Defining the Undefined:
What is Tier Zero? – Part 4

Martin Christensen, Lee Chagolla-Christensen, Jonas Bülow Knudsen

ghst.ly/novlive-tw

SPECTEROPS

Release Recap

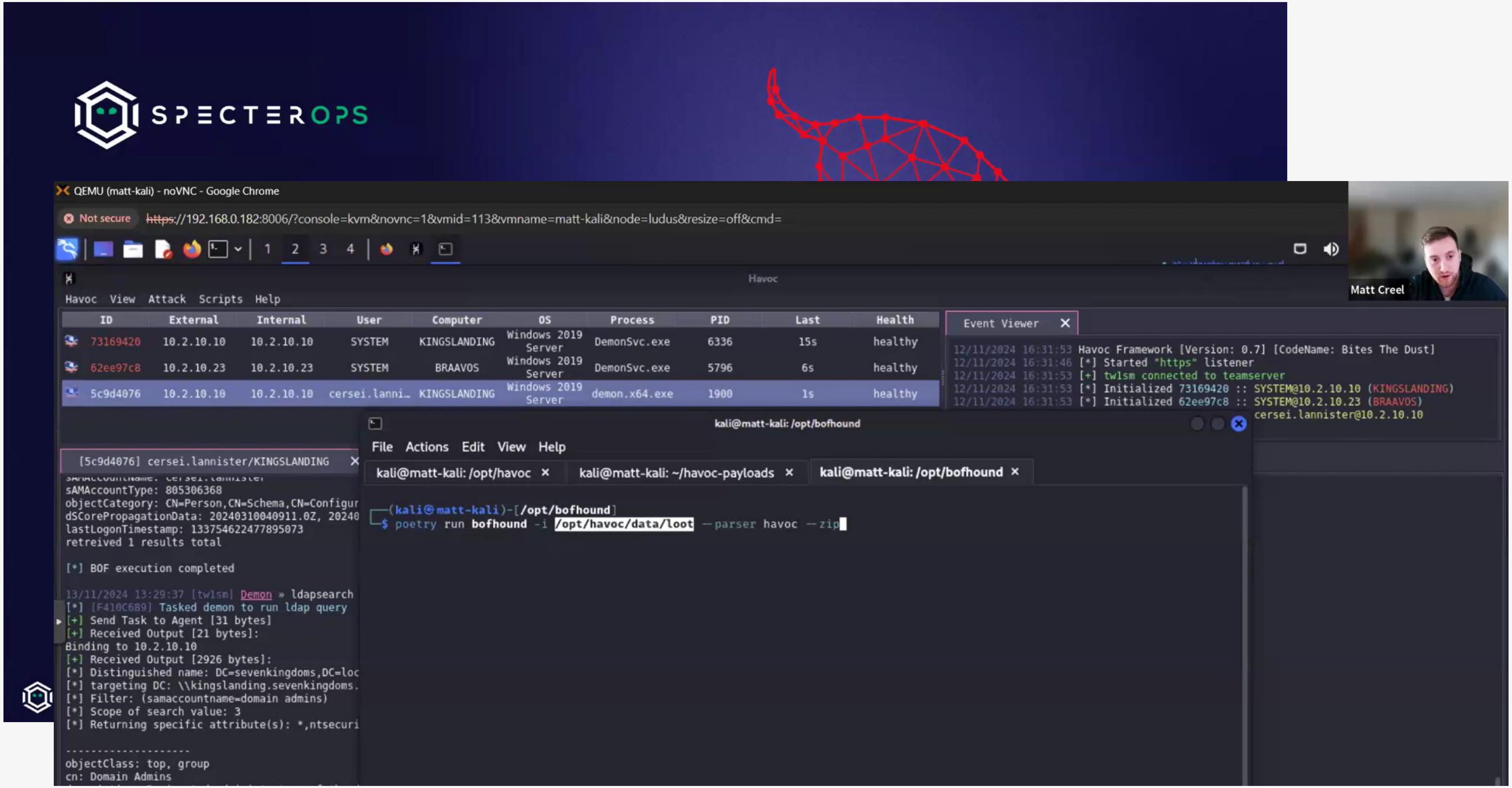
November 2024

BLOODHOUND
COMMUNITY EDITION

BLOODHOUND
ENTERPRISE

SPECTEROPS

ghst.ly/novlive-tw


SPECTEROPS
QEMU (matt-kali) - noVNC - Google Chrome
Not secure
~~https~~://192.168.0.182:8006/?console=kvm&novnc=1&vmid=113&vmname=matt-kali&node=ludus&resize=off&cmd=
1
2
3
4
Havoc
Havoc
View
Attack
Scripts
Help
Event Viewer
Matt Creel

ID	External	Internal	User	Computer	OS	Process	PID	Last	Health
73169420	10.2.10.10	10.2.10.10	SYSTEM	KINGSLANDING	Windows 2019 Server	DemonSvc.exe	6336	15s	healthy
62ee97c8	10.2.10.23	10.2.10.23	SYSTEM	BRAAVOS	Windows 2019 Server	DemonSvc.exe	5796	6s	healthy
5c9d4076	10.2.10.10	10.2.10.10	cersei.lanni…	KINGSLANDING	Windows 2019 Server	demon.x64.exe	1900	1s	healthy

```
12/11/2024 16:31:53 Havoc Framework [Version: 0.7] [CodeName: Bites The Dust]
12/11/2024 16:31:46 [*] Started "https" listener
12/11/2024 16:31:53 [+] twlsm connected to teamserver
12/11/2024 16:31:53 [*] Initialized 73169420 :: SYSTEM@10.2.10.10 (KINGSLANDING)
12/11/2024 16:31:53 [*] Initialized 62ee97c8 :: SYSTEM@10.2.10.23 (BRAAVOS)
                                                  cersei.lannister@10.2.10.10
```

[5c9d4076] cersei.lannister/KINGSLANDING

```
sAMAccountName: cersei.lannister
sAMAccountType: 805306368
objectCategory: CN=Person,CN=Schema,CN=Configur
dSCorePropagationData: 20240310040911.0Z, 20240
lastLogonTimestamp: 133754622477895073
retreived 1 results total

[*] BOF execution completed

13/11/2024 13:29:37 [twlsm] Demon » ldapsearch
[*] [F410C689] Tasked demon to run ldap query
[+] Send Task to Agent [31 bytes]
[+] Received Output [21 bytes]:
Binding to 10.2.10.10
[+] Received Output [2926 bytes]:
[*] Distinguished name: DC=sevenkingdoms,DC=loc
[*] targeting DC: \\kingslanding.sevenkingdoms.
[*] Filter: (samaccountname=domain admins)
[*] Scope of search value: 3
[*] Returning specific attribute(s): *,ntsecuri

--------------------
objectClass: top, group
cn: Domain Admins
```

kali@matt-kali: /opt/bofhound
File
Actions
Edit
View
Help
kali@matt-kali: /opt/havoc
kali@matt-kali: ~/havoc-payloads
kali@matt-kali: /opt/bofhound

```
┌──(kali㉿matt-kali)-[/opt/bofhound]
└─$ poetry run bofhound -i /opt/havoc/data/loot --parser havoc --zip
```

MARCH 31 – APRIL 1, 2025

CALL FOR PRESENTERS

SPECTEROPS.IO/SO-CON

Defining the Undefined:
What is Tier Zero? – Part 4

Martin Christensen, Lee Chagolla-Christensen, Jonas Bülow Knudsen

Who are we?

Martin
Sohn Christensen

Technical Account Manager

Lee
Chagolla-Christensen

Security Researcher

Jonas
Bülow Knudsen

Product Architect

Agenda

- Recap
- Community contributions
- Isolating Tier Zero - Insights from working with BloodHound Enterprise customers
- Microsoft Exchange on-prem
- Active Directory Certificate Services (ADCS)

Recap

Recap – Part 1, 2, and 3

- Part 1:
    - Our definition of Tier Zero:
      Tier Zero is a set of assets in control of enterprise identities and their security dependencies
        - *Control: A relationship that can contribute to compromising the controlled asset or impact its operability*
        - *Security dependency: A component whose security impacts another component's security*
    - Microsoft's original list of Tier Zero AD groups
    - Tier Zero Table: https://github.com/SpecterOps/TierZeroTable
- Part 2: More on-prem AD objects
- Part 3: Entra ID admin roles

Community contributions

- DnsAdmins
  - Controls DNS – relay attacks and disruption
  - Contributors: kberkheiser and Adam Przybyszewski (sludgework)
- Performance Log Users (and Distributed COM Users)
  - Permissions to activate DCOM on DCs
  - Remote compromise users logged in on DCs through a coerce + NTLM relay attack
    - https://decoder.cloud/2024/04/24/hello-im-your-domain-admin-and-i-want-to-authenticate-against-you/
  - Contributor: Andrea Pierini (decoder)

Isolating Tier Zero

Insights from working with BloodHound Enterprise customers

Tiering at different scales

- Tiering is for everyone - small to very large
  - Woodside, leading Australian natural gas producer, ~5 000 employees
  - HEMA, leading Dutch retailer, ~17 000 employees
  - Global top-5 car company

- Technical Account Manager = BloodHound expertise and tiering guidance

BloodHound Enterprise case studies: https://specterops.io/spec-resources/#case-studies

Challenges

- Stakeholder Investment
- Classify Tier Zero
- Identify Violations
- Quantify Risk & Know Your Unknowns
- Usable Tiering & Continuous Audit

Stakeholder Investment

- Tiering = significant effort (design, implement, operationalize, sustain)

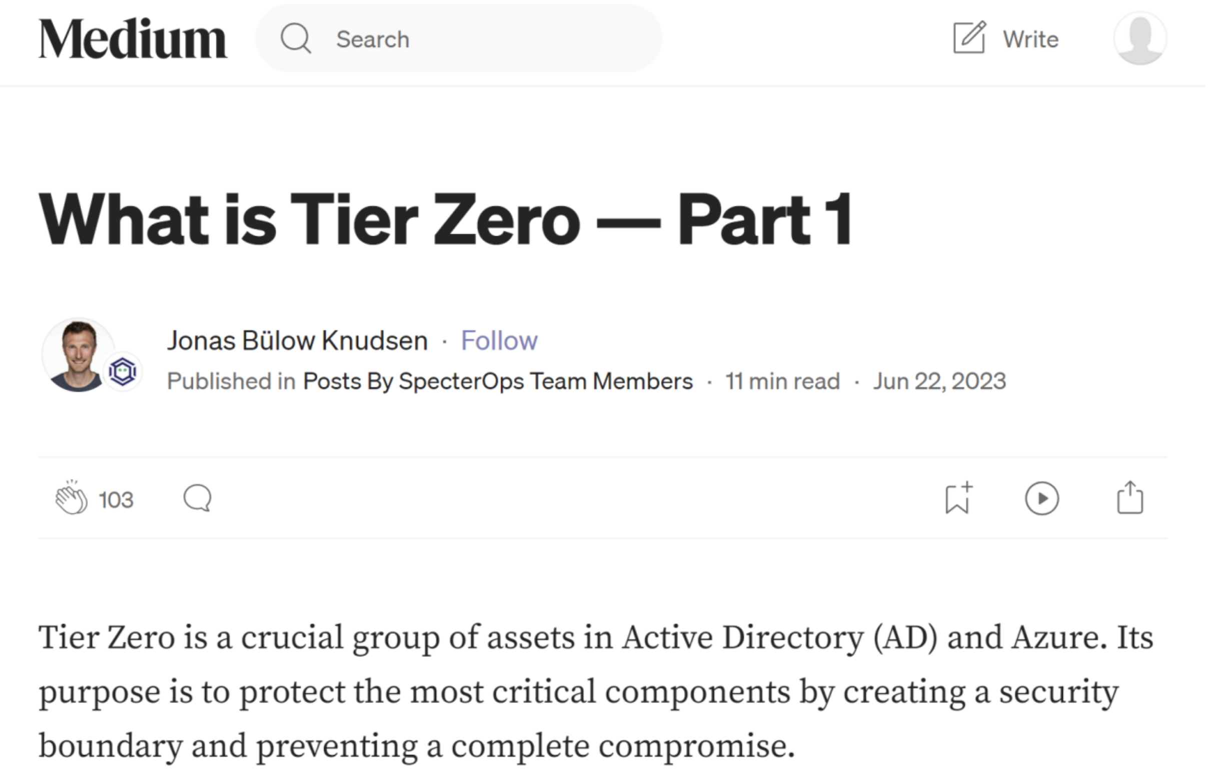
- Security organizations must “think in graphs”
  - Top-level support & make tiering a security policy
  - Security and Infrastructure must collaborate

- Sell the concept of tiering
  - What does every pentest reveal?
  - Assess your Tier Zero attack paths – at least just implement Tier Zero

Classify Tier Zero

- We gave you the definition, now you classify YOUR Tier Zero
    - BloodHound does a lot for you: Groups, GPOs, OUs, etc.

