021/06/21/Shadow-Credentials.html>

² <https://eladshamir.com/2019/01/28/Wagging-the-Dog.html>

Why this is still relevant – what we see in the field

ACL-based attacks has been a known problem for a while
... but they are still common

Crown Jewels →



Purple edge: Exposure > 95%



Why this is still relevant – what we see in the field

1. AD ACLs are complicated
2. New attack narratives are still being found
3. It is difficult to determine what ACEs are bad
4. The scale of the problem is overwhelming

Why this is still relevant – what we see in the field

1. AD ACLs are complicated
 - AD schema and Default Security Descriptor

Security descriptor - CN=andy,CN=Users,DC=dumpster,DC=fire

Owner DUMPSTER\Domain Admins

Group DUMPSTER\Domain Admins

SD control

<input checked="" type="checkbox"/> SELF_RELATIVE	<input checked="" type="checkbox"/> DACL_PRESENT
<input type="checkbox"/> OWNER_DEFAULTED	<input type="checkbox"/> DACL_PROTECTED
<input type="checkbox"/> GROUP_DEFAULTED	<input checked="" type="checkbox"/> DACL_AUTO_INHERITED
	<input type="checkbox"/> DACL_DEFAULTED

DACL (32 ACEs)

Type	Trustee	Rights	Flags
Allow	BUILTIN\Account Operators	Full control	
Allow	BUILTIN\Administrators	Write, List object, Write DACL, Write owner, Create c...	Inherit, Inherited

Why this is still relevant – what we see in the field

1. AD ACLs are complicated
 - AD schema and Default Security Descriptor
 - AdminSDHolder

Security descriptor - CN=Domain Admins,CN=Users,DC=dumpster,DC=fire

Owner: DUMPSTER\Domain Admins
Group: DUMPSTER\Domain Admins

SD control

<input checked="" type="checkbox"/> SELF_RELATIVE	<input checked="" type="checkbox"/> DACL_PRESENT	<input type="checkbox"/> SACL_PRESENT
<input type="checkbox"/> OWNER_DEFAULTED	<input checked="" type="checkbox"/> DACL_PROTECTED	<input type="checkbox"/> SACL_PROTECTED
<input type="checkbox"/> GROUP_DEFAULTED	<input checked="" type="checkbox"/> DACL_AUTO_INHERITED	<input checked="" type="checkbox"/> SACL_AUTO_INHERITED
	<input type="checkbox"/> DACL_DEFAULTED	<input type="checkbox"/> SACL_DEFAULTED

DACL (13 ACEs)

T...	Trustee	Rights	Flags
Allow	DUMPSTER\Cert Publishers	Read property, Write property (userCertificate)	
Allow	BUILTIN\Windows Authorization Acc...	Read property (tokenGroupsGlobalAndUniversal)	
Allow	BUILTIN\Terminal Server License Se...	Read property, Write property (terminalServer)	
Allow	BUILTIN\Terminal Server License Se...	Read property, Write property (Terminal Server Li...	
Allow	Everyone	Control access (Change Password)	
Allow	NT AUTHORITY\SELF	Control access (Change Password)	
Allow	NT AUTHORITY\SELF	Read property, Write property, Control access (Pri...	Inherit
Allow	DUMPSTER\Domain Admins	Write, List object, Write DACL, Write owner, Creat...	
Allow	DUMPSTER\Enterprise Admins	Write, List object, Write DACL, Write owner, Creat...	
Allow	BUILTIN\Pre-Windows 2000 Compat...	Read	
Allow	BUILTIN\Administrators	Write, List object, Write DACL, Write owner, Creat...	
Allow	NT AUTHORITY\Authenticated Users	Read property, List, Read permissions	
Allow	NT AUTHORITY\SYSTEM	Full control	