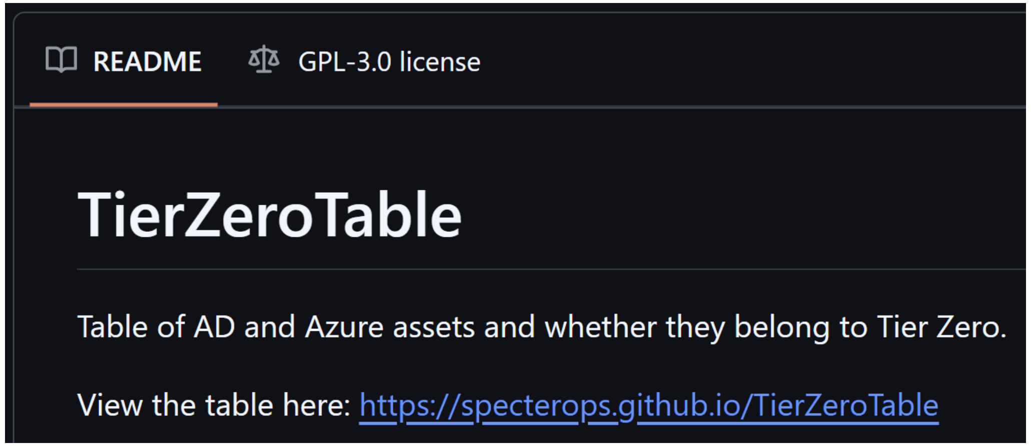
- Audit Tier Zero Memberships
    - *“Is that Tier Zero service account following the principle of least privilege?”*



What is Tier Zero — Part 1

Jonas Bülow Knudsen · Follow
Published in Posts By SpecterOps Team Members · 11 min read · Jun 22, 2023

Tier Zero is a crucial group of assets in Active Directory (AD) and Azure. Its purpose is to protect the most critical components by creating a security boundary and preventing a complete compromise.

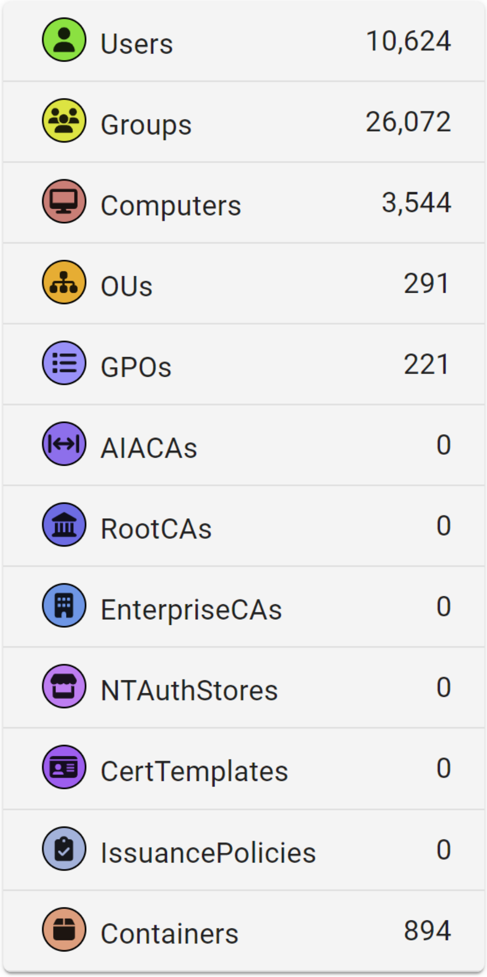


TierZeroTable

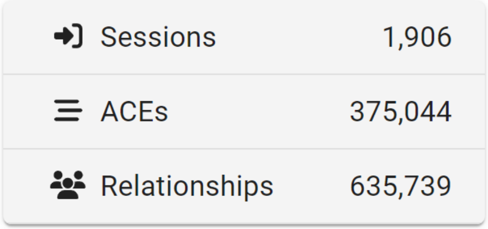
Table of AD and Azure assets and whether they belong to Tier Zero.

View the table here: https://specterops.github.io/TierZeroTable

Identify Violations



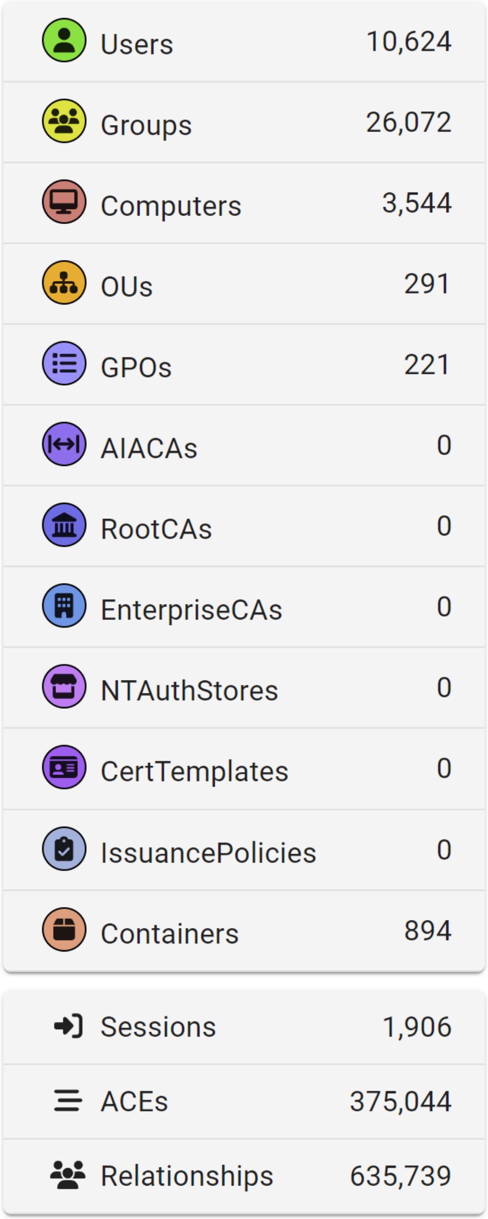
Users	10,624
Groups	26,072
Computers	3,544
OUs	291
GPOs	221
AIACAs	0
RootCAs	0
EnterpriseCAs	0
NTAuthStores	0
CertTemplates	0
IssuancePolicies	0
Containers	894



Sessions	1,906
ACEs	375,044
Relationships	635,739

Identify Violations

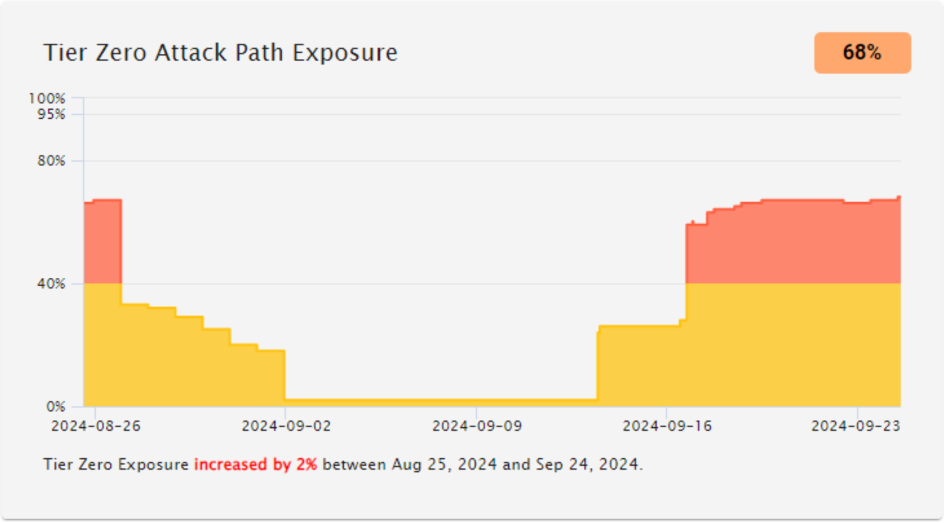
- *“Which of our 635 739 relationships are tiering violations?”*
- All onboarded customers have violations
- Attack Path Management must be a strategic approach
- The graph (i.e., BloodHound) can solve the problem



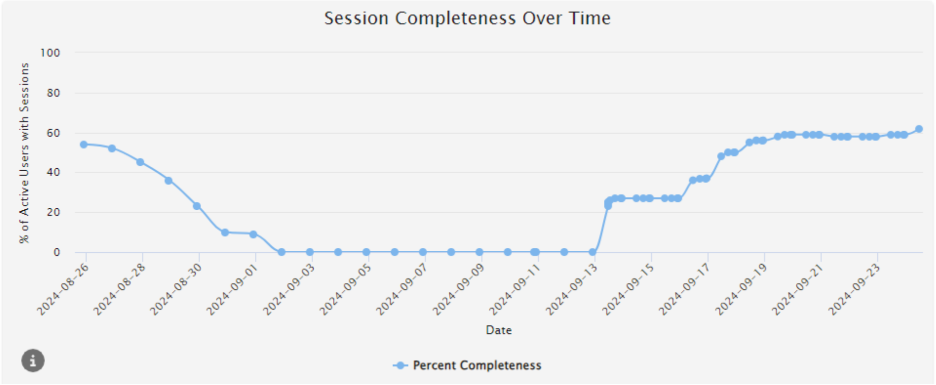
Users	10,624
Groups	26,072
Computers	3,544
OUs	291
GPOs	221
AIACAs	0
RootCAs	0
EnterpriseCAs	0
NTAuthStores	0
CertTemplates	0
IssuancePolicies	0
Containers	894
Sessions	1,906
ACEs	375,044
Relationships	635,739

Quantify Risk & Knowing Your Unknowns

- Increase Graph Visibility = Increase Known Risk
- Ensure collection of all data types
  - Logon Sessions, Local Group Memberships, User Rights Assignments, DC Registry, CA Registry
- Did you miss anything?
  - Where are the DC backups?
  - Which key vaults store Tier Zero credentials?



Tier Zero Exposure increased by 2% between Aug 25, 2024 and Sep 24, 2024.



Usable Tiering & Continuous Audit

- *“Security at the expense of usability, comes at the expense of security”*
  - Example: Logon restrictions in place; admin created an exception and logged in at a critical point…

Continuous Audit

Usability expense = Security expense

- Industry changes, security now has more usability… but also new risks
  - Example: PAM rotates passwords.. but now PAM is Tier Zero and added complexity

- Risk Management Approach
  - Example: Accept clean source violation (no PAW) and reduce risk with MFA – risk of screen capture, keylogging, session hijack, MFA bypass, …

Microsoft Exchange on-prem

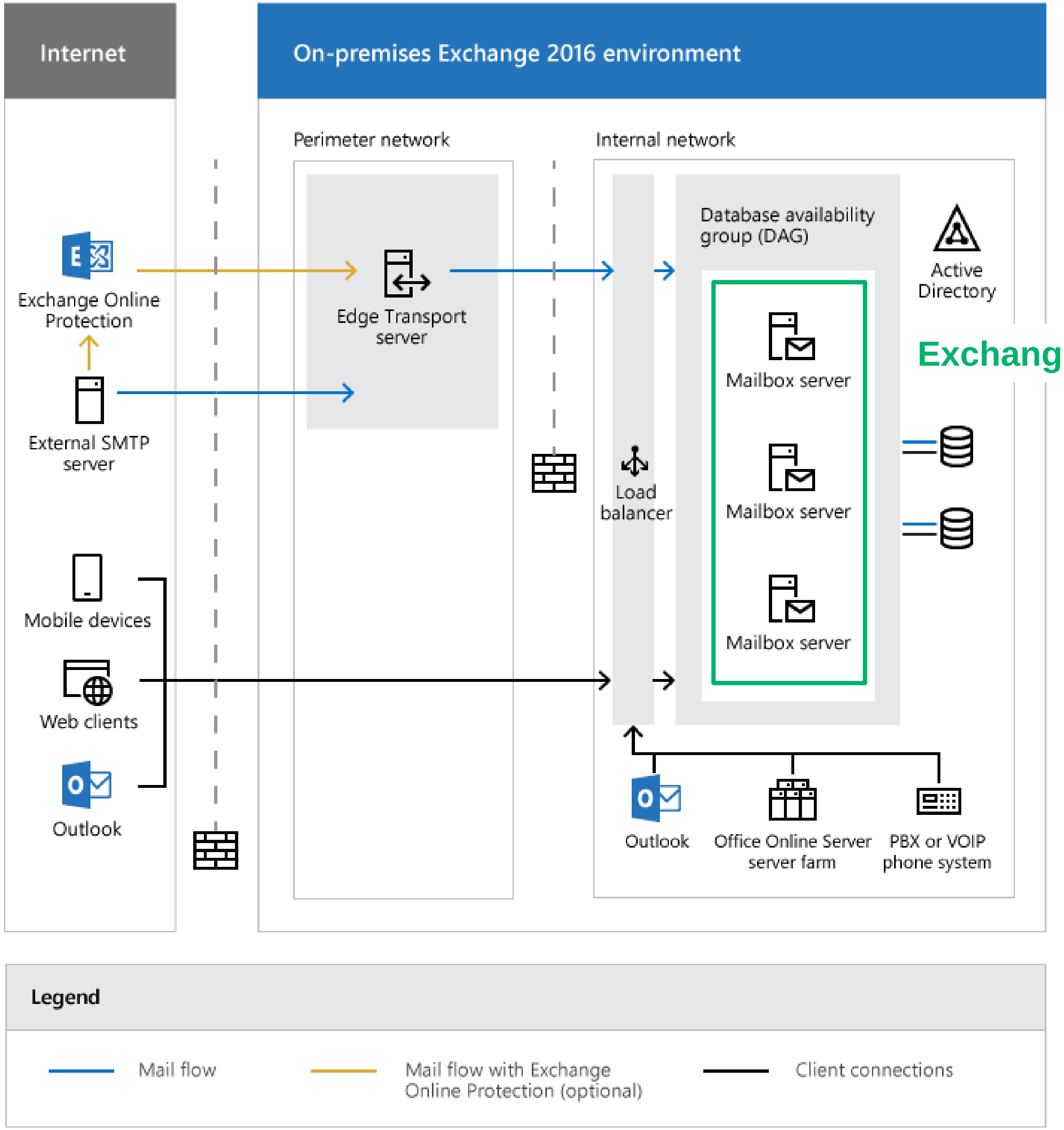
Microsoft Exchange on-prem

- On-prem (or hybrid) solution for communication
    - Email, calendar, contacts, and tasks

- Should not be a Tier Zero security dependency

- .. but has it control over Tier Zero?