Security descriptor - CN=AdminSDHolder,CN=System,DC=dumpster,DC=fire

Owner: DUMPSTER\Domain Admins
Group: DUMPSTER\Domain Admins

SD control

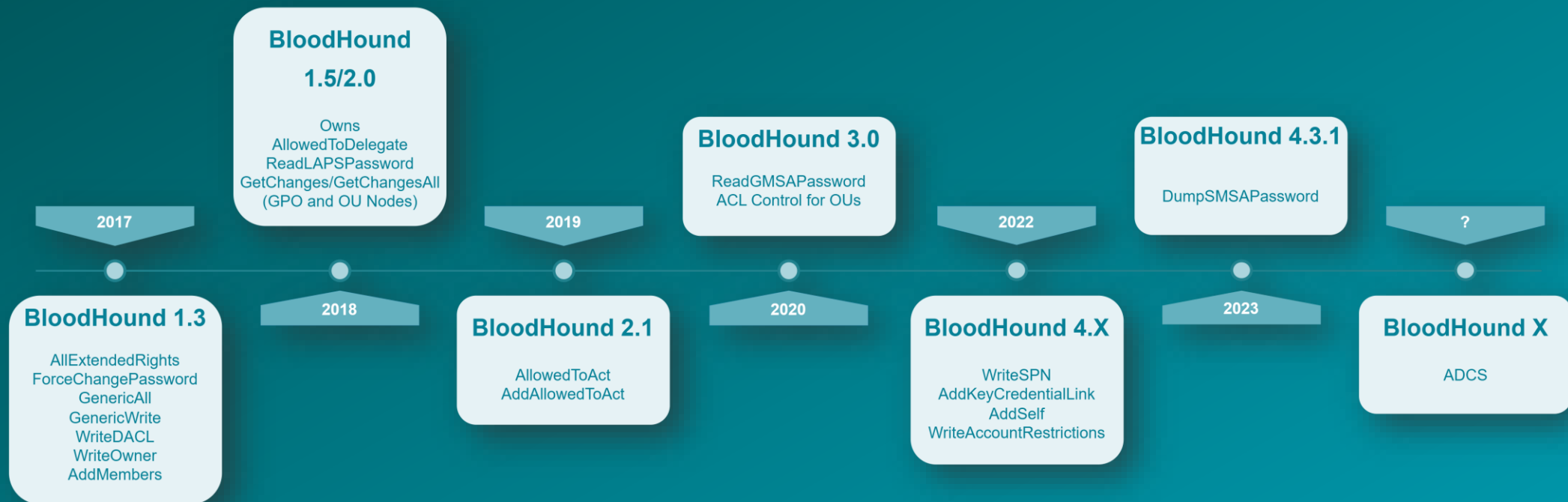
<input checked="" type="checkbox"/> SELF_RELATIVE	<input checked="" type="checkbox"/> DACL_PRESENT	<input type="checkbox"/> SACL_PRESENT
<input type="checkbox"/> OWNER_DEFAULTED	<input checked="" type="checkbox"/> DACL_PROTECTED	<input type="checkbox"/> SACL_PROTECTED
<input type="checkbox"/> GROUP_DEFAULTED	<input checked="" type="checkbox"/> DACL_AUTO_INHERITED	<input checked="" type="checkbox"/> SACL_AUTO_INHERITED
	<input type="checkbox"/> DACL_DEFAULTED	<input type="checkbox"/> SACL_DEFAULTED

DACL (13 ACEs)

Type	Trustee	Rights	Flags
Allow	DUMPSTER\Cert Publishers	Read property, Write property (userCertificate)	
Allow	BUILTIN\Windows Authorization Acc...	Read property (tokenGroupsGlobalAndUniversal)	
Allow	BUILTIN\Terminal Server License Se...	Read property, Write property (terminalServer)	
Allow	BUILTIN\Terminal Server License Se...	Read property, Write property (Terminal Server Li...	
Allow	Everyone	Control access (Change Password)	
Allow	NT AUTHORITY\SELF	Control access (Change Password)	
Allow	NT AUTHORITY\SELF	Read property, Write property, Control access (Pri...	Inherit
Allow	DUMPSTER\Domain Admins	Write, List object, Write DACL, Write owner, Creat...	
Allow	DUMPSTER\Enterprise Admins	Write, List object, Write DACL, Write owner, Creat...	
Allow	BUILTIN\Pre-Windows 2000 Compat...	Read	
Allow	BUILTIN\Administrators	Write, List object, Write DACL, Write owner, Creat...	
Allow	NT AUTHORITY\Authenticated Users	Read property, List, Read permissions	
Allow	NT AUTHORITY\SYSTEM	Full control	

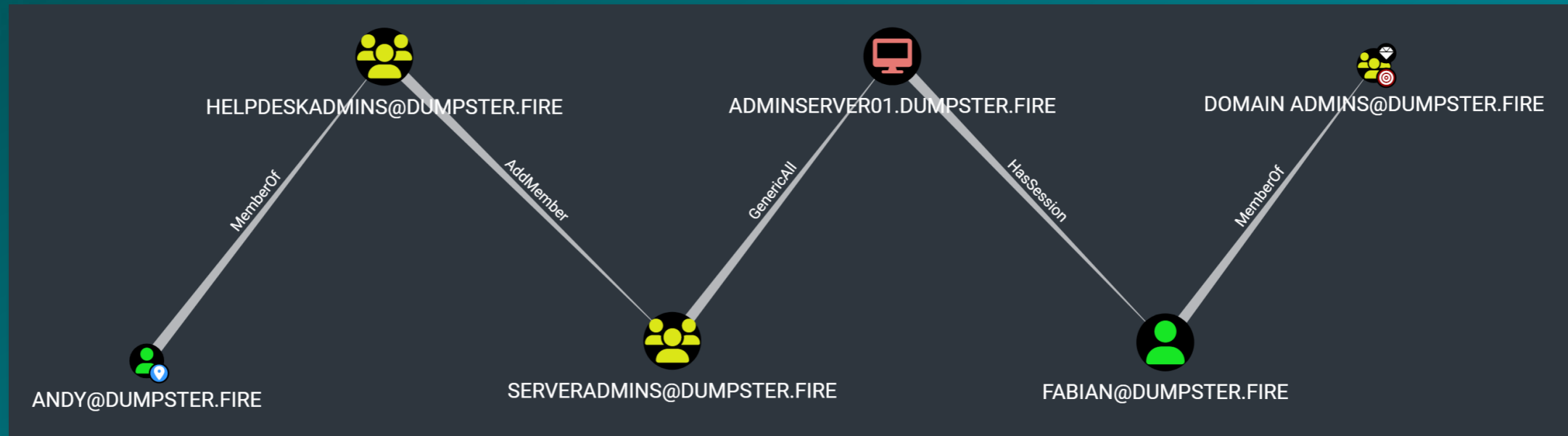
Why this is still relevant – what we see in the field

1. AD ACLs are complicated
2. New attack narratives are still being found















Why this is still relevant – what we see in the field

1. AD ACLs are complicated
2. New attack narratives are still being found
3. It is difficult to determine what ACEs are bad



Why this is still relevant – what we see in the field

1. AD ACLs are complicated
2. New attack narratives are still being found
3. It is difficult to determine what ACEs are bad
4. The scale of the problem is overwhelming

 Users		4,459
 Groups		24,646
 Computers		4,207
 OUs		9,951
 GPOs		65
 Containers		46
 Sessions		89
 ACLs		360,372
 Relationships		486,151



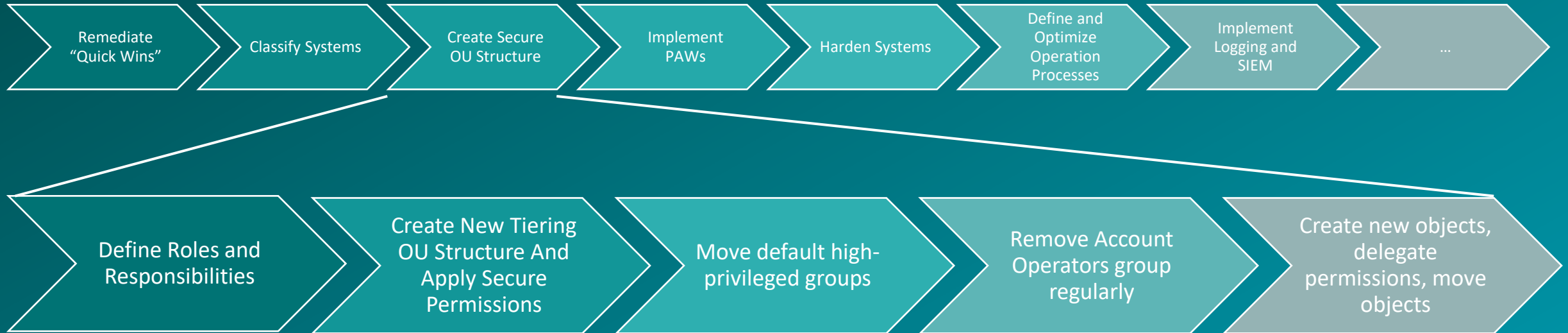
TEAL
ALWAYS CHALLENGING IT



What can we do about it?