- We need to understand:
    - What are the Exchange components
    - Do the components have Tier Zero control



Internet

On-premises Exchange 2016 environment

Perimeter network

Internal network

Exchange Online Protection

External SMTP server

Edge Transport server

Load balancer

Database availability group (DAG)

Mailbox server

Mailbox server

Mailbox server

Active Directory

Mobile devices

Web clients

Outlook

Outlook

Office Online Server server farm

PBX or VOIP phone system

Legend

Mail flow

Mail flow with Exchange Online Protection (optional)

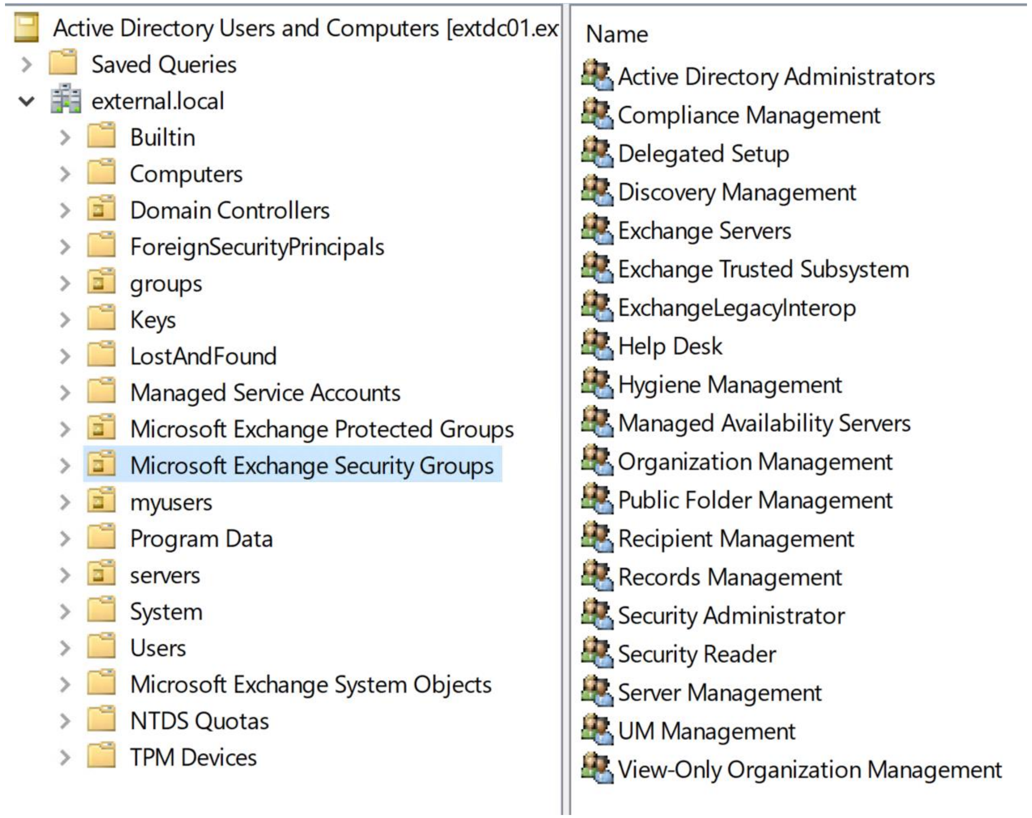
Client connections

Exchange servers

Microsoft Exchange on-prem components

- Components (we care about)
  - Exchange servers (mailbox servers)
  - AD groups

- What permissions do the components have in AD?



Active Directory Users and Computers [extdc01.ex
- Saved Queries
- external.local
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - groups
  - Keys
  - LostAndFound
  - Managed Service Accounts
  - Microsoft Exchange Protected Groups
  - Microsoft Exchange Security Groups
  - myusers
  - Program Data
  - servers
  - System
  - Users
  - Microsoft Exchange System Objects
  - NTDS Quotas
  - TPM Devices

Name
- Active Directory Administrators
- Compliance Management
- Delegated Setup
- Discovery Management
- Exchange Servers
- Exchange Trusted Subsystem
- ExchangeLegacyInterop
- Help Desk
- Hygiene Management
- Managed Availability Servers
- Organization Management
- Public Folder Management
- Recipient Management
- Records Management
- Security Administrator
- Security Reader
- Server Management
- UM Management
- View-Only Organization Management

Microsoft Exchange on-prem components

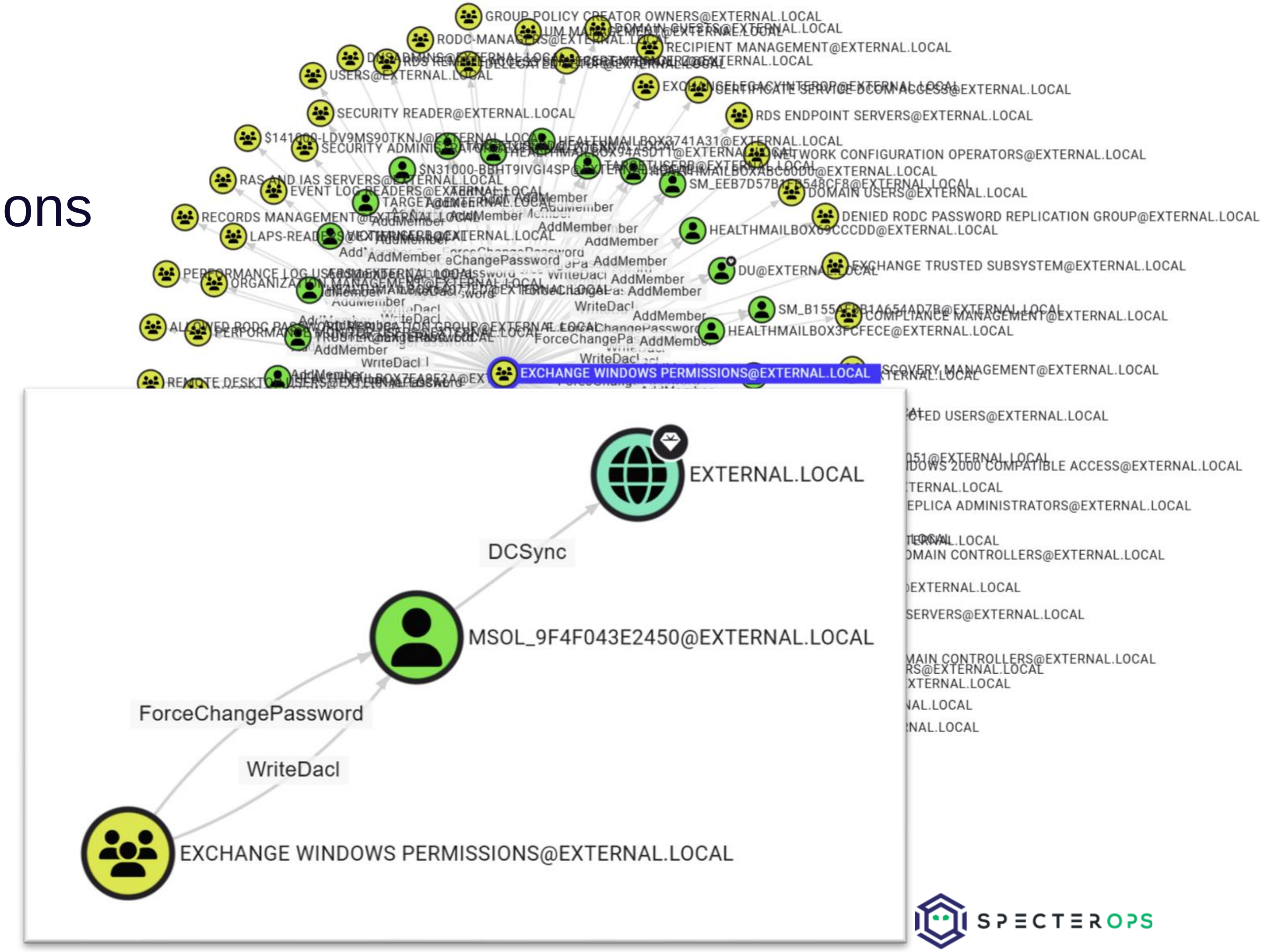
- What permissions do the components have in AD?

- Depends on the Exchange permission model:
    1. Shared permission model (default)
    2. Role-Based Access Control (RBAC) split permissions model
    3. AD split permissions model

- Approach: Deploy each model and audit permissions

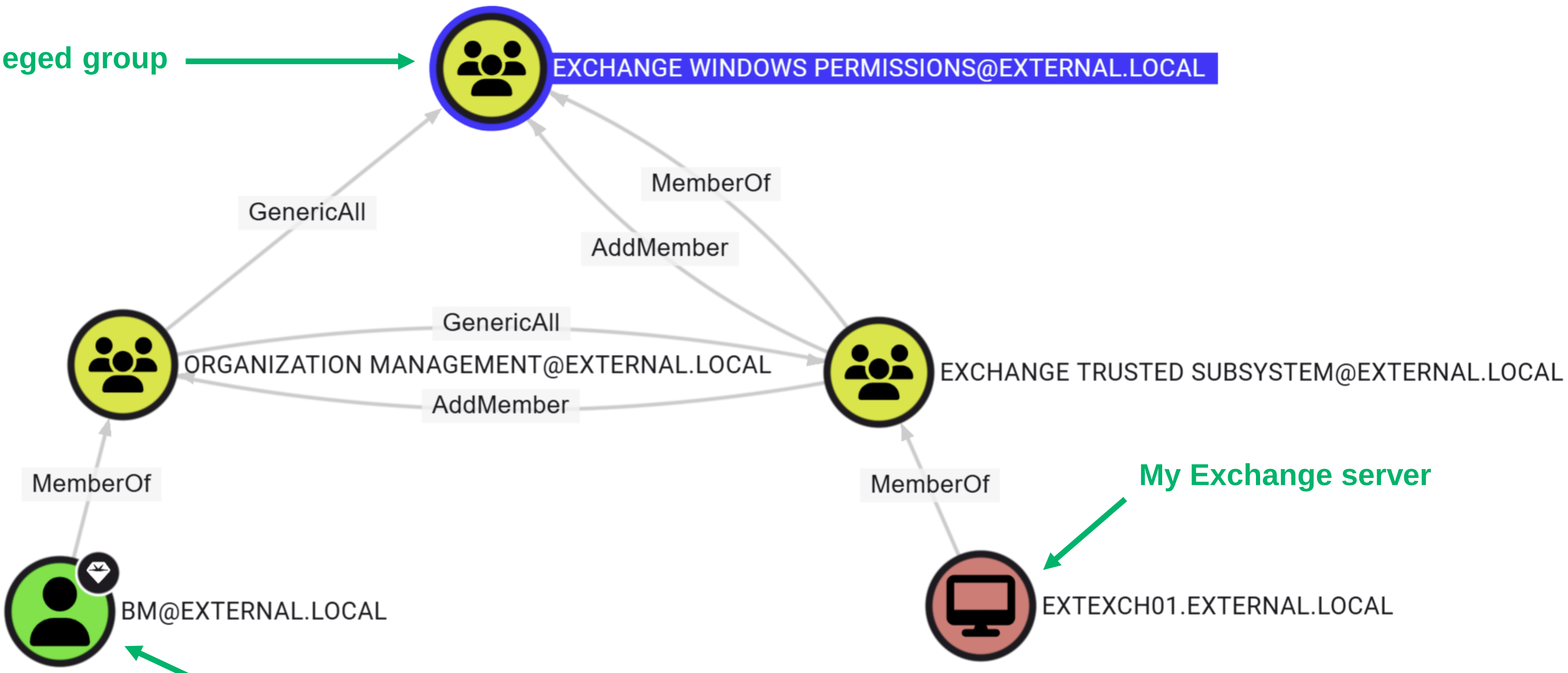
Shared permission model (default)

- BloodHound analysis
- Exchange Windows Permissions (group) has outbound control
- ACEs on domain object:
  - Users: ForceChangePassword, WriteDacl
  - Groups: AddMember
- Who controls this group?



GROUP POLICY CREATOR OWNERS@EXTERNAL.LOCAL
RODC-MANAGERS@EXTERNAL.LOCAL
RECIPIENT MANAGEMENT@EXTERNAL.LOCAL
USERS@EXTERNAL.LOCAL
SECURITY READER@EXTERNAL.LOCAL
RDS ENDPOINT SERVERS@EXTERNAL.LOCAL
NETWORK CONFIGURATION OPERATORS@EXTERNAL.LOCAL
DOMAIN USERS@EXTERNAL.LOCAL
DENIED RODC PASSWORD REPLICATION GROUP@EXTERNAL.LOCAL
RECORDS MANAGEMENT@EXTERNAL.LOCAL
HEALTHMAILBOX69CCCDD@EXTERNAL.LOCAL
EXCHANGE TRUSTED SUBSYSTEM@EXTERNAL.LOCAL
COMPLIANCE MANAGEMENT@EXTERNAL.LOCAL
HEALTHMAILBOX3FCFECE@EXTERNAL.LOCAL
EXCHANGE WINDOWS PERMISSIONS@EXTERNAL.LOCAL
DISCOVERY MANAGEMENT@EXTERNAL.LOCAL
AddMember
ForceChangePassword
WriteDacl
EXTERNAL.LOCAL
DCSync
MSOL_9F4F043E2450@EXTERNAL.LOCAL
ForceChangePassword
WriteDacl
EXCHANGE WINDOWS PERMISSIONS@EXTERNAL.LOCAL

Shared permission model (default)


EXCHANGE WINDOWS PERMISSIONS@EXTERNAL.LOCAL
GenericAll
MemberOf
AddMember
GenericAll
ORGANIZATION MANAGEMENT@EXTERNAL.LOCAL
EXCHANGE TRUSTED SUBSYSTEM@EXTERNAL.LOCAL
AddMember
MemberOf
MemberOf
BM@EXTERNAL.LOCAL
EXTEXCH01.EXTERNAL.LOCAL

The privileged group

My Exchange server

My Exchange admin

Shared permission model (default)

- Components with Tier Zero control:
  - Exchange Windows Permissions (group)
- Indirect controllers:
  - Organization Management (group)
  - Exchange Trusted Subsystem (group)
  - Exchange servers
  - Exchange admins
- Tier Zero control removable: Disable ACL inheritance from domain on Tier Zero objects

Shared model

Tier Zero security dependency: ✗

Tier Zero control: ✓

Tier Zero control removable: ✓

Exchange permission models

Shared model

Tier Zero security dependency: ✗

Tier Zero control: ✓

Tier Zero control removable: ✓

RBAC split model

Tier Zero security dependency: ?