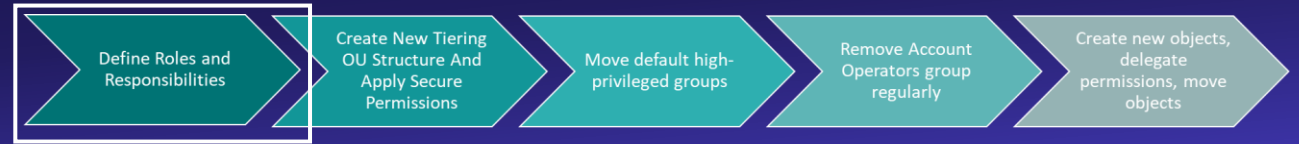
What can we do about it?

- One solution is to implement a tiering structure in Active Directory
- Tiering, when we talk about it, is more than a secure OU structure:



- We do not recommend to clean-up (many) old ACLs but start from scratch in a secured OU structure
- Our recommendation is based on the [Best Practice Guide for Securing Active Directory Installations](#) (from 2011 🐒)

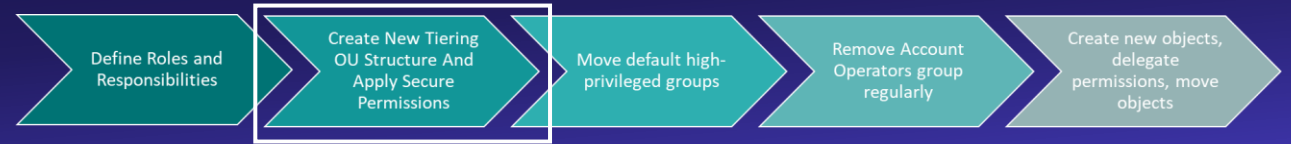
Define Roles and Responsibilities



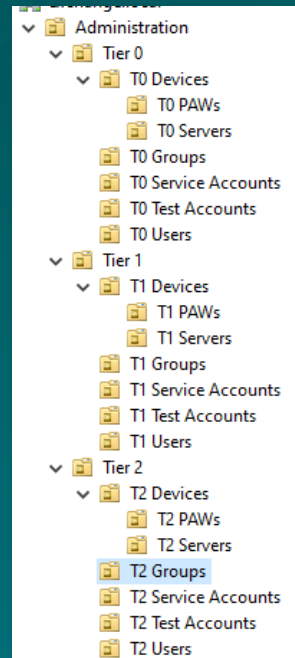
- Ask the question: Who is supposed to do what?
- It will be a painful and cumbersome task 😞

Role	Servers	Tasks / Responsibilities	Persons	Accounts	Necessary Rights	Role Group	Permission Groups
Tier 0 AD Admins	DC01 DC02	Active Directory system administration	Alexander Schmitt Fabian Böhm	AlexT0adm FabianT0adm	Domain Admin	RG_T0_IAM_Admin	Domain Admins
Tier 1 Server Admins	All tier 1 servers	Install updates	Manuel Hoffmann Jonas Knudsen	ManuelT1adm JonasT1adm	Local admin on all tier 1 servers	RG_T1_Server_Admin	PG_HRWEB01_localadmin PG_HRDB01_localadmin ...
Tier 2 Help Desk Admins	Adminserver1	Reset end user passwords Manage non-admin group memberships	Fabian Böhm Andy Robbins	FabianT2adm AndyT2adm	Reset Passwords in OU "Users" Manage groups in OU "T2AppGroups"	RG_T2_HelpDesk_Admin	PG_UsersPWD_w PG_T2AppGroupsGM_w

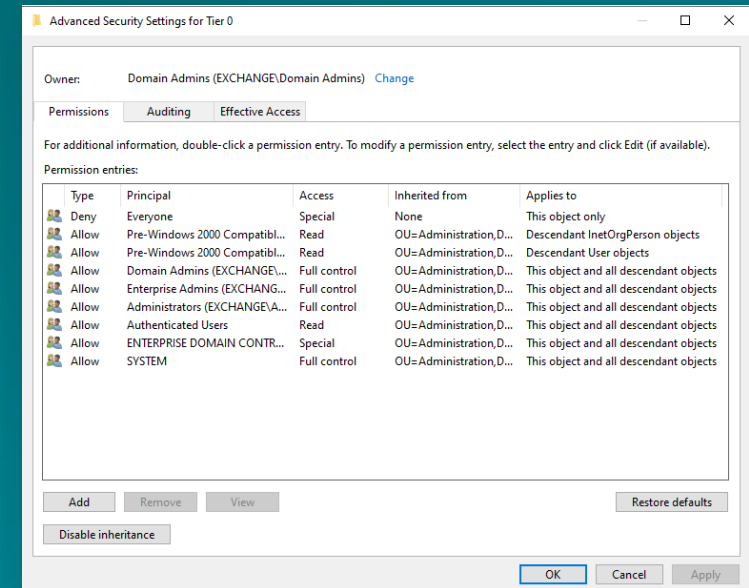
Create New Tiering OU Structure And Apply Secure Permissions



- Customizable to your needs
- For example:



- Block inheritance and apply secure permissions¹



- A script for easy creation will be released after the talk on <https://github.com/teal-technology-consulting/New-TealTierOUs>

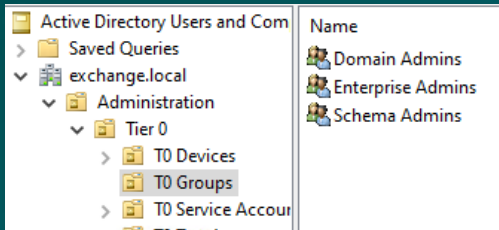
- A script that sets the permissions will be released after the talk on <https://github.com/teal-technology-consulting/Set-TealTierOUAcI>

¹ Establishing Secure Service Administration Practices | Microsoft Learn

Move default high-privileged groups



“Move Domain Admins, Schema Admins and Enterprise Admins to the secure OU structure



The built-in groups (Administrators, Server Operators, Account Operators, and Backup Operators) cannot be moved from their default container to the controlled subtree. However, built-in groups are protected by default in Windows Server 2003 by AdminSDHolder.”¹

- We recommend to move all default security groups in the Users container AFTER TESTING
 - There is documentation² but we are not sure how reliable it is
- Monitor these groups for membership changes

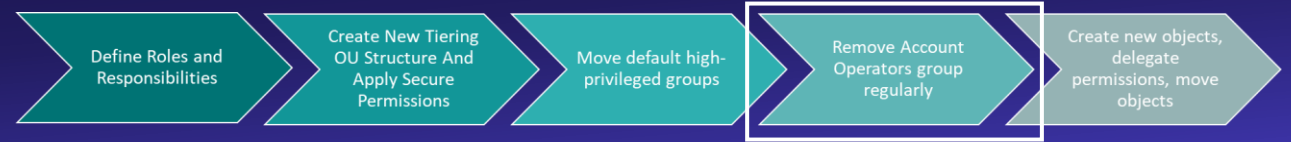
Safe to move out of default container?

You can move the group, but we don't recommend it

¹ [Establishing Secure Service Administration Practices | Microsoft Learn](#)

² [Active Directory security groups | Microsoft Learn](#)

Remove Account Operators regularly

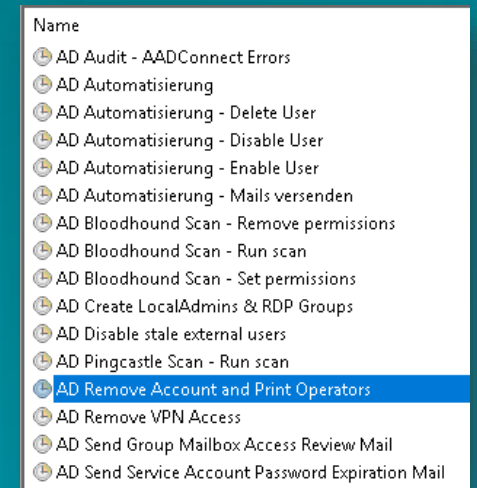


- New objects get the ACLs based on the Default Security Descriptor
- The Account Operators group has extensive permissions over various objects¹:

“The Account Operators group grants limited account creation privileges to a user. Members of this group can create and modify most types of accounts, including accounts for users, Local groups, and Global groups. Group members can log in locally to domain controllers.”²

- We recommend not to use the group at all – it can still be abused
 - Changing Default Security Descriptor might have unforeseen side effects
- We recommend to create a scheduled task that removes the Account Operators groups (and Print Operators for good measure) from all objects in the secure OU structure.

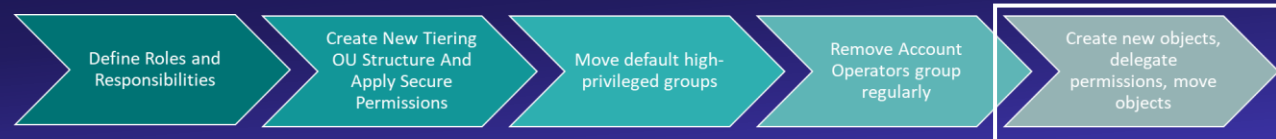
The script for the scheduled task will be released after the talk on our <https://github.com/teal-technology-consulting/Remove-AccAndPrintOpsFromOU>



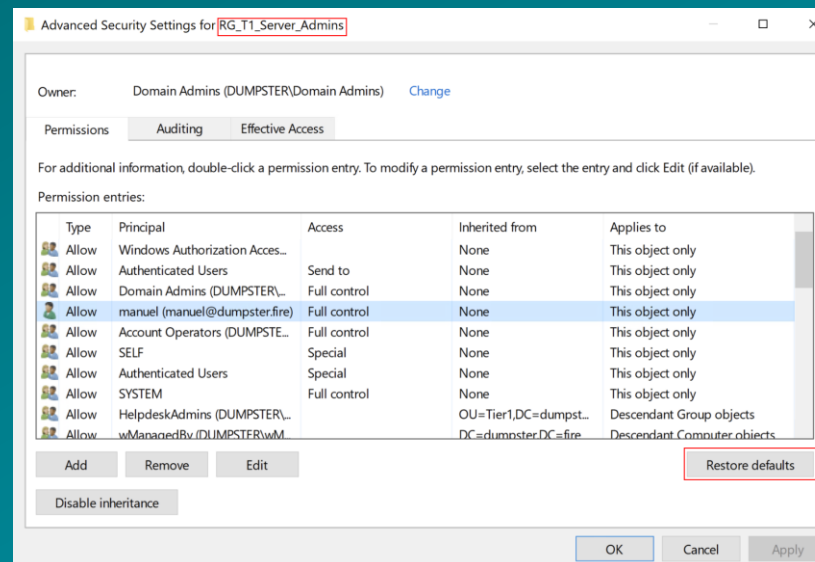
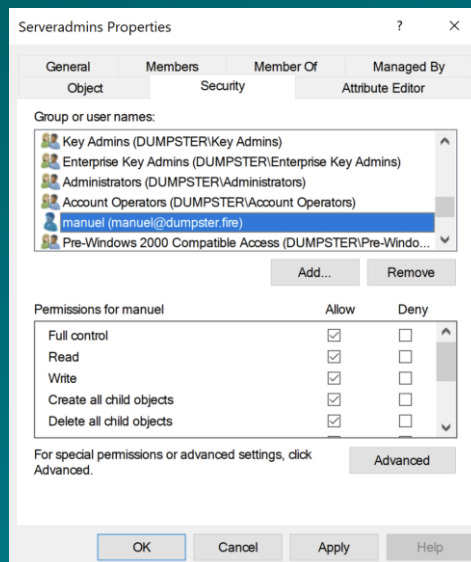
¹ 5 ways Attackers Exploit Account Operators - Secframe