Tier Zero control: ?

Tier Zero control removable: ?

AD split model

Tier Zero security dependency: ?

Tier Zero control: ?

Tier Zero control removable: ?

RBAC split permissions model

- Microsoft recommended model
- Better options for delegating limited control in Exchange RBAC
- AD permissions analysis: Same as shared model!
- Split permissions in Exchange RBAC (not in AD!)

Exchange shared model AD attack paths
Exchange RBAC split model AD attack paths
Corporate needs you to find the differences between this picture and this picture.
They're the same picture.

Exchange permission models

Shared model

Tier Zero security dependency:	✗
Tier Zero control:	✓
Tier Zero control removable:	✓

RBAC split model

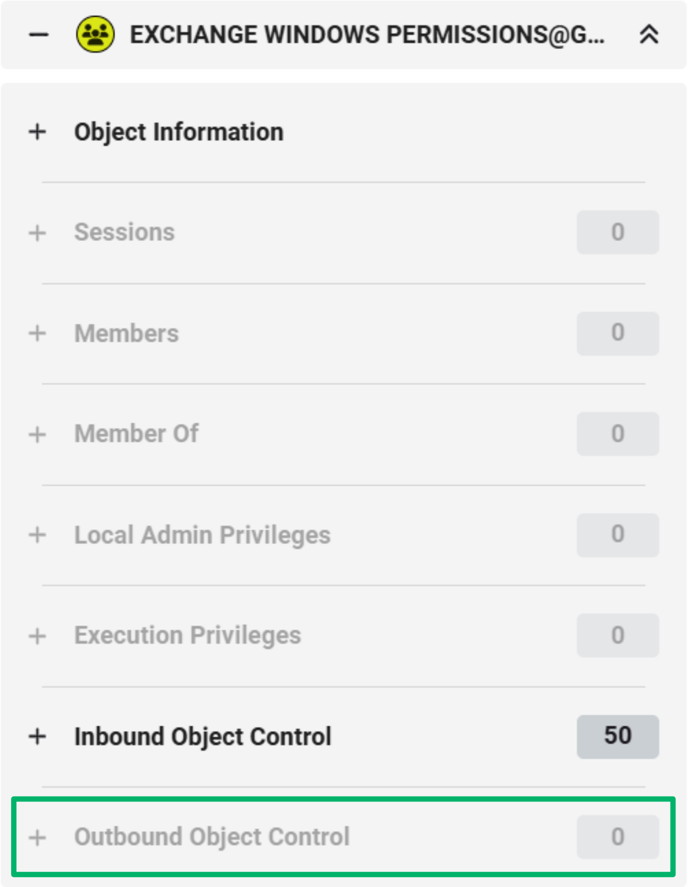
Tier Zero security dependency:	✗
Tier Zero control:	✓
Tier Zero control removable:	✓

AD split model

Tier Zero security dependency:	?
Tier Zero control:	?
Tier Zero control removable:	?

AD split permissions model

- Exchange Windows Permissions edges: Gone!
- Exchange now has limited write access in AD
- Admin challenge:
  Grant the necessary permissions in AD



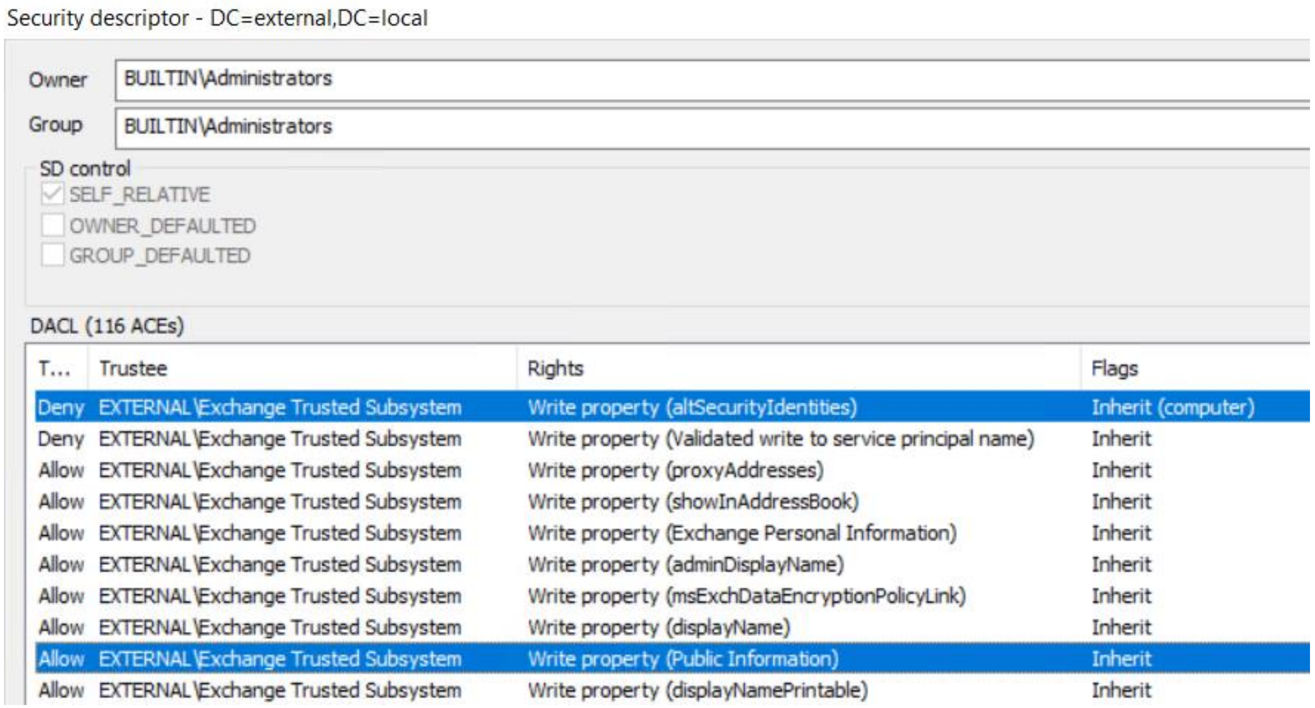
EXCHANGE WINDOWS PERMISSIONS@G...

Object Information	
Sessions	0
Members	0
Member Of	0
Local Admin Privileges	0
Execution Privileges	0
Inbound Object Control	50
Outbound Object Control	0

https://www.teal-consulting.de/en/2023/05/15/exchange-split-permission/

AD split permissions model

- BloodHound does not capture everything
- Exchange Trusted Subsystem (group) has Write Public-Information on users
  - ACE on domain object
  - Includes Alt-Security-Identities attribute
  - Attack: ESC14 Scenario A



Security descriptor - DC=external,DC=local

Owner: BUILTIN\Administrators

Group: BUILTIN\Administrators

SD control

☑ SELF_RELATIVE
□ OWNER_DEFAULTED
□ GROUP_DEFAULTED

DACL (116 ACEs)

T...	Trustee	Rights	Flags
Deny	EXTERNAL\Exchange Trusted Subsystem	Write property (altSecurityIdentities)	Inherit (computer)
Deny	EXTERNAL\Exchange Trusted Subsystem	Write property (Validated write to service principal name)	Inherit
Allow	EXTERNAL\Exchange Trusted Subsystem	Write property (proxyAddresses)	Inherit
Allow	EXTERNAL\Exchange Trusted Subsystem	Write property (showInAddressBook)	Inherit
Allow	EXTERNAL\Exchange Trusted Subsystem	Write property (Exchange Personal Information)	Inherit
Allow	EXTERNAL\Exchange Trusted Subsystem	Write property (adminDisplayName)	Inherit
Allow	EXTERNAL\Exchange Trusted Subsystem	Write property (msExchDataEncryptionPolicyLink)	Inherit
Allow	EXTERNAL\Exchange Trusted Subsystem	Write property (displayName)	Inherit
Allow	EXTERNAL\Exchange Trusted Subsystem	Write property (Public Information)	Inherit
Allow	EXTERNAL\Exchange Trusted Subsystem	Write property (displayNamePrintable)	Inherit

Exchange permission models

Shared model

Tier Zero security dependency:	✗
Tier Zero control:	✓
Tier Zero control removable:	✓

RBAC split model

Tier Zero security dependency:	✗
Tier Zero control:	✓
Tier Zero control removable:	✓

AD split model

Tier Zero security dependency:	✗
Tier Zero control:	✓
Tier Zero control removable:	✓

Microsoft Exchange on-prem - Summary

- Exchange components with Tier Zero control:
  - Exchange Windows Permissions – direct (except in AD split model)
  - Exchange Trusted Subsystem – direct
  - Organization Management – indirect
  - Exchange servers – indirect
  - Exchange admins – indirect
- Are the above components Tier Zero?
  - Yes, unless all Tier Zero users and groups are protected against ACL inheritance from the domain
- Microsoft's take: Exchange is typically Tier Zero

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-security-levels#privileged

Active Directory Certificate Services

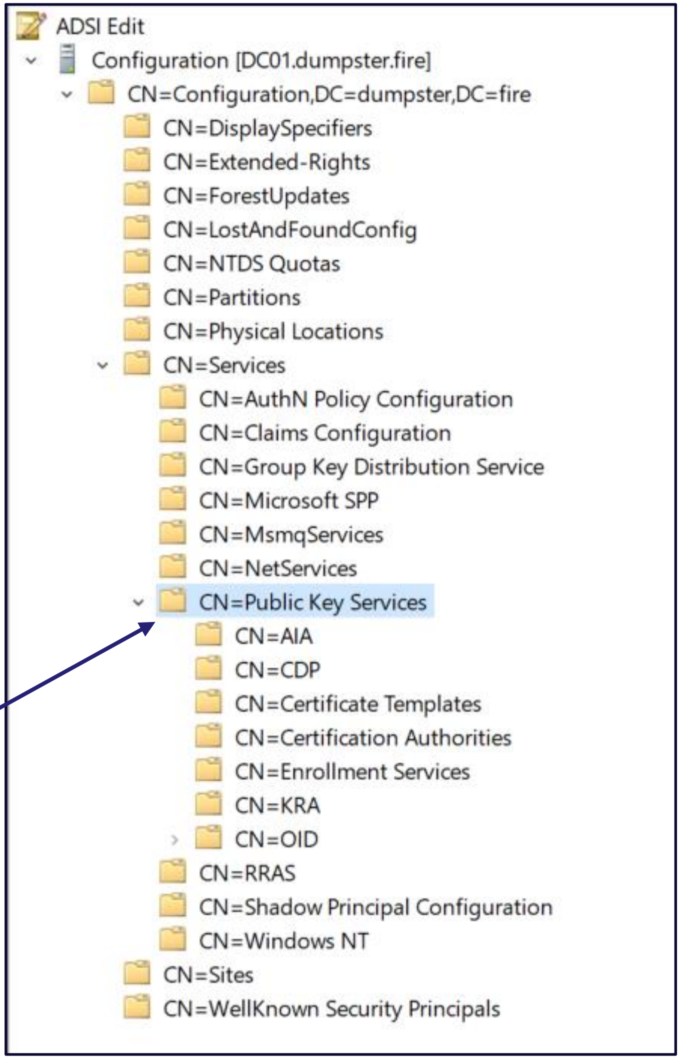
Active Directory Certificate Services (ADCS)

- Microsoft’s Public Key Infrastructure (PKI) solution for Windows environments

- Issues and manages digital certificates
  - Example uses include SSL/TLS certificates, email digital signatures, code signing, and **authentication**

- Largely configured inside of Active Directory
  - See the Public Key Services container

- Old!!! First parts released in Windows Server 2000



```
ADSI Edit
  ⌄ Configuration [DC01.dumpster.fire]
    ⌄ CN=Configuration,DC=dumpster,DC=fire
        CN=DisplaySpecifiers
        CN=Extended-Rights
        CN=ForestUpdates
        CN=LostAndFoundConfig
        CN=NTDS Quotas
        CN=Partitions
        CN=Physical Locations
      ⌄ CN=Services
          CN=AuthN Policy Configuration
          CN=Claims Configuration
          CN=Group Key Distribution Service
          CN=Microsoft SPP
          CN=MsmqServices
          CN=NetServices
        ⌄ CN=Public Key Services
            CN=AIA
            CN=CDP
            CN=Certificate Templates
            CN=Certification Authorities
            CN=Enrollment Services
            CN=KRA
          › CN=OID
          CN=RRAS
          CN=Shadow Principal Configuration
          CN=Windows NT
        CN=Sites
        CN=WellKnown Security Principals
```

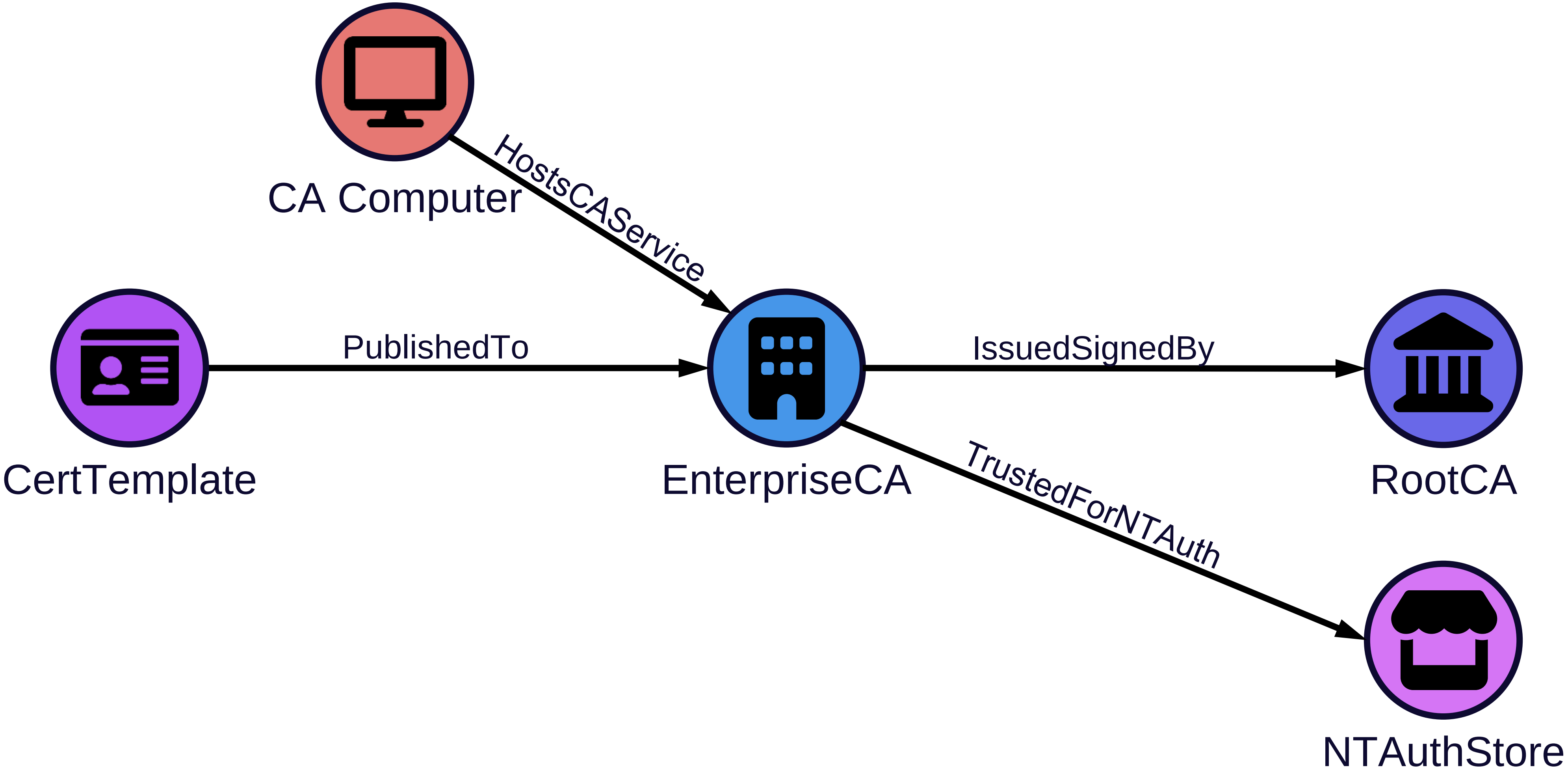
Active Directory Certificate Services (ADCS)

- 2021: Certified Pre-Owned ADCS whitepaper
  - Eight domain escalation techniques (ESC1 - ESC8)
  - AD CS persistence techniques
  - Detection guidance

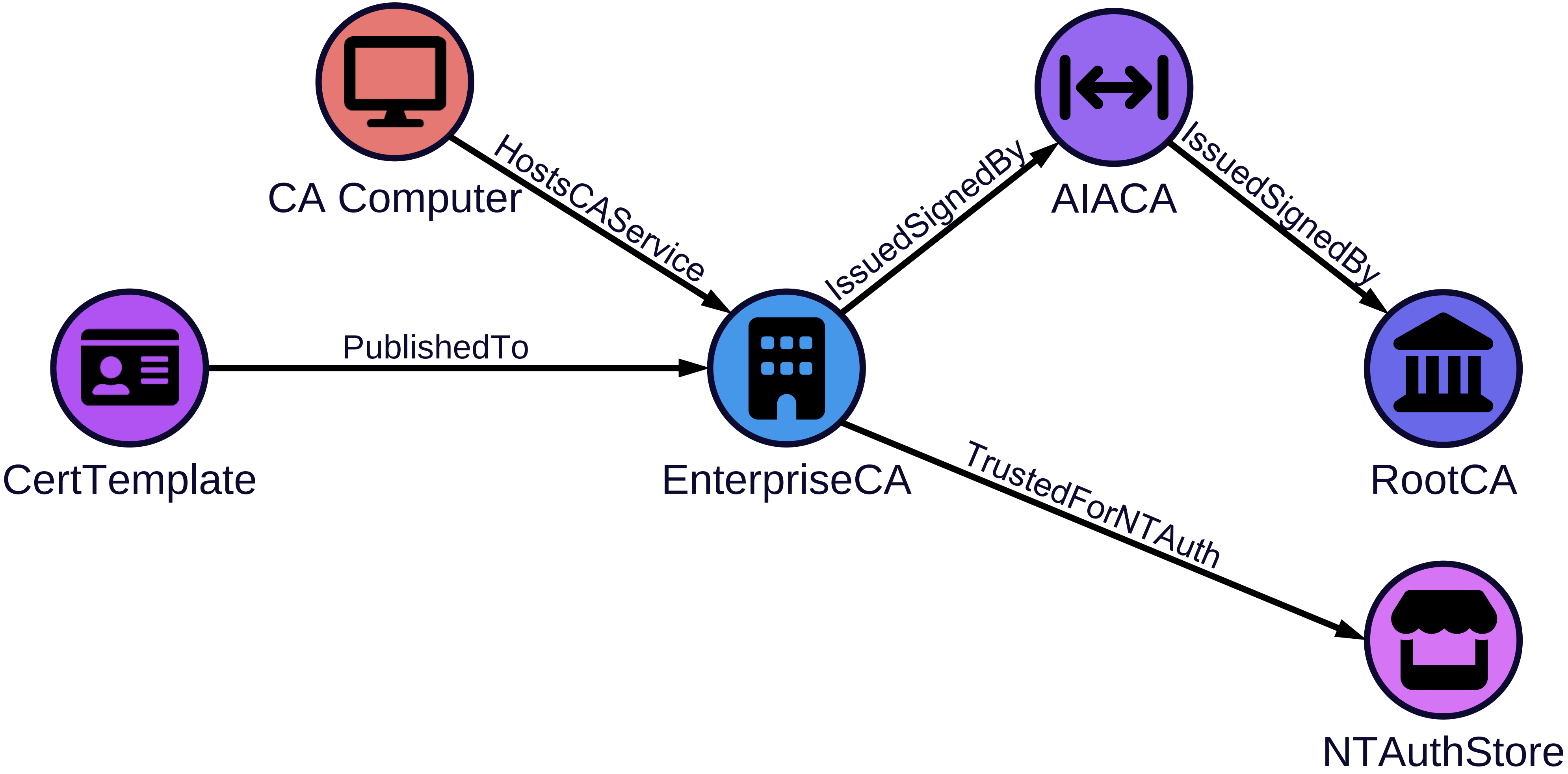
- Since then
  - ***MANY*** full forest compromises on our assessments (and by threat actors 😬)
  - More escalation techniques (ESC9 - ESC15)
  - Several CVEs and resulting changes in AD
  - Limited security improvements in ADCS itself

https://posts.specterops.io/certified-pre-owned-d95910965cd2

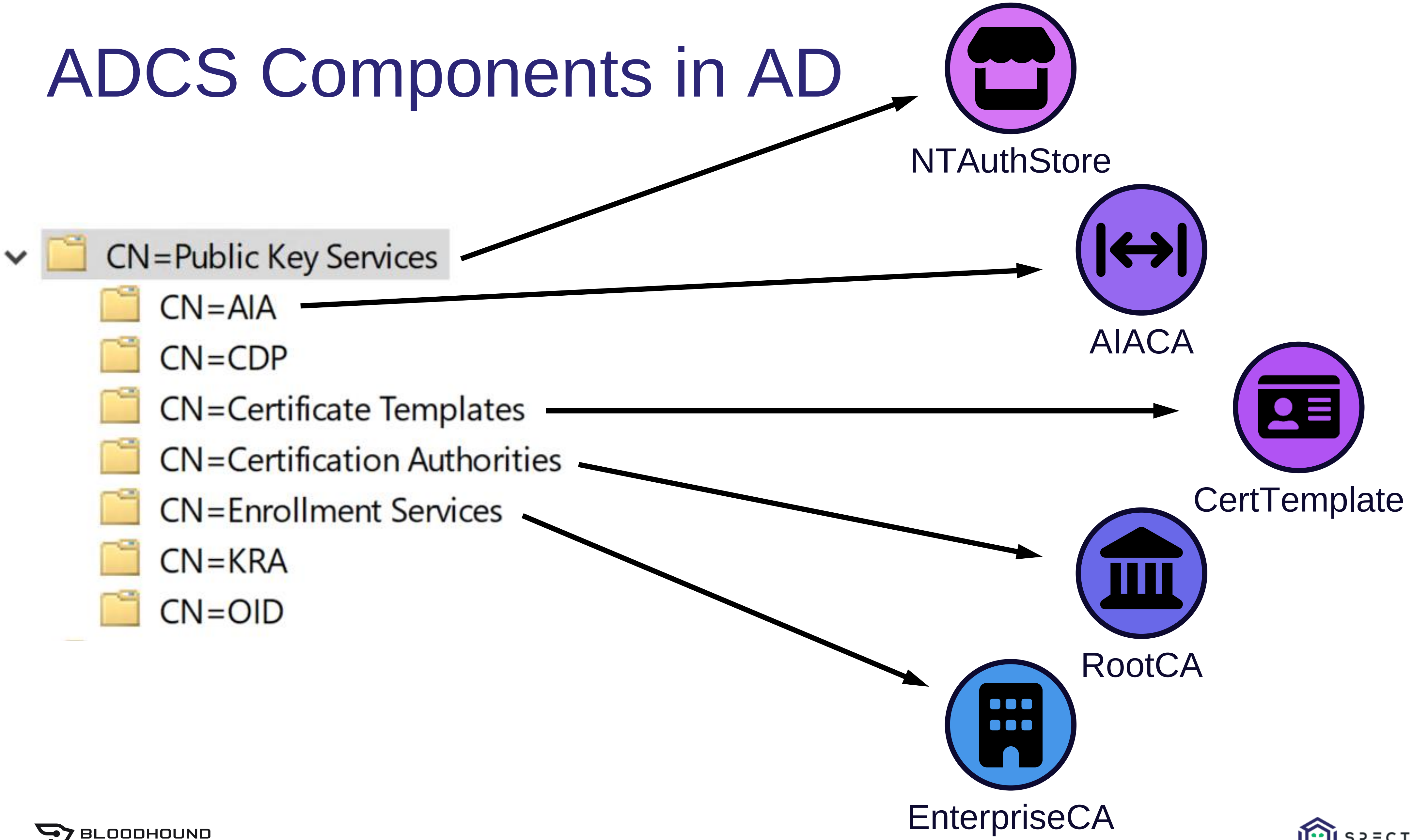
ADCS Components



ADCS Components



ADCS Components in AD



- CN=Public Key Services
  - CN=AIA
  - CN=CDP
  - CN=Certificate Templates
  - CN=Certification Authorities
  - CN=Enrollment Services
  - CN=KRA
  - CN=OID