² Active Directory security groups | Microsoft Learn

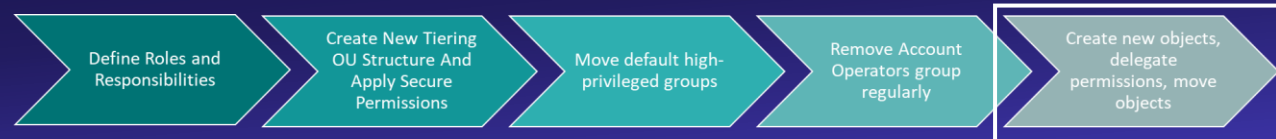
Create new objects, delegate permissions, move objects I



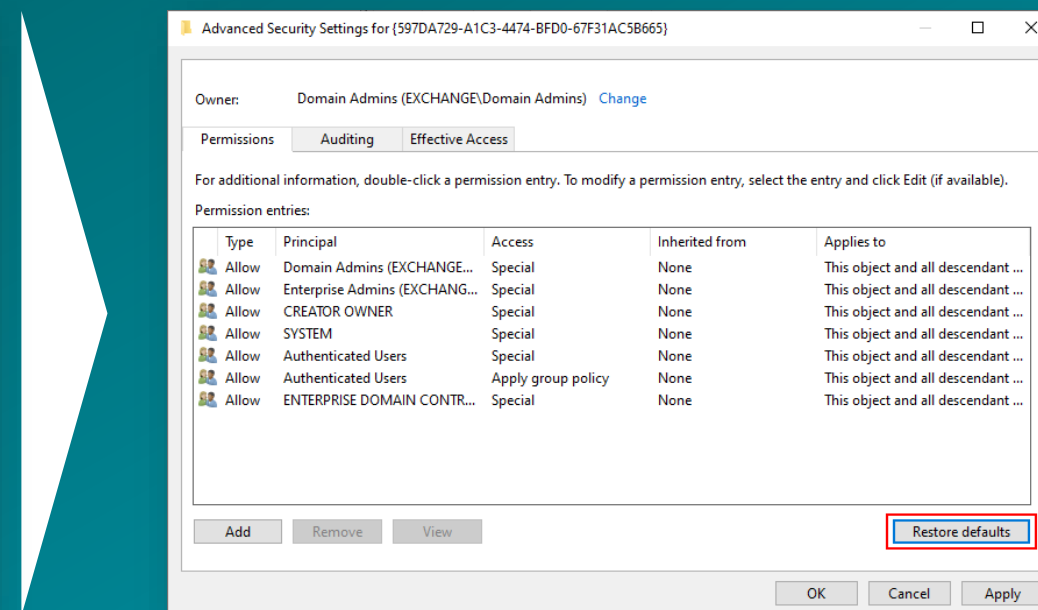
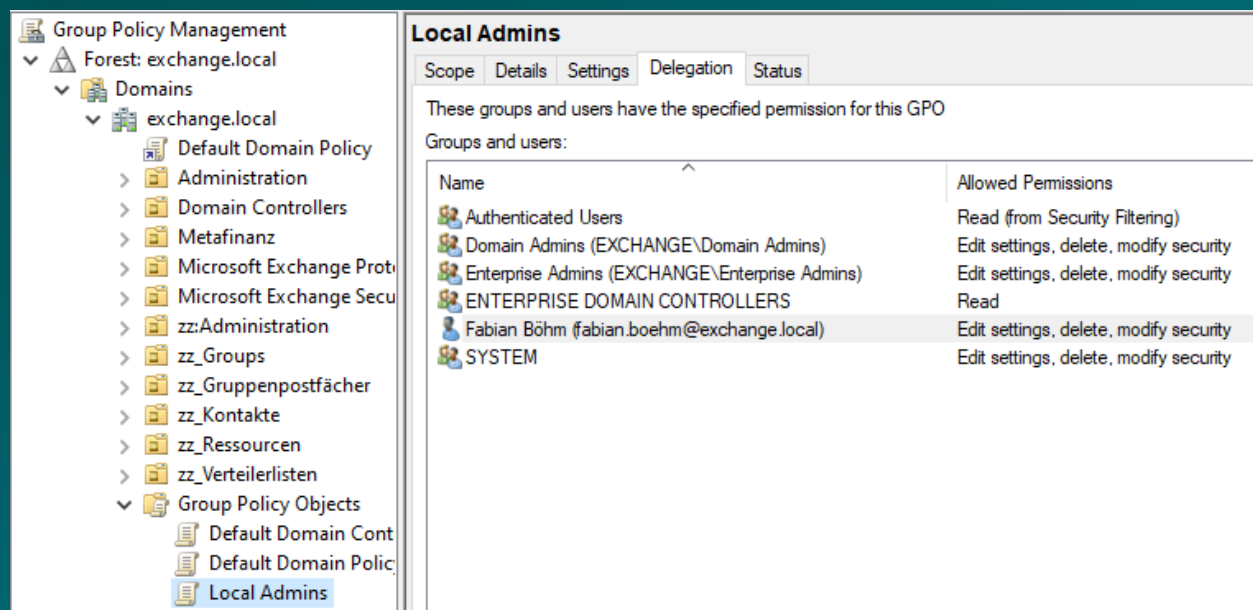
- Create new accounts and groups and delegate access
 - Create Logon Restriction Policies / Kerberos Authentication Silos
 - Train admins how to work with the new structure
 - This process takes quite some time depending on the size of the organization
 - Moved objects will keep directly assigned permission when moved to the secured OU structure
- When objects are moved into the secured OU structure check and sanitize the ACL



Create new objects, delegate permissions, move objects II



- Applies to GPO objects as well!



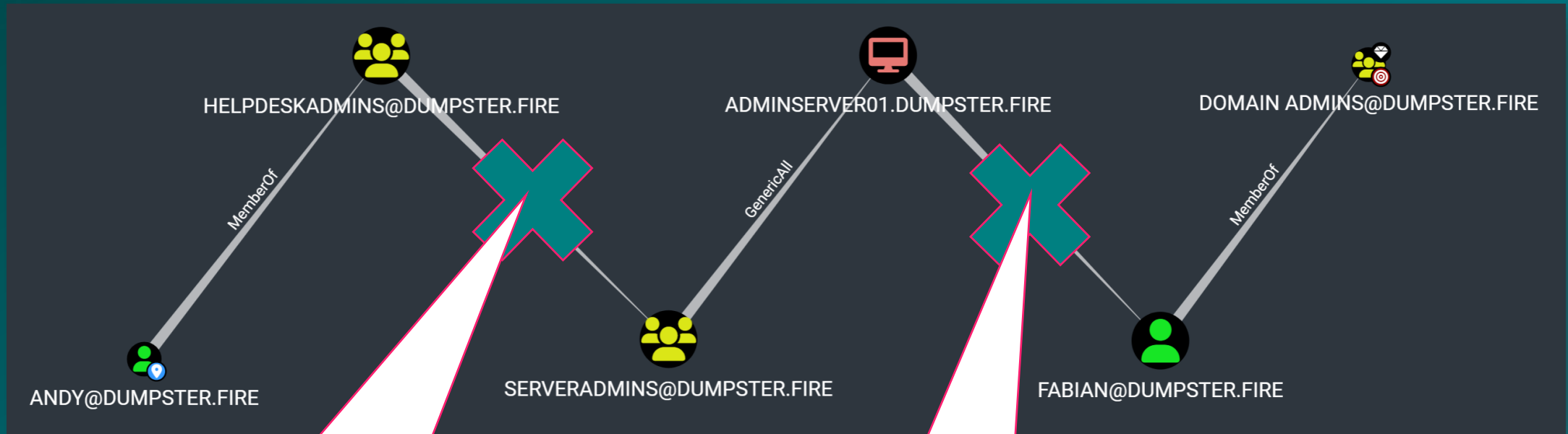


TEAL
ALWAYS CHALLENGING IT



Verification

Did the new OU structure solve the attack path?



Andy can no longer add group members to the server admins group as this group resides now in the Tier 1 groups OU

Fabian has no longer sessions on Tier 1 systems with his T0 account

- Keep monitoring the OU structure that no attack paths arise over time



TEAL
ALWAYS CHALLENGING IT

Wrap-Up and Q&A



**WE GUIDE YOU
THROUGH DANGEROUS PATHS**