ESC1 Cert Template

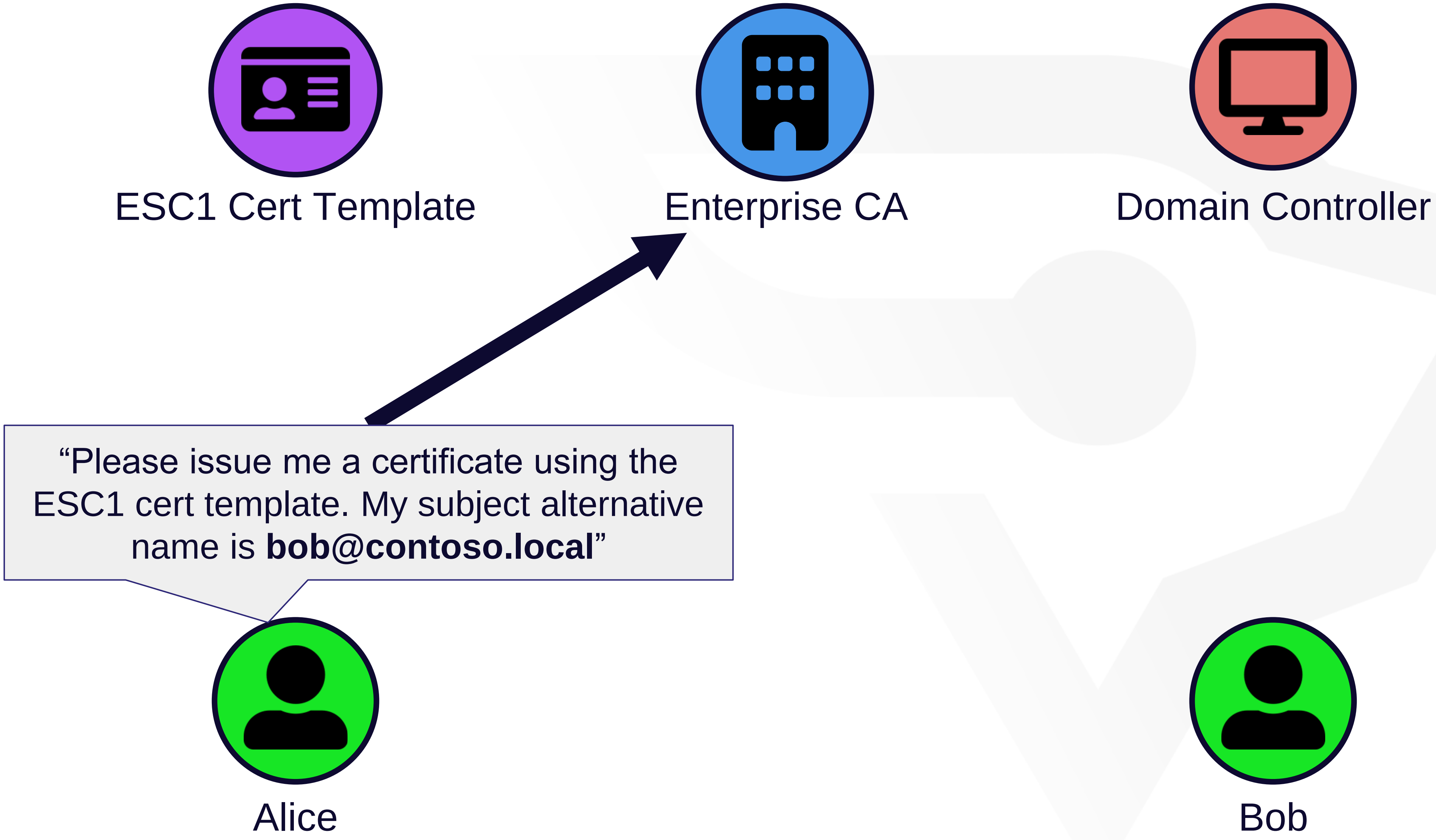
Enterprise CA

Domain Controller

ADCS Abuse Example: ESC1

Alice

Bob



ESC1 Cert Template

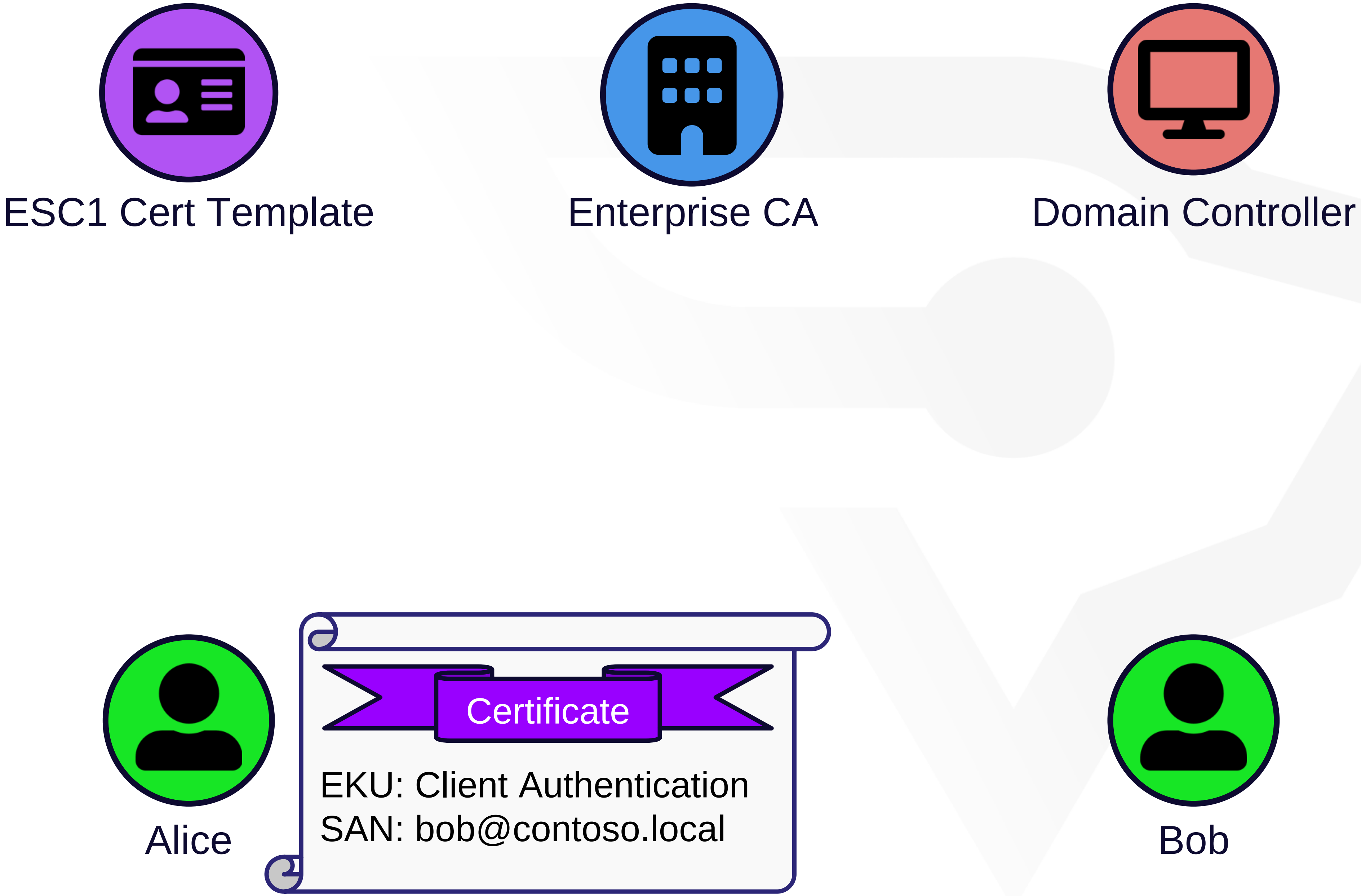
Enterprise CA

Domain Controller

“Please issue me a certificate using the ESC1 cert template. My subject alternative name is **bob@contoso.local**”

Alice

Bob



ESC1 Cert Template

Enterprise CA

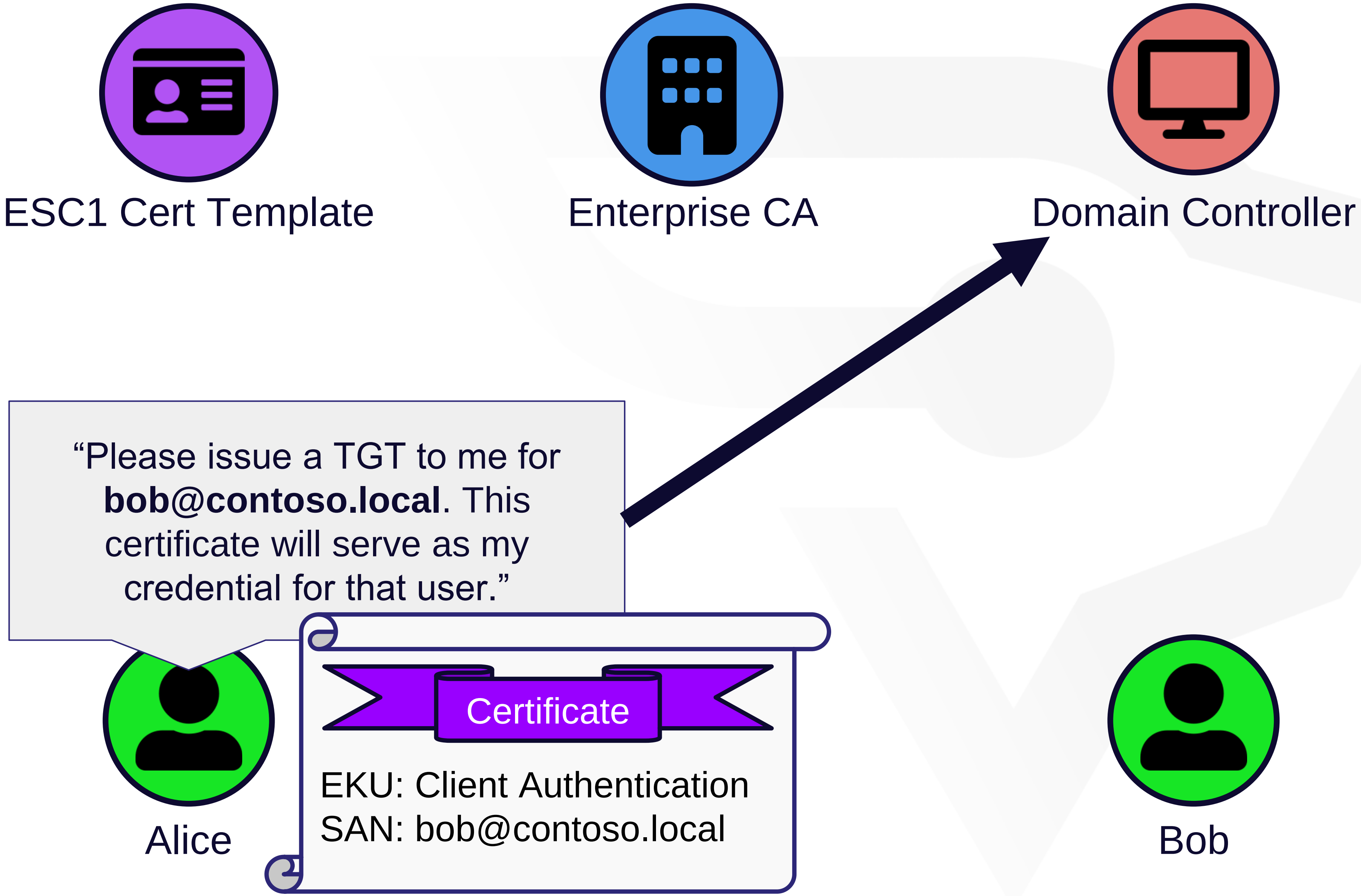
Domain Controller

Alice

Certificate

EKU: Client Authentication
SAN: bob@contoso.local

Bob



ESC1 Cert Template

Enterprise CA

Domain Controller

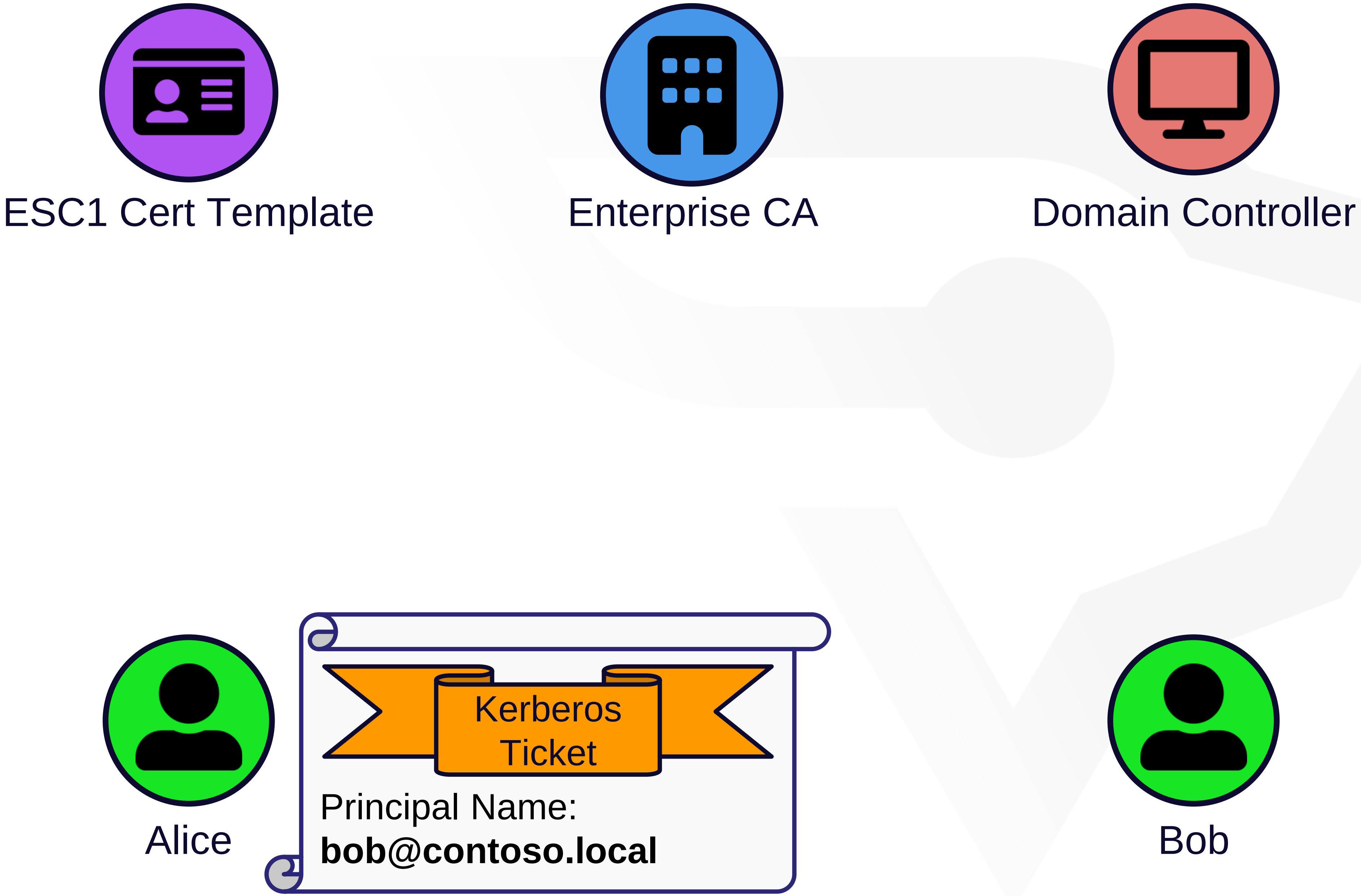
“Please issue a TGT to me for **bob@contoso.local**. This certificate will serve as my credential for that user.”

Certificate

EKU: Client Authentication
SAN: bob@contoso.local

Alice

Bob



ESC1 Cert Template

Enterprise CA

Domain Controller

Alice

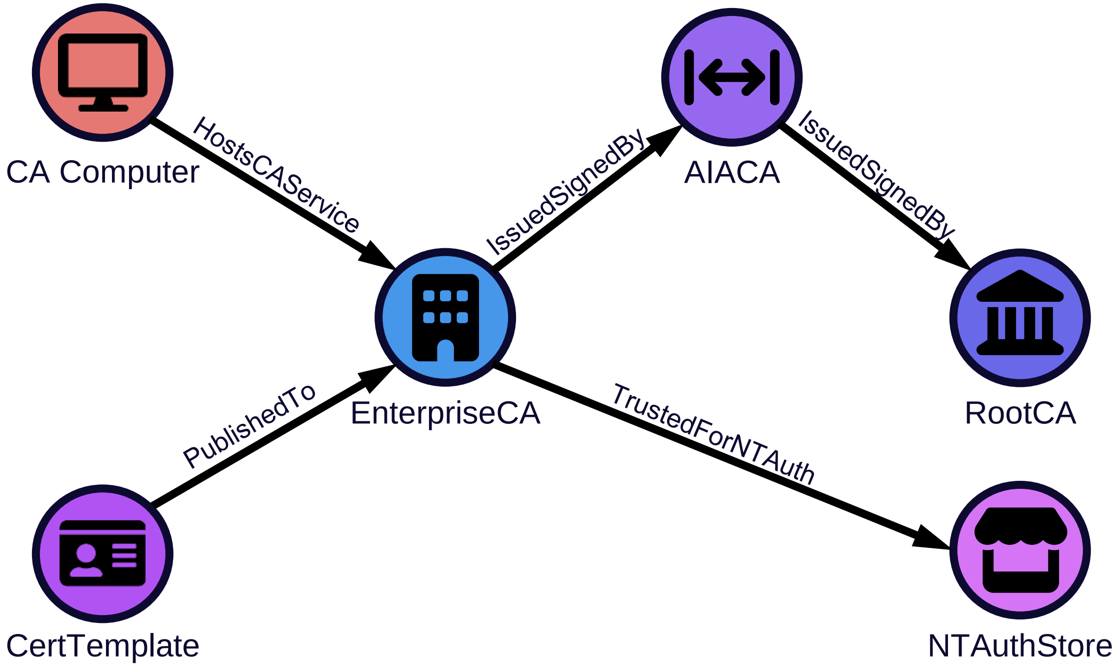
Kerberos Ticket

Principal Name:
bob@contoso.local

Bob

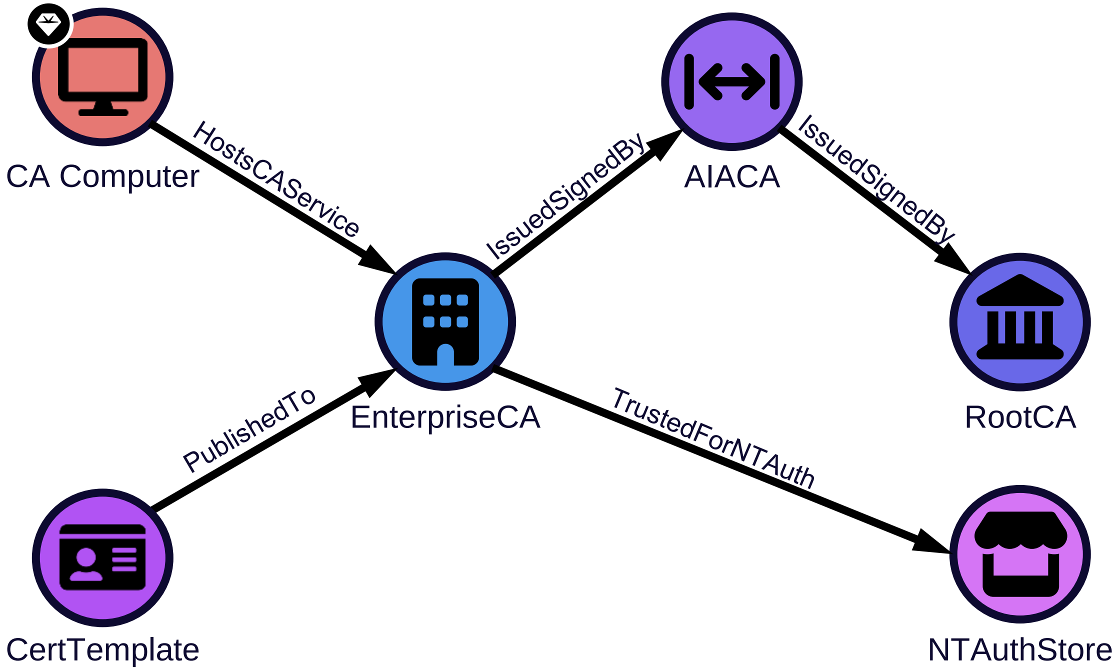
ADCS Components

- ADCS enables impersonation as anyone
  - Takeover control of Tier Zero
- Which components enables takeover?
  - Or disruption of Tier Zero



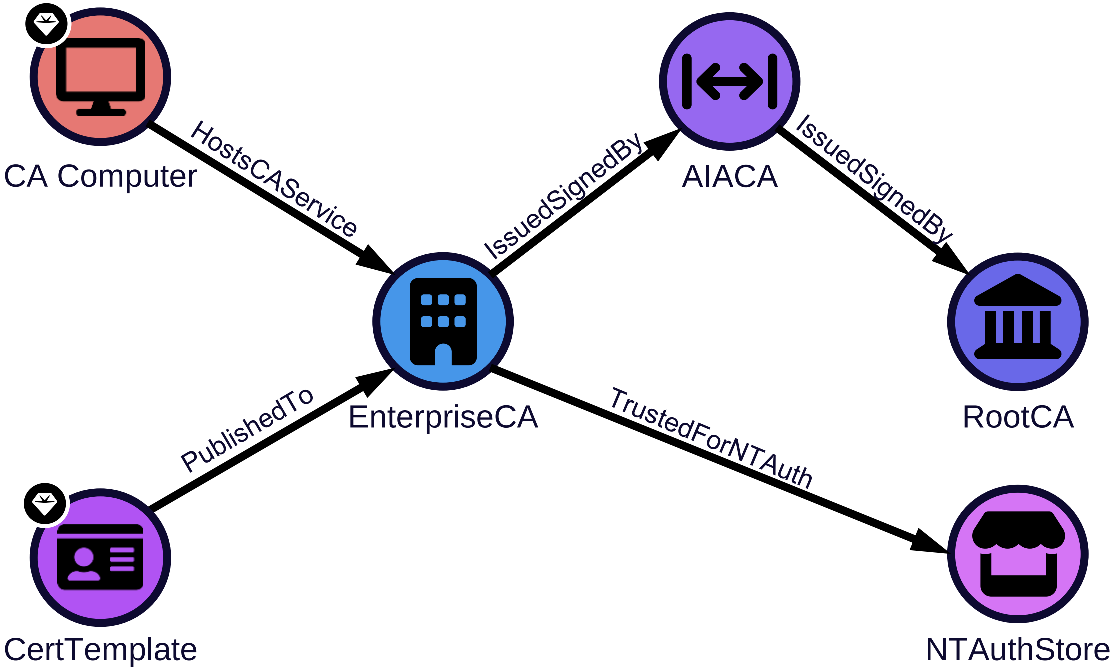
CA Computer

Tier Zero Compromise	Possibly (GoldenCert or ESC7)
Compromise actions	Forge cert, approve denied requests, modify pending requests ..
Compromise pre-reqs	CA certificate is trusted
Is Tier Zero	Yes



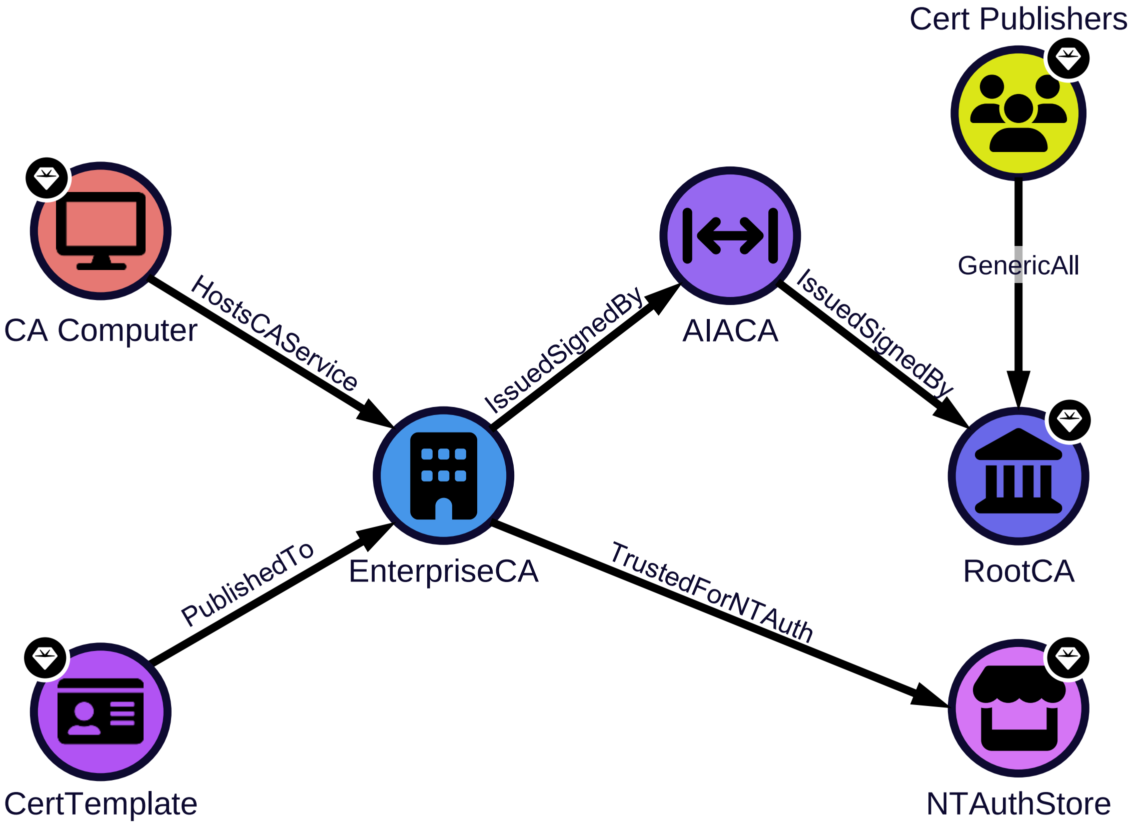
CertTemplate

Tier Zero Compromise	Possibly (ESC4)
Compromise actions	Modify template to enable ESCx
Compromise pre-reqs	Published to CA CA is trusted by NTAuth and root CA
Is Tier Zero	Yes



RootCA and NTAuthStore

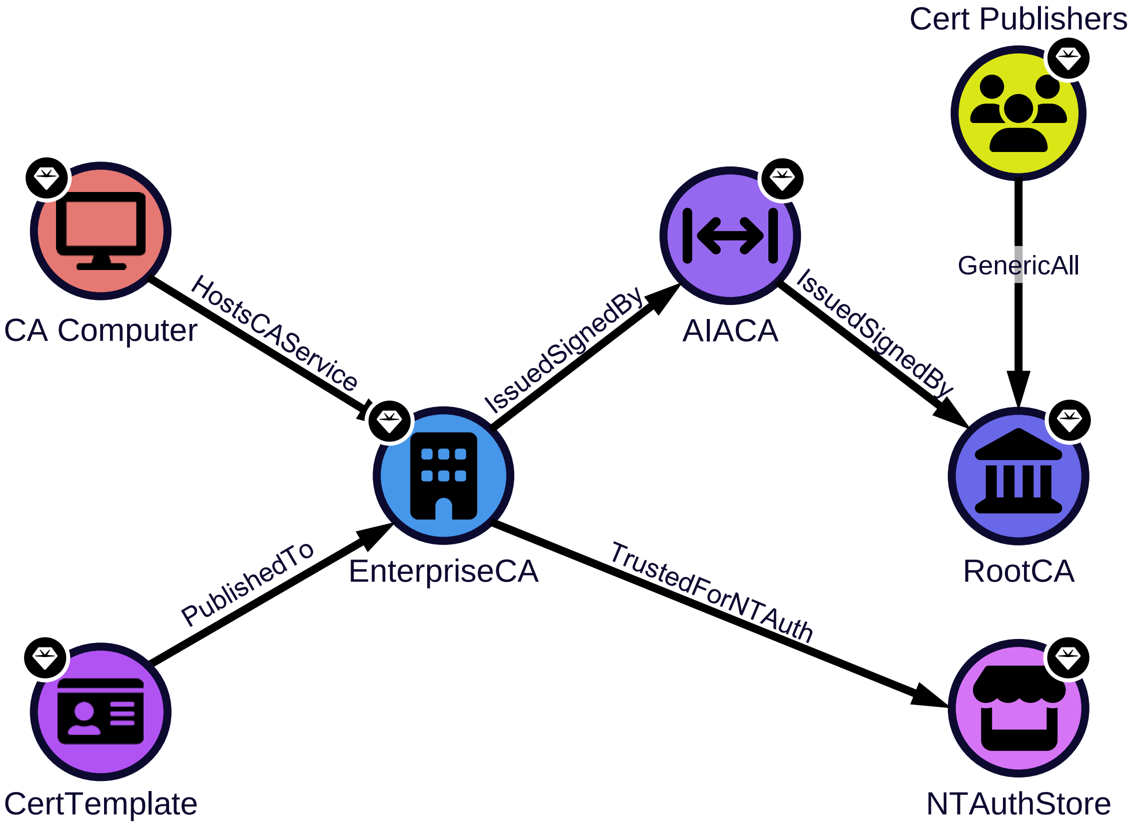
Tier Zero Compromise	ESC5
Compromise actions	Add attacker root CA certificate Make it trusted by NTAuth store
Compromise pre-reqs	None
Is Tier Zero	Yes



https://decoder.cloud/2023/11/20/a-deep-dive-in-cert-publishers-group/ (Andrea Pierini)

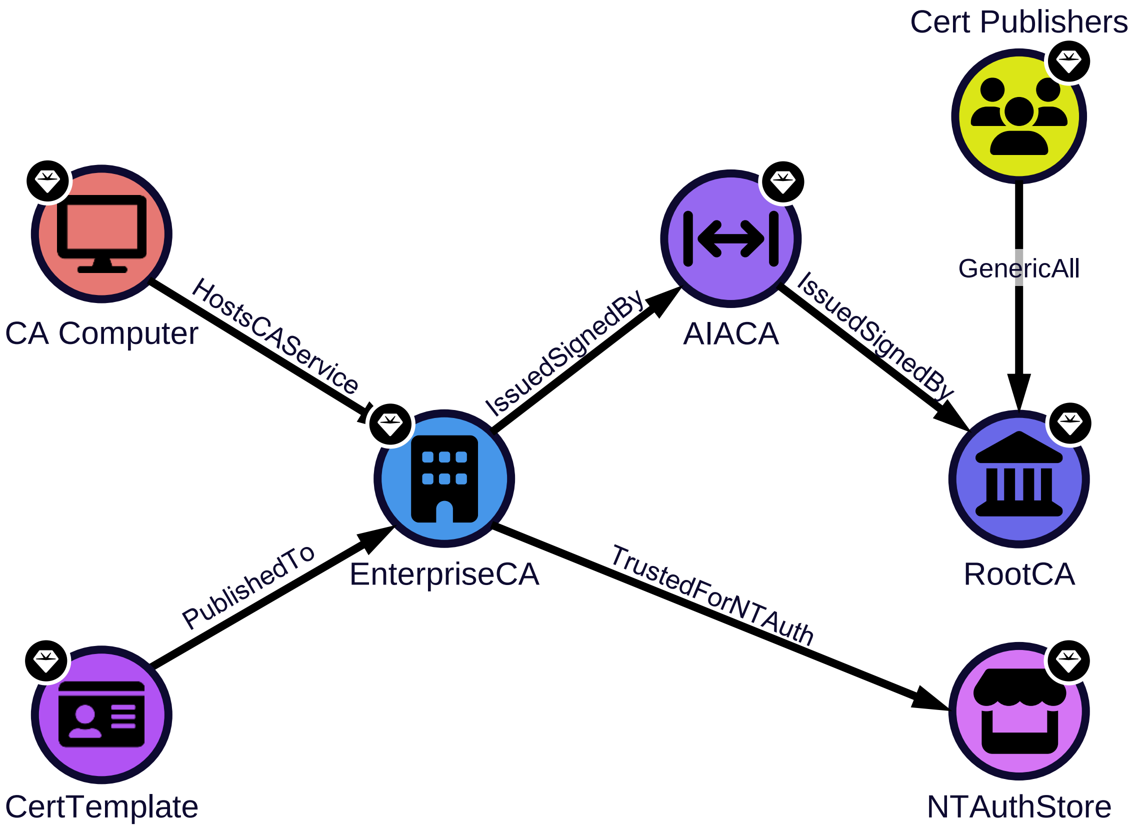
EnterpriseCA and AIACA

Tier Zero Compromise	Disruption
Compromise actions	Delete the objects (break CA chain)
Compromise pre-reqs	None
Is Tier Zero	Yes

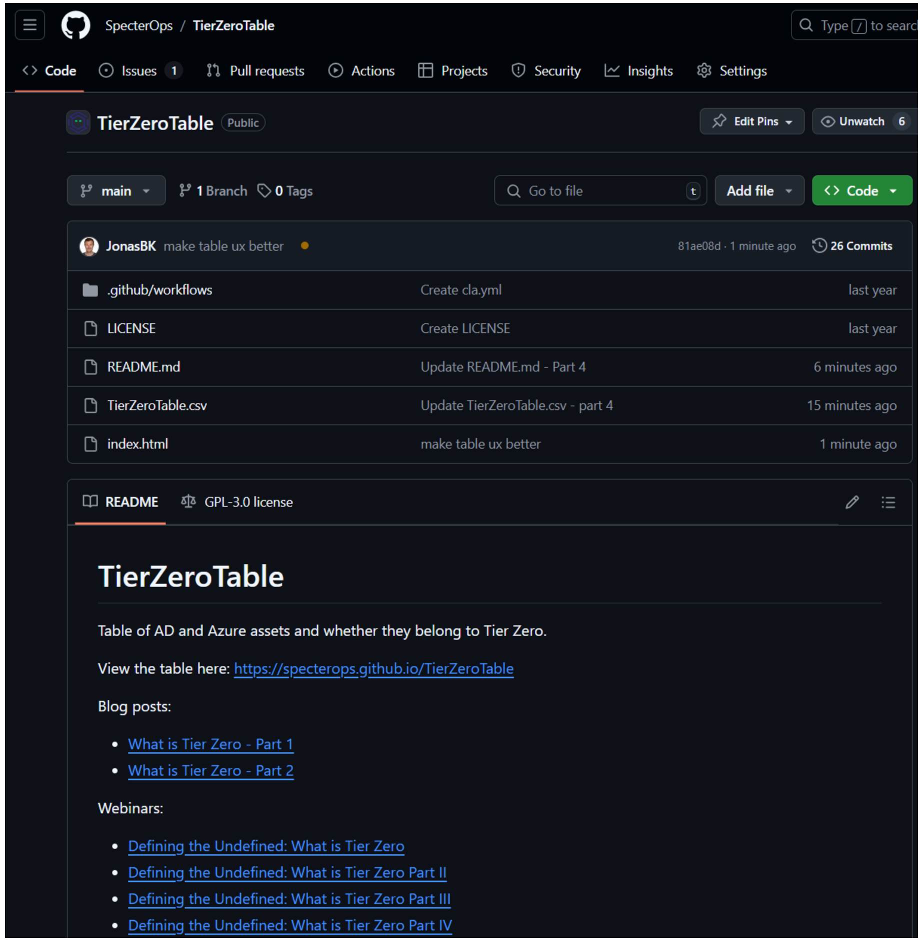


ADCS - Summary

- ADCS has Tier Zero takeover control
- Many components are Tier Zero security dependencies
- **Recommendation:**
  - Treat ADCS as Tier Zero
  - Non-Tier Zero has no control over ADCS by default – don't change that!
  - No ADCS? Maybe another PKI solution?



Tier Zero Table



TierZeroTable

JonasBK make table ux better 81ae08d · 1 minute ago

.github/workflows	Create cla.yml	last year
LICENSE	Create LICENSE	last year
README.md	Update README.md - Part 4	6 minutes ago
TierZeroTable.csv	Update TierZeroTable.csv - part 4	15 minutes ago
index.html	make table ux better	1 minute ago

TierZeroTable

Table of AD and Azure assets and whether they belong to Tier Zero.

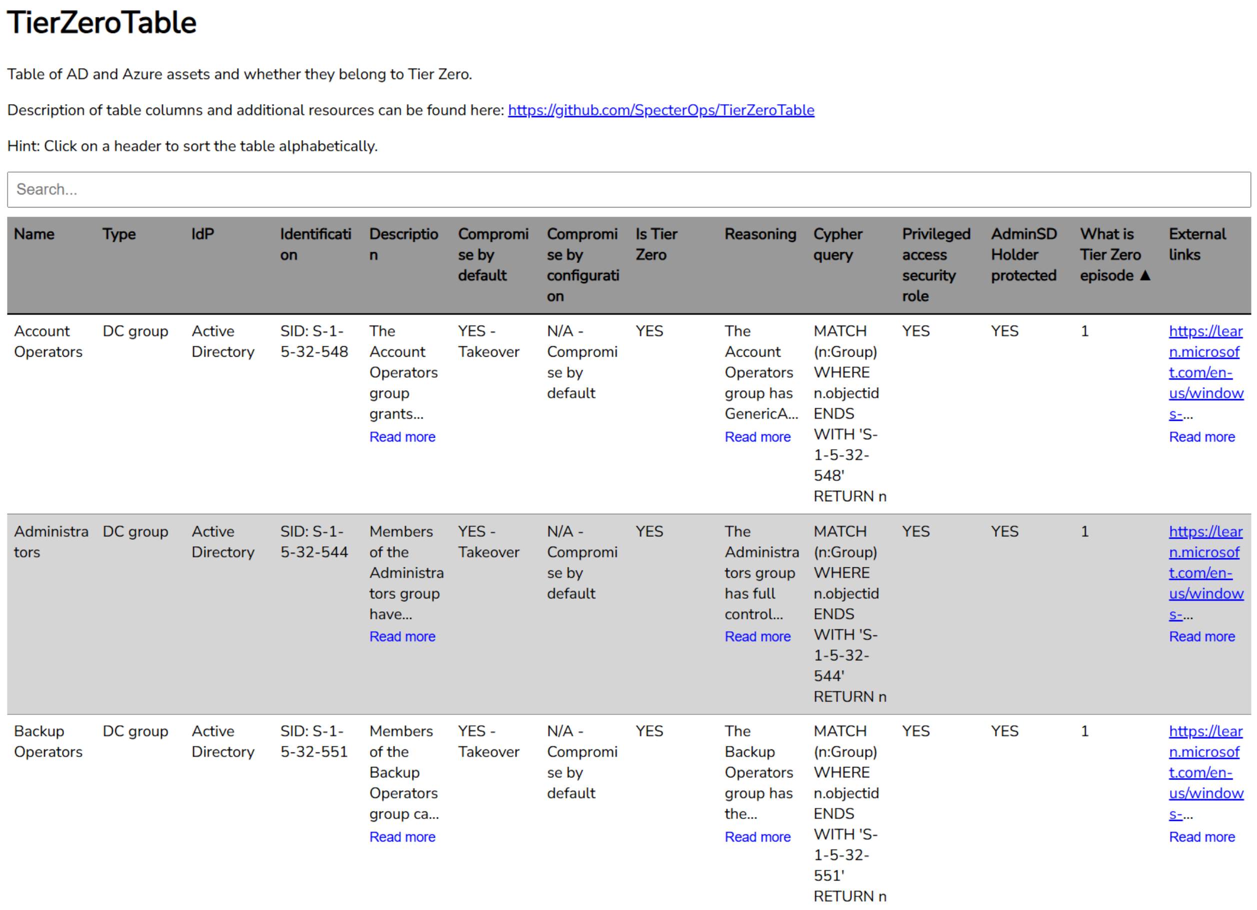
View the table here: https://specterops.github.io/TierZeroTable

Blog posts:

- What is Tier Zero - Part 1
- What is Tier Zero - Part 2

Webinars:

- Defining the Undefined: What is Tier Zero
- Defining the Undefined: What is Tier Zero Part II
- Defining the Undefined: What is Tier Zero Part III
- Defining the Undefined: What is Tier Zero Part IV



TierZeroTable

Table of AD and Azure assets and whether they belong to Tier Zero.

Description of table columns and additional resources can be found here: https://github.com/SpecterOps/TierZeroTable

Hint: Click on a header to sort the table alphabetically.

Search...

Name	Type	IdP	Identification	Description	Compromise by default	Compromise by configuration	Is Tier Zero	Reasoning	Cypher query	Privileged access security role	AdminSD Holder protected	What is Tier Zero episode ▲	External links
Account Operators	DC group	Active Directory	SID: S-1-5-32-548	The Account Operators group grants... Read more	YES - Takeover	N/A - Compromise by default	YES	The Account Operators group has GenericA... Read more	MATCH (n:Group) WHERE n.objectid ENDS WITH 'S-1-5-32-548' RETURN n	YES	YES	1	https://learn.microsoft.com/en-us/windows-... Read more
Administrators	DC group	Active Directory	SID: S-1-5-32-544	Members of the Administrators group have... Read more	YES - Takeover	N/A - Compromise by default	YES	The Administrators group has full control... Read more	MATCH (n:Group) WHERE n.objectid ENDS WITH 'S-1-5-32-544' RETURN n	YES	YES	1	https://learn.microsoft.com/en-us/windows-... Read more
Backup Operators	DC group	Active Directory	SID: S-1-5-32-551	Members of the Backup Operators group ca... Read more	YES - Takeover	N/A - Compromise by default	YES	The Backup Operators group has the... Read more	MATCH (n:Group) WHERE n.objectid ENDS WITH 'S-1-5-32-551' RETURN n	YES	YES	1	https://learn.microsoft.com/en-us/windows-... Read more

- https://github.com/SpecterOps/TierZeroTable
- Submit your contributions or refinements

Questions